# РЕШЕНИЕ (ЕС) 2022/640 НА КОМИСИЯТА

**от 7 април 2022 година**

**относно правилата за прилагане на ролите и отговорностите на основните участници в областта на сигурността**

ЕВРОПЕЙСКАТА КОМИСИЯ,

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

като взе предвид Решение (ЕС, Евратом) 2015/443 на Комисията от 13 март 2015 г. относно сигурността в Комисията ([1]),

като взе предвид Решение (ЕС, Евратом) 2015/444 на Комисията от 13 март 2015 г. относно правилата за сигурност за защита на класифицираната информация на ЕС ([2]),

като има предвид, че:

(1) Решения (ЕС, Евратом) 2015/443 и (ЕС, Евратом) 2015/444 се прилагат за всички отдели на Комисията и във всички помещения на Комисията.

(2) При необходимост се приемат правила за прилагане с цел допълване или подкрепа на Решение (ЕС, Евратом) 2015/444 в съответствие с член 60 от него.

(3) Мерките за сигурност за защита на класифицираната информация на ЕС по време на целия ѝ жизнен цикъл следва да бъдат съобразени по-специално с нейната класификация за сигурност.

(4) Мерките за сигурност за защита на комуникационните и информационните системи в Комисията са определени в Решение (ЕС, Евратом) 2017/46 на Комисията ([3]), по-специално в член 3 относно принципите на информационна сигурност в Комисията и член 9 относно отговорниците на системи.

(5) Целта на правилата за прилагане относно ролите и отговорностите на основните участници в областта на сигурността е да се предоставят насоки относно предварителните условия и задълженията, определени за тези роли в решения (ЕС, Евратом) 2015/443 и (ЕС, Евратом) 2015/444.

(6) В член 36, параграф 7 от Решение (ЕС, Евратом) 2015/444 са определени редица допълнителни функции, свързани със сигурността, които да бъдат поети от органа по сигурността на Комисията. Задачите, свързани с тези функции, са определени в настоящото решение.

(7) Местните служители по сигурността и ръководителите на регистратурата имат специфични отговорности за защитата на класифицираната информация на ЕС в своите отдели в съответствие с Решение (ЕС, Евратом) 2015/444.

(8) На 4 май 2016 г. Комисията прие решение ([4]) за оправомощаване на члена на Комисията, който отговаря за въпросите на сигурността, да приеме от името на Комисията и на нейна отговорност правилата за прилагане, предвидени в член 60 от Решение (ЕС, Евратом) 2015/444; впоследствие на 13 април 2021 г. членът на Комисията, отговарящ за въпросите на сигурността, прие от името на Комисията и на нейна отговорност решение ([5]) за вторично делегиране на тези правила за прилагане на генералния директор на Генерална дирекция „Човешки ресурси и сигурност“,

([1]) ОВ L 72, 17.3.2015 г., стр. 41.
([2]) ОВ L 72, 17.3.2015 г., стр. 53.
([3]) Решение (ЕС, Евратом) 2017/46 на Комисията от 10 януари 2017 г. относно сигурността на комуникационните и информационните системи в Европейската комисия (ОВ L 6, 11.1.2017 г., стр. 40).
([4]) Решение C(2016) 2797 final от 4 май 2016 г. относно оправомощаване, свързано със сигурността.
([5]) Решение C(2021) 2684 final от 13 април 2021 г. за вторично делегиране на правомощия, предоставени с Решение C(2016) 2797 на Комисията относно оправомощаване, свързано със сигурността.

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Глава 1

## Общи разпоредби

*Член 1*

### Предмет и приложно поле

1. В настоящото решение се определят ролите и отговорностите на основните участници в областта на сигурността, които отговарят за защитата на класифицираната информация на ЕС (КИЕС) в Комисията съгласно решения (ЕС, Евратом) 2015/443 и (ЕС, Евратом) 2015/444.

2. Настоящото решение се прилага за всички отдели на Комисията и във всички помещения на Комисията.

Глава 2

## Генерална дирекция „Човешки ресурси и сигурност“

*Член 2*

### Орган по сигурността на Комисията

1. Директорът на дирекция „Сигурност“ на Генерална дирекция „Човешки ресурси и сигурност“ е органът по сигурността на Комисията, посочен в член 7 от Решение (ЕС, Евратом) 2015/444.

2. Органът по сигурността на Комисията изпълнява функциите си в следните области, както е посочено в Решение (ЕС, Евратом) 2015/444, в съответствие с членове 3—7 от това решение:

а) мерки за сигурност по отношение на персонала;

б) физическа сигурност;

в) управление на КИЕС;

г) акредитация на комуникационните и информационни системи (КИС), работещи с КИЕС;

д) индустриална сигурност; както и

е) обмен на класифицирана информация.

3. Органът по сигурността на Комисията осигурява задължително обучение за местните служители по сигурността и заместниците им, както и за ръководителите на регистратурата и заместниците им относно техните отговорности и задължения.

*Член 3*

### Орган по осигуреността на информацията

Органът по осигуреността на информацията отговаря за следните дейности във връзка със защитата на КИЕС:

а) разработване на политики и насоки за сигурност по отношение на осигуреността на информацията и наблюдение на тяхната ефективност и целесъобразност;

б) опазване и администриране на техническата информация, свързана с криптографските продукти;

в) гарантиране, че мерките за осигуряване на информация са в съответствие с политиките на Комисията за сигурност и възлагане на обществени поръчки, ако е целесъобразно;

г) гарантиране, че криптографските продукти се подбират в съответствие с политиките, уреждащи тяхната пригодност и избор;

д) провеждане на консултации с отговорниците на системи, доставчиците на системи, участниците в областта на сигурността и представителите на потребителите във връзка с политиките и насоките за сигурност по отношение на осигуреността на информацията.

*Член 4*

**Орган по акредитиране на сигурността**

1. Органът по сигурността на Комисията отговаря за акредитацията на зоните за сигурност, които отговарят на изискванията на член 18 от Решение 2015/444, и на КИС за работа с КИЕС.

2. Отделите на Комисията се консултират с органа по акредитиране на сигурността в координация със своите местни служители по сигурността и ръководители на регистратурата, ако е целесъобразно, когато даден отдел възнамерява:

а) да създаде зона за сигурност;

б) да въведе КИС за работа с КИЕС;

в) да инсталира друго оборудване за работа с класифицирана информация, включително връзки с КИС на трета страна.

Органът по акредитиране на сигурността предоставя консултации по отношение на тези дейности както по време на планирането, така и по време на изграждането или разработването.

3. С КИЕС не се работи в зона за сигурност или КИС, преди органът по акредитиране на сигурността да е издал акредитация на съответното ниво на КИЕС.

4. Изискванията за акредитиране на зона за сигурност включват:

а) одобряване на плановете за зоната за сигурност;

б) одобряване на всички договори за дейности, извършвани от външни изпълнители, като се вземат предвид разпоредбите относно индустриалната сигурност, като например изискванията за провеждане на проучване за надеждност на изпълнителите и техния персонал;

в) наличие на всички необходими декларации и сертификати за съответствие;

г) физическа инспекция на зоната за сигурност, за да се провери дали строителните материали и методи, контролът на достъпа, оборудването за сигурност и всички други елементи отговарят на изискванията, издадени от органа по сигурността на Комисията;

д) валидиране на мерките за противодействие срещу електромагнитното излъчване за всяка техническа зона за сигурност;

е) одобряване на оперативните процедури за сигурност за зоната за сигурност.

5. Изискванията за акредитиране на КИС, работеща с КИЕС, включват:

а) създаване на стратегия за акредитация на системата;

б) валидиране на плана за сигурност на КИС въз основа на подход за управление на риска;

в) валидиране на оперативните процедури за сигурност за КИС;

г) валидиране на всички други необходими документи за сигурност, определени от органа по акредитиране на сигурността;

д) одобрение на всяко използване на технологии за криптиране;

е) валидиране на мерките за противодействие срещу електромагнитното излъчване за КИС, работещи с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо;

ж) проверка на КИС, за да се провери дали документираните мерки за сигурност се прилагат правилно.

6. След успешно изпълнение на изискванията за акредитация органът по акредитация на сигурността издава официално разрешение за работа с КИЕС в зоната за сигурност или КИС за определено максимално ниво на КИЕС и за срок до 5 години в зависимост от нивата на КИЕС, с които се работи, и свързаните с тях рискове.

7. При уведомление за нарушение на сигурността или значителна промяна в проекта или мерките за сигурност на зона за сигурност или КИС органът по акредитиране на сигурността преразглежда и, ако е необходимо, може да отнеме разрешението за работа с КИЕС, докато не бъдат разрешени всички установени проблеми.

*Член 5*

**Орган по TEMPEST**

1. Мерките за сигурност по TEMPEST се прилагат за защита на КИС, работещи с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, и могат да се прилагат за информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED.

2. Органът по TEMPEST отговаря за одобряването на мерките, предприети за защита против компрометирането на КИЕС чрез непреднамерени електронни излъчвания.

3. По искане на отговорник на система за КИС, работеща с КИЕС, органът по TEMPEST издава спецификации за мерките за сигурност по TEMPEST, които са подходящи за нивото на класификация на информацията.

4. Органът по TEMPEST извършва технически изпитвания по време на акредитацията на зоните за сигурност и КИС за работа с КИЕС с ниво на класификация за сигурност CONFIDENTIAL UE/EU CONFIDENTIAL или по-високо и след успешно изпитване издава удостоверение по TEMPEST.

5. В сертификата по TEMPEST се посочва най-малко следното:

а) датата на провеждане на теста;

б) описание на мерките за сигурност по TEMPEST с планове на помещенията;

в) срока на валидност на сертификата;

г) всякакви промени, които ще обявят сертифицирането за невалидно;

д) подпис на органа по TEMPEST.

6. Местен служител по сигурността или организатор на заседание, отговарящ за организирането на класифицирано заседание, в координация с местен служител по сигурността, може да поиска от органа по TEMPEST да тества заседателните зали, за да се гарантира, че те са технически обезопасени.

*Член 6*

**Орган за криптографско одобрение**

1. Органът за криптографско одобрение отговаря за одобряването на използването на технологии за криптиране.

2. Органът за криптографско одобрение издава насоки относно изискванията за използването и одобряването на технологии за криптиране.

3. Органът за криптографско одобрение одобрява използването на решения за криптиране въз основа на искане от отговорника на система. Одобрението се дава въз основа на задоволителна оценка най-малко на следното:

а) нуждите от сигурност на информацията, която трябва да бъде защитена;

б) преглед на КИС, участващи в решението;

в) оценка на присъщите и остатъчните рискове;

г) описание на предложеното решение;

д) оперативните процедури за сигурност за решението за криптиране.

4. Органът за криптографско одобрение води регистър на одобрените решения за криптиране.

*Член 7*

**Орган за разпределение на криптографски материали**

1. Органът за разпределение на криптографски материали отговаря за разпределението на криптографски материали, използвани за защита на КИЕС (главно оборудване за криптиране, криптографски ключове, удостоверения и съответни средства за удостоверяване на автентичността), на:

а) потребители или отдели в рамките на Комисията във връзка с КИС, които се администрират от външни лица;

б) потребители или организации извън Комисията във връзка с КИС, които се администрират от Комисията.

2. Органът за разпределение на криптографски материали може да делегира на други отдели разпределението на криптографски материали за трети страни в съответствие с член 17, параграф 3 от Решение 2015/443.

3. Органът за разпределение на криптографски материали гарантира, че всички криптографски материали се изпращат по сигурни канали, които защитават срещу подправяне и показват доказателства за това, в съответствие с правилата за сигурност, приложими за нивото на класификация на КИЕС, която ще бъде защитена с тези материали.

4. Органът за разпределение на криптографски материали предоставя насоки на местния служител по сигурността и, когато е приложимо, на местния служител по ИТ сигурността на всеки отдел на Комисията, който участва в производството, разпределението или използването на криптографските материали.

5. Органът за разпределение на криптографски материали гарантира, че са създадени подходящи оперативни процедури за сигурност за процеса на разпределение.

Глава 3

**Отдели на Комисията**

*Член 8*

**Началници на отдели**

1. Всеки началник на отдел назначава:

а) местен служител по сигурността и един или повече заместници, когато това е уместно за отдела или кабинета;

б) ръководител на регистратурата и един или повече заместници, когато това е уместно за всеки отдел, който управлява регистратура на КИЕС;

в) отговорник на система за всяка КИС, работеща с КИЕС.

2. Началникът на отдела иска одобрение от директора на дирекция „Сигурност“ на Генерална дирекция „Човешки ресурси и сигурност“ преди назначаването на местните служители по сигурността и заместниците им, както и на ръководителите на регистратурата и заместниците им.

3. Началникът на отдела определя всички длъжности, за които е необходимо разрешение за достъп до КИЕС, като се консултира с местния служител по сигурността. Кандидатите за такива длъжности се уведомяват за изискването за провеждане на проучване за надеждност по време на процеса на набиране на персонал.

4. Началникът на всеки отдел, притежаващ КИЕС, отговаря за активирането на планове за унищожаване и евакуация при извънредни ситуации, когато това е необходимо. Плановете включват алтернатива за ситуации, при които не може да се осъществи връзка с началника на отдела.

*Член 9*

**Отговорници на системи за КИС, работещи с КИЕС**

1. Отговорникът на система се свързва с органа по акредитиране на сигурността на възможно най-ранен етап в рамките на проект за внедряване на КИС, работеща с КИЕС, за да определи съответните стандарти и изисквания за сигурност и да започне процеса на акредитиране на сигурността.

2. Отговорникът на система гарантира, че мерките за сигурност отговарят на изискванията на органа по акредитиране на сигурността и че КИС не работи с КИЕС, преди да бъде акредитирана.

3. Отговорникът на система се свързва с органа за криптографско одобрение, за да получи одобрение да използва дадена технология за криптиране. Отговорниците на системи не използват технологии за криптиране в производствените системи без предварително одобрение.

4. Отговорникът на система се консултира с ръководителя на регистратурата на отдела по въпросите, свързани със сигурността на КИС.

5. Най-малко веднъж годишно отговорникът на система прави преглед на мерките за сигурност, които се прилагат към дадена система, включително на нейния план за сигурност.

6. Когато в КИС възникне инцидент, свързан със сигурността, при който се посочва, че КИС вече не може да осигури адекватна защита на КИЕС, отговорникът на система информира местния служител по сигурността и незабавно се свързва с органа по акредитиране на сигурността, за да получи съвет как да се процедира. В този случай акредитацията може да бъде временно прекратена и системата може да бъде извадена от експлоатация, докато не бъдат предприети подходящи коригиращи действия.

7. Отговорникът на система предоставя на органа по акредитиране на сигурността пълна подкрепа по всяко време за задълженията му, свързани с акредитирането на КИС.

*Член 10*

**Оперативен орган по осигуреността на информацията**

Оперативният орган по осигуреността на информацията за всяка КИС:

а) изготвя документация по сигурността в съответствие с политиките и насоките за сигурност, по-специално плана за сигурност, свързаните със системата оперативни процедури за сигурност и криптографската документация в рамките на процеса на акредитиране на КИС;

б) участва в избора и изпитването на специфичните за системата мерки, уреди и софтуер за техническа сигурност с цел контрол на прилагането им и гарантиране, че те са инсталирани, конфигурирани и поддържани съгласно съответната документация по сигурността;

в) участва в избора на мерки и устройства за сигурност по TEMPEST, ако това се изисква в плана за сигурност, и в сътрудничество с органа по TEMPEST гарантира, че те са монтирани и поддържани по сигурен начин;

г) наблюдава изпълнението и прилагането на оперативните процедури за сигурност, свързани с функционирането на системата;

д) управлява и работи с криптографски продукти в сътрудничество с органа за разпределение на криптографски продукти, за да гарантира правилното съхранение на криптографски материали и контролирани елементи и, ако е необходимо, осигурява генерирането на криптографски променливи;

е) извършва анализи, прегледи и изпитвания на сигурността, по-специално за изготвяне на съответните доклади за риска, съгласно изискванията на органа по акредитиране на сигурността;

ж) предоставя специфично за КИС обучение по осигуреността на информацията;

з) въвежда и прилага специфични за КИС мерки за сигурност.

Глава 4

**Местен служител по сигурността**

*Член 11*

**Назначаване на местния служител по сигурността**

1. Местните служители по сигурността и заместниците им са длъжностни лица или срочно наети служители.

2. Всички местни служители по сигурността и заместниците им притежават валидно разрешение за достъп до КИЕС с ниво на класификация за сигурност до ниво SECRET UE/EU SECRET и при необходимост до ниво TRES SECRET UE/EU TOP SECRET. Местните служители по сигурността и заместниците им получават разрешение за достъп преди тяхното назначаване.

3. Представителствата на Комисията могат да поискат от органа по сигурността на Комисията да предостави изключение от изискванията, посочени в параграфи 1 и 2.

*Член 12*

**Оперативни процедури за сигурност за зоните за сигурност**

1. Местният служител по сигурността на съответния отдел на Комисията изготвя оперативни процедури за сигурност за всяка зона за сигурност, за която отговаря.

2. Местният служител по сигурността гарантира, че оперативните процедури за сигурност включват следните изисквания:

а) само служители с валидно разрешение за достъп и установена необходимост от достъп до документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо получават достъп без придружител до зона за сигурност в работно време;

б) достъп без придружител до зона за сигурност извън работно време се предоставя само на местния служител по сигурността на отдела, на ръководителя/ите на регистратурата в зоната за сигурност, на техните заместници и на упълномощени служители от дирекция „Сигурност“ на Генерална дирекция „Човешки ресурси и сигурност“;

в) устройства за записване и комуникация, като например мобилни телефони, компютри, камери или други интелигентни устройства, не се допускат в зоните за сигурност без предварително разрешение от органа по сигурността на Комисията; за всяка дерогация се изисква предварително разрешение от органа по сигурността на Комисията; местният служител по сигурността действа като звено за контакт;

г) целият вътрешен или външен персонал, който се нуждае от достъп до зона за сигурност, но не отговаря на критериите, посочени в буква а) по-горе, ще бъде придружаван и наблюдаван по всяко време от надлежно упълномощен служител; всеки такъв достъп до зона за сигурност се записва в дневник, който се води на входа на зоната за сигурност;

д) местният служител по сигурността гарантира, че системите за откриване на проникване, които наблюдават дадена зона за сигурност, са активни и функционират правилно по всяко време, и управлява всички свързани с тях пароли, ключове, PIN номера или други механизми за достъп и удостоверяване на идентичността.

е) алармените сигнали в зона за сигурност се докладват на дирекция „Сигурност“ на Генерална дирекция „Човешки ресурси и сигурност“, която незабавно уведомява местния служител по сигурността;

ж) местният служител по сигурността на отдела, в който се намира зоната за сигурност, води регистър за всяка намеса след алармен сигнал или инцидент, свързан със сигурността;

з) налице са процедури, които обхващат случаите на тревога или друга извънредна ситуация в зоната за сигурност, включително евакуация на персонала и осигуряване на бързо реагиране от авариен екип под ръководството на органа по сигурността на Комисията и външни служби за спешна помощ, ако е необходимо;

и) местният служител по сигурността незабавно докладва на органа по сигурността на Комисията за всяко нарушение на сигурността, настъпило в зона за сигурност или включващо такава зона, за да определи подходящия отговор;

й) отделните офиси, стаи и сейфове в рамките на дадена зона за сигурност се държат заключени, когато бъдат оставени без надзор;

к) служителите избягват обсъждането на класифицирана информация в коридорите или други общи части на зоната за сигурност, когато в близост се намират неоправомощени лица.

*Член 13*

**Ключове и комбинации за сигурност**

1. Местният служител по сигурността носи цялата отговорност за осигуряване на правилното боравене и съхранение на ключовете и комбинациите, използвани в зоните за сигурност или за достъп до тях. Ключовете и комбинациите се съхраняват в сейф и са защитени най-малко на същото ниво като материала, до който дават достъп.

2. Местният служител по сигурността поддържа регистър на сейфовете и блиндираните помещения, заедно с актуален списък на всички служители, които имат достъп до тях без придружител.

3. Местният служител по сигурността поддържа регистър на ключовете за сейфовете и блиндираните помещения, включително на служителите, на които те са разпределени. За всеки издаден ключ се съхранява разписка, която включва идентификацията на ключа, получателя, датата и часа.

4. Ключове и комбинации се издават само на служители, които отговарят на условието „необходимост да се знае“ и на които е предоставено съответното разрешение за достъп до КИЕС. Местният служител по сигурността отнема ключовете, когато тези условия вече не са изпълнени.

5. Местният служител по сигурността съхранява резервни ключове и писмен запис на всяка комбинация в отделни запечатани, непрозрачни, подписани и датирани пликове, които се предоставят от служителя, отговарящ за ключовете. Тези пликове се съхраняват в сейф, който е одобрен за съхранение на материали с най-високо ниво на класификация, които се съхраняват в съответния сейф или в блиндирано помещение.

6. Ако при промяна на комбинацията или смяна на притежателя на ключа има доказателства за нарушаване на целостта или за повреда на даден плик, местният служител по сигурността третира това като инцидент, свързан със сигурността, и незабавно уведомява органа по сигурността на Комисията.

7. Промените в шифровите комбинации на сейфовете в зоните за сигурност се извършват под надзора на местния служител по сигурността. Комбинациите се актуализират най-малко на всеки 12 месеца и всеки път, когато:

а) е получен нов сейф или е монтирана нова ключалка (по-специално комбинациите по подразбиране се сменят незабавно);

б) налице е съмнение за компрометиране на информация или случай на компрометиране на информация;

в) достъпът вече не е разрешен за лице, притежаващо комбинация.

8. Местният служител по сигурността води регистър на датите на промените в комбинациите, посочени в параграф 7.

*Член 14*

**Планове за евакуация и унищожаване на КИЕС при извънредни ситуации**

1. Местният служител по сигурността подпомага ръководителя на отдела при изготвянето на планове за евакуация и унищожаване на КИЕС при извънредни ситуации въз основа на насоките, предоставени от дирекция „Сигурност“ на Генерална дирекция „Човешки ресурси и сигурност“.

2. Местният служител по сигурността гарантира, че оборудването, необходимо за изпълнението на плановете, предвидени в параграф 1, е леснодостъпно и се поддържа в добро работно състояние.

3. Местният служител по сигурността, заедно с длъжностните лица, номинирани в плановете, предвидени в параграф 1, прави преглед на степента на готовност на плановете най-малко на всеки 12 месеца и предприема всички необходими действия за актуализирането им.

*Член 15*

**Разрешения за достъп**

1. Местният служител по сигурността поддържа регистър на всички длъжности в отдела, за които се изисква разрешение за достъп от Комисията, и на персонала, заемащ тези длъжности. Провеждането на проучване за надеждност трябва да бъде посочено в обявлението за свободна длъжност по време на процеса на набиране на персонал и да бъде съобщено на кандидата по време на събеседването.

2. Местният служител по сигурността наблюдава всички искания за разрешения за достъп до КИЕС. Местният служител по сигурността е звеното за контакт в рамките на отдела и поддържа връзка с органа по сигурността на Комисията относно разрешенията за достъп.

3. Местният служител по сигурността подава искане за започване на процедура за издаване на разрешение за достъп на съответния служител и гарантира, че служителят незабавно връща на органа по сигурността на Комисията въпросника за национално разрешение за достъп до класифицирана информация.

4. Местният служител по сигурността гарантира, че служителите в отдела, които са преминали проучването за надеждност, посещават задължителното обучение за работа с КИЕС, за да получат разрешението си за достъп.

5. Местният служител по сигурността поддържа редовна връзка със службата за човешки ресурси на отдела за информация относно всички промени в длъжностите, за които се изисква разрешение за достъп, и незабавно информира органа по сигурността на Комисията за всяка такава промяна.

6. Местният служител по сигурността уведомява органа по сигурността на Комисията за пристигането на нов служител, притежаващ съществуващо разрешение за достъп до класифицирана информация, за да заеме длъжност, за която е необходим упълномощен служител с достъп.

7. Местният служител по сигурността гарантира, че служителите в отдела завършват процедурата за подновяване на разрешение за достъп до класифицирана информация в определения срок. Всеки служител, който откаже да приключи процедурата, е длъжен да се премести на длъжност, за която не е необходим упълномощен служител с достъп.

*Член 16*

**Регистратура на КИЕС**

1. Когато даден отдел управлява регистратура на КИЕС, местният служител по сигурността упражнява надзор върху дейностите на ръководителите на регистратурата, свързани с работата с КИЕС, и спазването на правилата за сигурност за защита на КИЕС.

2. Местният служител по сигурността извършва следните проверки най-малко на всеки 12 месеца и при смяна на ръководител на регистратурата или негов заместник:

а) проверка на извадка от документи в регистратурата на КИЕС, за да се потвърди техният статус и точността на регистъра на класифицираните документи;

б) проверка на извадка от разписки и фишове за предаване относно разпределението на КИЕС към регистратурата на КИЕС и от нея;

в) проверка на извадка от сертификати за унищожаване.

3. Поне веднъж месечно местният служител по сигурността извършва проверки на място на регистъра на класифицираните документи и на наскоро получените класифицирани документи, за да се увери, че документите се регистрират правилно.

4. Всички проверки се вписват в дневника на регистъра на класифицираните документи.

*Член 17*

**Други отговорности, свързани със сигурността**

Другите отговорности на местния служител по сигурността, свързани със сигурността, се посочват в известие за сигурност, което обхваща по-специално физическата сигурност на лицата, помещенията и другите активи, както и информацията.

Глава 5

**Ръководител на регистратурата**

*Член 18*

**Назначаване на ръководителя на регистратурата**

1. Ръководителите на регистратурата и заместниците им са длъжностни лица или срочно наети служители.

2. Всички ръководители на регистратурата и заместниците им притежават валидно разрешение за достъп до КИЕС с ниво на класификация за сигурност до ниво SECRET UE/EU SECRET и при необходимост до ниво TRES SECRET UE/EU TOP SECRET. Ръководителите на регистратурата и заместниците им получават разрешение за достъп преди тяхното назначаване.

3. Представителствата на Комисията могат да поискат от органа по сигурността на Комисията да предостави изключение от изискванията, посочени в параграфи 1 и 2.

*Член 19*

**Отговорности**

1. Ръководителите на регистратурата регистрират информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо за целите на сигурността в следните случаи:

а) при постъпването ѝ в отдел на Комисията или при излизането ѝ от него; или

б) при постъпването ѝ в КИС или при излизането ѝ от нея.

2. Ръководителите на регистратурата регистрират всички събития през жизнения цикъл на цялата информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо. Ръководителите на регистратурата също така гарантират, че се поддържа регистър на цялата информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED или негов еквивалент, която се обменя с трети държави и международни организации. Това се извършва в координация с регистратурата на КИЕС, управлявана от Генералния секретариат.

3. Ръководителят на регистратурата регистрира документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо в регистъра на класифицираните документи и гарантира, че те се съхраняват по сигурен начин в регистратурата на КИЕС.

4. Ръководителят на регистратурата подпомага служителите на Комисията при създаването и изпращането на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо.

5. Когато документи с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо се получават от други отдели или външни лица, ръководителят на регистратурата гарантира, че разписката за доставка е надлежно върната на наредителя.

6. Преди да разреши на даден служител достъп до класифициран документ, съхраняван от регистратурата на КИЕС, ръководителят на регистратурата проверява при местния служител по сигурността дали служителят има разрешение за достъп от органа по сигурността на Комисията.

7. Ръководителят на регистратурата регистрира всички служители, влизащи и излизащи от регистратурата на КИЕС, които нямат разрешение за достъп без придружител, и ги придружава по време на посещението им.

8. Когато служител вземе документ за справка извън регистратурата на КИЕС, ръководителят на регистратурата се уверява, че служителят е запознат със съответните компенсаторни мерки за сигурност и че документът е върнат веднага щом вече не е необходим. Ръководителят на регистратурата напомня на служителите да върнат всеки такъв документ във възможно най-кратък срок.

9. Регистратурата на КИЕС издава удостоверение за куриер, ако класифицираните документи се пренасят на ръка извън държавата, в която се намира регистратурата.

10. В известието за сигурност се съдържат подробни инструкции за ръководителите на регистратурата относно регистрирането на класифицирани документи.

*Член 20*

**Понижаване на нивото на класификация и декласифициране**

Ръководителят на регистратурата подпомага отделите, изготвящи информацията, в процеса на преглед на регистрираната КИЕС, за да се установи дали първоначалното ниво на класификация все още е подходящо или дали нивото на класификация на документа може да бъде понижено или премахнато.

*Член 21*

**Унищожаване**

1. Ръководителите на регистратурата отговарят за унищожаването на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и по-високо с одобрени средства, когато е целесъобразно, в присъствието на свидетели с разрешение за достъп.

2. Ръководителите на регистратурата вписват всяко унищожаване на информация с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL и по-високо в регистъра на класифицираните документи и съхраняват съответните удостоверения за унищожаване в регистъра на КИЕС.

*Член 22*

**Допълнителни задачи**

1. Ръководителят на регистратурата оказва цялото необходимо съдействие на местния служител по сигурността при извършването на надзорни дейности в регистратурата на КИЕС.

2. Ръководителят на регистратурата докладва всички предполагаеми или действителни инциденти, свързани със сигурността, на местния служител по сигурността, който на свой ред ги докладва на органа по сигурността на Комисията.

3. Ръководителят на регистратурата на КИЕС на отдел на Комисията, който организира заседание с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, подготвя КИЕС, с която ще се работи по време на заседанието, и координира действията си с организатора на заседанието, за да се гарантира, че всички документи и разписки се обработват в съответствие с приложимите правила.

Глава 6

**Заключителни разпоредби**

*Член 23*

**Прозрачност**

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

*Член 24*

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

Съставено в Брюксел на 7 април 2022 година.

*За Комисията,*
*от името на председателя,*
Gertrud INGESTAD
*Генерален директор*
*Генерална дирекция „Човешки ресурси и сигурност“*