ЕВРОПЕЙСКА СМЕТНА ПАЛАТА

Решение № 041-2021 на Сметната палата относно правилата за сигурност за защита на класифицираната информация на ЕС (КИЕС)

ЕВРОПЕЙСКАТА СМЕТНА ПАЛАТА,

КАТО ВЗЕ ПРЕДВИД — Член 13 от Договора за Европейския съюз,

КАТО ВЗЕ ПРЕДВИД — Член 287 от Договора за функционирането на Европейския съюз,

КАТО ВЗЕ ПРЕДВИД — Член 257 от Регламент (ЕС, Евратом) 2018/1046 на Европейския парламент и на Съвета от 18 юли 2018 г. относно финансовите правила, приложими за общия бюджет на Съюза,

КАТО ВЗЕ ПРЕДВИД — Член 1, параграф 6 от правилата за прилагане на Процедурния правилник на Сметната палата (Решение № 21-2021 на Сметната палата),

КАТО ВЗЕ ПРЕДВИД — правилата за сигурност за защита на класифицираната информация на ЕС на другите институции, агенции и органи на ЕС,

КАТО ВЗЕ ПРЕДВИД — политиката на Сметната палата за сигурност на информацията (Решение № 127/15 FINAL) и политиката за класифициране на информацията (Съобщение до персонала № 123/2020),

КАТО ИМА ПРЕДВИД, ЧЕ — съгласно член 287, параграф 3 от ДФЕС Сметната палата има право на достъп до всички съответни документи и информация, които счита за необходими за изпълнението на своите провомощия, включително класифицирана информация на ЕС (КИЕС), които трябва да се осъществяват при пълно спазване на принципа на лоялно сътрудничество между институциите и принципа на предоставената компетентност; че правото на достъп до КИЕС, гарантирано от ДФЕС, не може да бъде поставено под въпрос от създателя на КИЕС, като има предвид, че от Сметната палата може да бъде поискано да въведе определени мерки за сигурност и да ги спазва, както е описано подробно в настоящото решение;

КАТО ИМА ПРЕДВИД, ЧЕ — членовете на Сметната палата, длъжностните ѝ лица, както и другите ѝ служители, са обвързани дори след прекратяване на служебното правоотношение със задължението за поверителност съгласно член 339 от ДФЕС, член 17 от Правилника за длъжностните лица и актовете, приети в съответствие с него;

КАТО ИМА ПРЕДВИД, ЧЕ — предвид чувствителния характер на КИЕС, работата с нея изисква спазване на задължението за поверителност, което следва да се

гарантира посредством подходящи мерки за сигурност, които могат да осигурят високо ниво на защита на тази информация и които са еквивалентни на тези, установени с правилата за защита на КИЕС, приети от другите институции, агенции и органи на ЕС. В следствие на това, ако Сметната палата счете, че такива мерки за сигурност не са обосновани предвид естеството и вида на КИЕС, тя си запазва правото да отправя всички възражения, които счита за целесъобразни, като същевременно се запазва нивото на класификация на КИЕС;

КАТО ИМА ПРЕДВИД, ЧЕ мерките за сигурност за защита на поверителността, интегритета и наличността на информацията, която се съобщава на Сметната палата, трябва да бъдат подходящи за естеството и вида на съответната информация;

КАТО ИМА ПРЕДВИД, ЧЕ на Сметната палата трябва да бъде осигурен достъп до класифицирана информация в съответствие с принципа „необходимост да се знае“ с цел изпълнение на задачите, възложени от Договорите и от приетите въз основа на Договорите правни актове;

КАТО ИМА ПРЕДВИД, ЧЕ предвид естеството и чувствителното съдържание на определена информация, е целесъобразно да се създаде специална процедура за работата на Сметната палата с документи, съдържащи КИЕС;

КАТО ИМА ПРЕДВИД, ЧЕ институцията трябва да гарантира, че настоящото решение се изпълнява в съответствие с всички приложими правила, по-конкретно с разпоредбите относно защитата на личните данни, физическата сигурност на лица, сгради и ИТ, и публичния достъп до документи;

РЕШИ:

Член 1. Предмет и приложно поле

1. С настоящото решение се установяват основните принципи и минимални стандарти за сигурност с оглед на защитата на класифицираната информация, с която Сметната палата работи при упражняването на своите правомощия.

2. За целите на настоящото решение класифицирана информация означава всяка от следните видове информация:

   а) „класифицирана информация на ЕС“ (КИЕС), определена в правилата за сигурност на други институции, агенции, органи или служби на ЕС, и която носи един от следните грифове за сигурност:

   - TRÈS SECRET UE/EU TOP SECRET: информация и материали, чието неразрешено разкриване би могло да увреди изключително сериозно съществените интереси на Европейския съюз или на една или повече от държавите членки;
   - SECRET UE/EU SECRET: информация и материали, чието неразрешено разкриване би могло да увреди сериозно съществените интереси на Европейския съюз или на една или повече от държавите членки;

- CONFIDENTIEL UE/EU CONFIDENTIAL: информация и материали, чието неразрешено разкриване би могло да увреди съществените интереси на Европейския съюз или на една или повече от държавите членки;
- RESTREINT UE/EU RESTRICTED: информация и материали, чието неразрешено разкриване би се отразило неблагоприятно на интересите на Европейския съюз или на една или повече от държавите членки.

б) класифицирана информация, предоставена от държави членки, която носи национален гриф за сигурност, равностоен на един от грифовете за сигурност на КИЕС[1], изброени в буква а);

в) класифицирана информация, предоставена на Европейската сметна палата от трети държави или от международни организации, която носи гриф за сигурност, равностоен на един от грифовете за сигурност на КИЕС, изброени в буква а), в съответствие със съответните споразумения за сигурност на информацията или административни договорености.

3. Сметната палата работи с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED на място в сградите си и предприема всички необходими защитни мерки за тази цел. Предприемат се действия за осигуряване на достъп на служителите на Сметната палата, които се нуждаят от достъп до по-високи нива на КИЕС, в подходящи помещения на други институции, органи или агенции на ЕС.

4. Настоящото решение се прилага за всички структури и помещения на Сметната палата.

5. Освен ако дадена разпоредба не касае специфични групи служители, настоящото решение се прилага за членовете на Сметната палата, служителите на Сметната палата,които са обхванати от Правилника за длъжностните лица и Условията за работа на другите служители на Европейския съюз[2], командированите национални експерти (КНЕ) в Сметната палата, доставчиците на услуги и техните служители, стажантите и всички лица, имащи достъп до сгради или друга собственост на Сметната палата или до информация, която се управлява от Сметната палата.

6. Освен ако не е посочено друго, разпоредбите относно КИЕС се прилагат по еквивалентен начин за класифицираната информация, посочена в параграф 2, буква б) и буква в) от настоящия член.

Член 2. Определения

За целите на настоящото решение:

а) „Разрешение за достъп до КИЕС“ означава решение на директора на дирекция „Човешки ресурси, финанси и административно обслужване“ на Сметната палата въз основа на уверение, предоставено от компетентен орган на държава членка, че дадено длъжностно лице на Сметната палата, друг служител или командирован

[1] Вж. Споразумението между държавите — членки на Европейския съюз, заседаващи в рамките на Съвета, относно защитата на класифицирана информация, която се обменя в интерес на Европейския съюз, от 4 май 2011 г. и приложенията към него (ОВ 2011/C 202/13).

[2] Регламент № 31 (ЕИО) за установяване на Правилника за длъжностните лица и Условията за работа на другите служители, изменен, ОВ 01962R0031-01.01.2020-019.003-1 (https://eur-lex.europa.eu/eli/reg/1962/31 (1)/2020-01-01).

национален експерт може да получи достъп до КИЕС на определено ниво (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо) до определена дата, при условие че за това лице е била установена „необходимост да се знае“ и то е било информирано по подходящ начин за своите отговорности; тогава въпросното лице ще бъде „с издадено разрешение за достъп“.

б) „Класификация“ означава класифицирането на информация с определен гриф въз основа на степента на увреждане, която би могло да причини нейното неразрешено разкриване.

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

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

д) „Документ“ означава всяка записана информация, независимо от нейната форма или физически характеристики.

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

ж) „Удостоверение за сигурност на структура“ означава административно определяне от компетентен орган по сигурността, че от гледна точка на сигурността дадена структура може да осигури адекватна защита на КИЕС на определено ниво на класификация за сигурност.

з) „Работа с КИЕС“ означава всички възможни действия, на които може да бъде подложена КИЕС през жизнения ѝ цикъл: създаване, регистриране, обработване, пренасяне, понижаване на нивото на класификация, декласификация и унищожаване. По отношение на комуникационните и информационните системи (КИС) това включва и нейното събиране, показване, предаване и съхраняване.

и) „Притежател“ означава надлежно оправомощено лице с установена необходимост да знае“, което притежава класифицирана информация и поради това носи отговорност за нейната защита.

й) „Орган по сигурността на информацията“ означава служителят по сигурността на информацията на Сметната палата, който може изцяло или частично да делегира предвидените в настоящото решение задачи.

к) „Информация“ означава всяка писмена или устна информация, независимо от нейния материален носител или автор.

л) „Материал“ означава документ, носител на данни или машина или оборудване.

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

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

о) „Удостоверение за разрешение за достъп на служител“ (УРДС) означава удостоверение, издадено от директора на дирекция „Човешки ресурси, финанси

и административно обслужване“ на Сметната палата, с което се удостоверява, че дадено лице притежава валидно удостоверение за разрешение за достъп или разрешение за достъп, в което се посочва нивото на класификация на КИЕС, до което лицето може да има достъп (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо), датата, до която е валидно съответното удостоверение или разрешение, и датата, на която изтича валидността на самото удостоверение.

п) „Орган по физическата сигурност“ означава ръководителят по сигурността на Сметната палата, който отговаря за изпълнението на необходимите мерки и процедури за физическа сигурност за защита на КИЕС.

р) Служба „Документи“ се ръководи от Секретариата на Сметната палата, разположен в административна зона, за която отговаря директорът на дирекция „Човешки ресурси, финанси и административно обслужване“ на Сметната палата. Тя отговаря за влизането и излизането на информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED или неговия еквивалент, която се обменя със Сметната палата.

с) „Регистратура за КИЕС“ е зона, създадена в рамките на зона за сигурност. Тази регистратура се ръководи от ръководителя на регистратура на Сметната палата, който има разрешение за достъп и е оправомощен. Тя отговаря за влизането и излизането на информация с класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или неин еквивалент, която се обменя със Сметната палата.

т) „Орган по акредитиране на сигурността (ОАС)“ означава директорът на дирекция „Човешки ресурси, финанси и административно обслужване“ на Сметната палата.

Член 3. Мерки за защита на КИЕС

1. Сметната палата гарантира защитата на цялата класифицирана информация, която ѝ се предоставя, по определен от създателя и съизмерим с нивото на класификация начин, и в съответствие с настоящото решение.

2. За тази цел Сметната палата прави така, че работата с КИЕС да подлежи на мерки за физическа сигурност, а където е целесъобразно, и на подходящи мерки за сигурност по отношение на персонала, включително разрешения за достъп на определени лица и мерки за защита на комуникационните и информационните системи. Тези мерки са описани в членове 4—6 и се прилагат за целия жизнен цикъл на КИЕС. Те съответстват на нивото на класификация за сигурност на КИЕС, формата и обема на информацията или материалите, местоположението и конструкцията на структурите, в които се намира КИЕС, както и оценката на местно ниво на риска от злонамерени и/или престъпни действия, включително шпионаж, саботаж и тероризъм.

3. КИЕС се защитава с мерки за физическа сигурност, а информацията с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо се защитава допълнително с мерки за сигурност по отношение на персонала.

4. КИЕС може да се предоставя единствено на лица с „необходимост да се знае“ в рамките на институцията. Притежател на дадена КИЕС трябва да я защитава, както се изисква от настоящото решение.

5. КИЕС не трябва да се разкрива устно или писмено. Предварителните констатации и оценки, доклади, становища, съобщения за пресата и други продукти на Сметната палата, нейният уебсайт и интранет, устни интервенции, отговори на искания за достъп

до документи[3] и гласови или видео записи не трябва да съдържат или да се позовават на КИЕС или на цитати от нея. Ако обаче създателят е публикувал документи или информация, съдържаща препратка към КИЕС, тази препратка трябва да бъде посочена.

6. Независимо от параграф 5, Сметната палата и създателят на информацията може да се договорят, че в случай на специален одит Сметната палата може да възпроизведе или да използва в даден документ елементи от КИЕС. В такъв случай документът на Сметната палата първо се адресира до създателя на въпросната КИЕС преди или по време на съгласувателната процедура. В тази ситуация Сметната палата и създателят на информацията се договарят дали да класифицират публикувания от Сметната палата документ. Когато докладващ член на Сметната палата счете за необходимо да изпрати одитен доклад, който е класифициран изцяло или отчасти, до определени получатели в Европейския парламент или Съвета — като се вземат предвид всички мерки за сигурност, свързани с настоящото решение — това изисква съгласието на създателя на класифицираната информация. Правната рамка и процедура за обмен на такива документи е определена в член 7.

7. Когато упражняването на правомощията на Сметната палата изисква споделянето на класифициран документ или информация с по-широка аудитория, преди да реши да използва тези елементи или информация, Сметната палата се консултира със създателя на документа/информацията, като надлежно взема предвид грифа за сигурност, ако счита че е налице по-висш обществен интерес за това. Информацията се използва единствено в доклада по такъв начин, че да не може да навреди на интереса на нейния създател. Това може да се гарантира по подходящ начин, като от създателя на информацията се поиска да изрази коментари за постигане на споразумение за начина за анонимизиране, съкращаване или обобщаване на информацията и т.н., и същевременно се зачитат интересите на онези, които основно са засегнати от публикуваната информация.

8. Сметната палата не предоставя КИЕС на друга институция, агенция, орган или служба на ЕС, държава членка, трета държава или международна организация, без да се консултира предварително с нейния създател и без неговото изрично писмено съгласие.

9. Освен ако създателят на даден документ с ниво на класификация за сигурност SECRET UE/EU SECRET или по-ниско не е наложил ограничения за неговото размножаване или за превода му, такива документи могат да бъдат размножавани или превеждани по искане на притежателя и в съответствие с инструкциите за практическа работа на органа по сигурността на информацията в Сметната палата. Мерките за сигурност, приложими към оригиналния документ, се прилагат и към неговите копия и преводи.

10. Ако е необходимо Сметната палата да понижи или да премахне нивото на класификация на класифициран документ, който е получила или за който има разрешение за достъп, тя се свързва с неговия създател, за да го попита дали може да предостави версия на документа, която е с понижено ниво на класификация или е декласифицирана.

<u>Член 4.</u> Сигурност по отношение на персонала

1. По силата на изпълняваните от тях функции членовете на Сметната палата се оправомощават да имат достъп до цялата КИЕС и да участват в заседания, на които се

[3] Съгласно Решение № 12-2005 на Сметната палата относно публичния достъп до документи на Сметната палата, изменено с Решение № 14-2009 (ОВ 2009/C 67/1).

разглежда КИЕС. Членовете се информират за задълженията им по защитата на КИЕС и приемат писмено своята отговорност за защитата на такава информация.

2. Служител на Сметната палата, независимо дали е длъжностно лице или друг служител, който се подчинява на Условията за работа на другите служители, или КНЕ, получава достъп до КИЕС само след като:

   i. бъде установена неговата „необходимост да знае“;

   ii. е бил информиран за правилата за сигурност за защита на КИЕС и за съответните стандарти и насоки за сигурност и е заявил писмено своята отговорност за защитата на такава информация; и

   iii. в случай че дадена информация е с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, е преминал проучване за надеждност и е получил разрешение за достъп.

3. В контекста на процедурата за определяне дали на длъжностно лице или на друг член на персонала на Сметната палата може да бъде разрешен достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, се вземат под внимание лоялността, почтеността и надеждността на служителя. След получаване на уверение от компетентните органи на дадена държава членка, както е посочено в член 2, буква н), този достъп се определя в делегирано решение, взето в съответствие с член 10, параграф 10. Решенията за предоставяне на разрешение за достъп се вземат от директора на дирекция „Човешки ресурси, финанси и административно обслужване“ на Сметната палата.

4. Директорът на дирекция „Човешки ресурси, финанси и административно обслужване“ на Сметната палата може да издава УРДС, в което се посочва нивото на класификация за сигурност, за което на лицето може да се издава достъп до КИЕС (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо), датата, до която е валидно съответното разрешение за достъп, и датата на изтичане на УРДС.

5. Само лица с посоченото в параграф 2, подточка iii) по-горе разрешение и членове на Сметната палата съгласно параграф 1 по-горе могат да участват в заседания, на които се работи с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо. Сметната палата и създателят ни информацията осигуряват реда и условията за провеждане на такива заседания за всеки отделен случай.

6. Структурите на Сметната палата, които отговарят за организирането на заседанията, на които се работи с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, информират своевременно органа по сигурността на информацията за датата, часа и мястото на заседанията и предоставят списък на участниците.

7. Всяко лице, което притежава КИЕС без надлежно разрешение и/или без доказана „необходимост да се знае“, съобщава на органа по сигурността на информация за ситуацията възможно най-скоро и гарантира защитата на КИЕС, както се изисква в настоящото решение.

<u>Член 5.</u> Мерки за физическа сигурност за защита на класифицирана информация

1. „Физическа сигурност“ означава използване на физически и технически защитни мерки за предотвратяване на неразрешен достъп до КИЕС.

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

3. Зоните, в които се работи с КИЕС или се съхранява такава, подлежат на редовни проверки от компетентния орган по сигурността на Сметната палата.

4. За работа или за съхранение на КИЕС се използват само оборудване или устройства, които отговарят на приложимите в рамките на институциите, агенциите или органите на ЕС правила за защита на КИЕС.

5. Персоналът на Сметната палата може да има достъп до КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, или равностойно в зони за сигурност извън помещенията на Сметната палата.

6. Сметната палата може да сключи споразумение за нивото на обслужване с друга институция на ЕС в Люксембург, за да може да работи или да съхранява информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо в зона за сигурност на тази институция. Освен ако не е дадено специално съгласие от създателя, в помещенията на Сметната палата не се работи с КИЕС, нито такава информация се съхранява, дублира или превежда от Сметната палата.

7. Получена информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED се регистрира от Сметната палата. Разглеждане на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, или равностойно извън помещенията на Сметната палата се регистрира за целите на сигурността.

8. КИЕС с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED може да се съхранява в подходящи заключващи се офис мебели в административна зона или в зона за сигурност. КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET се съхранява в сейф в зона за сигурност на друга институция на ЕС в Люксембург съгласно споразумение за нивото на обслужване.

9. Извън регистратурата КИЕС се предава между структурите и помещенията, както следва:

   а) като общо правило КИЕС се предава чрез електронни средства, защитени чрез криптографски продукти, одобрени в съответствие с член 6, параграф 8;

   б) ако не се предава, както е описано в буква а), КИЕС се предава посредством носител на данни (напр. USB памет, компактдиск, твърд диск), защитен чрез криптографски продукти, одобрени в съответствие с член 6, параграф 8, или на хартиен носител в непрозрачен запечатан плик.

10. Информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICED може да бъде унищожена от притежателя в съответствие с приложимите в Сметната палата правила за архивиране. Информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо се унищожава единствено от ръководителя на регистратурата, когато е инструктиран за това от притежателя или от компетентен орган в съответствие с приложимите в Сметната палата правила за архивиране. Документи с ниво на класификация за сигурност SECRET UE/EU SECRET се унищожават в присъствието на свидетел с разрешение за достъп, съответстващо най-малко на нивото на класификация на документа, който ще се унищожава. Ръководителят на

регистратурата и свидетелят, когато се изисква присъствие на такъв, подписват документ за унищожаване, който се завежда в регистратурата. Ръководителят на регистратурата съхранява информация за унищожаването на документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET най-малко пет години.

11. Органът по физическа сигурност и органът по сигурността на информацията изготвят съвместен план, като вземат под внимание местните условия, за безопасното съхраняване на КИЕС по време на кризи, включително, когато е необходимо, планове за нейното унищожаване или евакуация в случай на извънредна ситуация. Те издават такива указания, каквито счетат за целесъобразни, за предотвратяване на попадането на КИЕС в ръцете на неоправомощени лица.

12. Когато е необходимо физическо транспортиране на КИЕС, Сметната палата спазва наложените от създателя мерки, за да я опази от неразрешено разкриване по време на транспорта.

13. Мерките за физическа сигурност, които се прилагат в административни зони, в които се съхранява или се работи с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, са посочени в приложението.

<u>Член 6.</u> Защита на КИЕС в комуникационни и информационни системи

1. За целите на настоящия член „комуникационна и информационна система“ означава система, даваща възможност за работа с КИЕС в електронен формат. Една комуникационна и информационна система обхваща всички активи, необходими за нейното функциониране, включително инфраструктура, организация, персонал и информационни ресурси.

2. „Легитимен ползвател“ означава член, длъжностно лице, друг служител на Сметната палата или КНЕ с установена и призната необходимост от достъп до конкретна информационна система.

3. Сметната палата дава уверение, че нейните системи ще защитават в подходяща степен информацията, с която работят, и ще функционират, както е необходимо и когато е необходимо, под контрола на легитимните ползватели. За тази цел те гарантират подходящи нива на:

   - автентичност: гаранцията, че информацията е истинска и от добросъвестни източници;
   - наличност: характеристиката на информацията да бъде достъпна и използваема при поискване от оправомощен субект;
   - поверителност: характеристиката, че информацията не е разкрита на неоправомощени лица, субекти или процеси;
   - цялост: характеристиката, че информацията и активите са запазили точността и пълнотата си;
   - невъзможност за отказ: способността да се докаже, че дадено действие или събитие действително е настъпило, така че това действие или събитие да не може впоследствие да бъде отречено.

   Тази осигуреност се основава на процес за управление на риска. „Риск“ означава възможността дадена заплаха да използва вътрешни или външни видове уязвимост на дадена организация или на някоя от системите, които тази организация използва, и по този начин да нанесе вреди на организацията и на нейните материални или нематериални активи. Рискът се измерва като съчетание от вероятността от

осъществяване на заплахи и тяхното въздействие. Процесът на управление на риска се състои от следните стъпки: определяне на заплахите и уязвимостите; оценка на риска; третиране на риска; приемане на риска и съобщаване на риска.

- „Оценка на риска“ — състои се от установяване на заплахите и видовете уязвимост и от анализ на съответните рискове, т.е. анализ на вероятността и въздействието.
- „Третиране на риска“ — изразява се в смекчаване, отстраняване, намаляване (чрез подходящо съчетание от технически, физически, организационни или процедурни мерки), прехвърляне или наблюдение на риска.
- „Приемане на риска“ означава решение за приемане на продължаващото съществуване на остатъчен риск след третиране на риска.
- „Остатъчен риск“ означава рискът, който продължава да съществува след прилагане на мерките за сигурност, предвид факта, че не може да се противодейства на всички заплахи и че не всички видове уязвимост могат да бъдат премахнати.
- „Съобщаване за рискове“ — изразява се в повишаване на осведомеността за рисковете сред общностите от ползватели на комуникационна и информационна система, информиране за такива рискове на органите, които дават одобрение, и докладване за тях на оперативните органи.

4. Всички електронни устройства и оборудване, използвани за работа с КИЕС, следва да са в съответствие с приложимите за защитата на КИЕС правила. Отдава се предпочитание на електронни устройства и оборудване, които вече са акредитирани от друга институция, агенция или орган на ЕС. Сигурността на устройствата се гарантира по време на целия им жизнен цикъл.

5. Комуникационната и информационната система на Сметната палата за работа с КИЕС се акредитира от подходящ орган. За тази цел Сметната палата се стреми да сключи споразумение за нивото на обслужване (СНО) с орган по акредитиране на сигурността на институция на ЕС, който може да акредитира КИС, работещи с КИЕС, с цел получаване на декларация за акредитация на информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, с която може да се работи в КИС на Сметната палата, както и за съответните условия за експлоатация. Освен това в СНО се посочват стандартите, които следва да се прилагат за процеса на акредитация, и то се сключва в съответствие с посочената в член 10, параграф 3 процедура.

6. В случай че е необходимо Сметната палата да установи свой собствен процес на акредитация за своята КИС, процесът се установява с делегирано решение, както е посочено в член 10, параграф 10 от настоящото решение, в съответствие със стандартите относно процеса на акредитация за работа с КИЕС в КИС в други институции, агенции и органи на ЕС.

7. Отговорност за изготвянето на акредитационните досиета и документи в съответствие с приложимите стандарти носи изцяло собственикът на КИС.

8. Когато КИЕС е защитена чрез криптографски продукти, Сметната палата отдава предпочитание на продукти, одобрени от Съвета или от генералния секретар на Съвета в качеството му на орган за криптографско одобрение, или, в противен случай, на продукти, одобрени от други институции, агенции и органи на ЕС за защита на КИЕС.

9. С информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED се работи само на електронни устройства (например работни станции, принтери, машини за копиране), разположени в административна зона или в зона за сигурност. Електронни устройства, които работят с информация с ниво на класификация за сигурност RESTREINT

UE/EU RESTRICTED, се отделят от други компютърни мрежи и се защитават посредством подходящи физически или технически мерки.

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

Член 7. Процедура за обмен и осигуряване на достъп до класифицирана информация

1. Когато е налице законово изискване по силата на Договорите или на правни актове, приети въз основа на Договорите, институциите, агенциите, органите и службите на ЕС и националните органи по собствена инициатива или при писмено искане от председателя, докладващите членове или генералния секретар предоставят достъп на Сметната палата до КИЕС съгласно процедурата по-долу.

2. Искания за достъп се изпращат на съответните институции чрез служба „Документи“ на Сметната палата.

3. Когато е необходимо, Сметната палата сключва административна договореност, обхващаща практическите аспекти за обмен на КИЕС или еквивалентна информация.

4. С цел сключване на такава административна договореност Сметната палата предоставя на създателя на информацията цялата необходима информация за своята система за информационна сигурност. Ако е необходимо, може да бъде организирано посещение за оценка.

5. Тези административни договорености се сключват при пълно спазване на принципите на предоставената компетентност и на лоялно сътрудничество, формулирани в член 13 от Договора за Европейския съюз. Те се сключват в съответствие с процедурата, определена в член 10, параграф 4.

6. Когато не съществува административна договореност с дадена институция, орган или агенция на ЕС, трета държава или международна организация за предоставяне на класифицирана информация на Сметната палата, тя подписва декларация за това, че се ангажира да защитава получената класифицирана информация.

Член 8. Нарушение на сигурността, загуба или компрометиране на класифицираната информация

1. Нарушение на сигурността означава действие или бездействие от физическо лице, което противоречи на правилата за сигурност, установени в настоящото решение и в правилата за неговото прилагане.

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

3. Всяко нарушение на сигурността или подозрение за такова нарушение се докладва незабавно на органа по сигурността на информацията на Сметната палата.

4. Когато е известно или когато има разумни основания да се предполага, че КИЕС е компрометирана или загубена, органът по сигурността на информацията информира директора на „Човешки ресурси, финанси и общи услуги“ и генералния секретар на Сметната палата. Директорът на „Човешки ресурси, финанси и общи услуги“ незабавно информира съответния орган по сигурността на създателя на информацията. Посоченият по-горе директор на Сметната палата извършва проучване, като информира генералния секретар на Сметната палата и органа по сигурността на създателя на информацията за резултатите и за предприетите мерки, за да се предотврати повторната поява на ситуацията. Когато става въпрос за член на Сметната палата, председателят на Сметната палата отговаря за предприемането на действия в сътрудничество с генералния секретар на Сметната палата.

5. Всяко длъжностно лице или друг служител на Сметната палата, който отговаря за нарушение на правилата за сигурност, установени в настоящото решение и в правилата за неговото прилагане, подлежи на предвидените в Правилника за длъжностните лица и Условията за работа на другите служители на Европейския съюз санкции.

6. Всеки член на Сметната палата, който не спазва условията на настоящото решение, подлежи на предвидените в член 286, параграф 6 от Договора мерки и санкции.

7. Всяко лице, отговорно за загуба или компрометиране на КИЕС, може да подлежи на дисциплинарно и/или съдебно производство в съответствие с приложимите закони, правила и подзаконови актове.

<u>Член 9.</u> Сигурност в случай на външна намеса

1. Сметната палата може да възложи изпълнението на задачи, които са свързани с достъп до КИЕС или изискват такъв, по силата на договор с регистрирани в дадена държава членка изпълнители. Това може да възникне по-специално във връзка с поддръжката на комуникационните и информационните системи и на компютърната мрежа.

2. В случай на външна намеса Сметната палата предприема всички необходими мерки за сигурност, посочени в параграф 3 от настоящия член, включително изискване на удостоверение за сигурност на структура, за да гарантира, че КИЕС е защитена от кандидатите или оферентите по време на процедурата за възлагане на поръчката, както и от изпълнителите и подизпълнителите през целия срок на договора. Възложителят гарантира, че предвидените в настоящото решение минимални стандарти за сигурност са посочени в договорите с цел задължаване на изпълнителите да ги спазват.

3. Правилата за сигурност, процедурите за възлагане на обществени поръчки, образците и моделите на договорите, и договорите с подизпълнител, включващи достъп до КИЕС, обявленията за обществени поръчки, насоките относно обстоятелствата, при които е необходимо удостоверение за сигурност на структура и на персонала, инструкциите за сигурност на програмата или проекта, приложенията относно аспектите на сигурността, посещенията, предаването и транспортирането на КИЕС по такива договори и договори с подизпълнители, спазват правилата, образците и моделите, установени от Европейската комисия за класифицирани договори в Решение (ЕС, Евратом) 2015/444 на Комисията от 13 март 2015 година относно правилата за сигурност за защита на класифицираната информация на ЕС.

Член 10. **Прилагане на решението и свързаните с него отговорности**

1. Структурите на Сметната палата предприемат всички необходими мерки в обхвата на техните правомощия, за да гарантират, че при работа с КИЕС или с друга класифицирана информация или при нейното съхраняване се прилагат настоящото решение и съответните правила за прилагането му.

2. Генералният секретар е органът по назначаване и органът, упълномощен да сключва трудови договори с всички длъжностни лица и други служители. Генералният секретар може да делегира отговорност на директора на дирекция „Човешки ресурси, финанси и административно обслужване“ за предоставяне на разрешение на длъжностни лица и друг персонал за достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, за упражняване на функцията му на орган по акредитиране на сигурността и за осъществяване на надзор върху Секретариата на Сметната палата по отношение на работата с КИЕС.

3. Генералният секретар е компетентен да сключва СНО относно акредитацията на комуникационно и информационно оборудване и системи на Сметната палата, относно използването на зона за сигурност в друга институция на ЕС и процедурата за искания за удостоверения за достъп на служители за достъп до КИЕС.

4. Директорът на дирекция „Човешки ресурси, финанси и административно обслужване“ е компетентен да сключва административни договорености с институциите, агенциите и други органи на ЕС за обмен на КИЕС, които се изискват от Сметната палата, за да изпълнява правомощията си. Този директор може да сключва и административни договорености с трети държави или с международни организации за защита на всяка получена класифицирана информация.

5. Директорът на дирекция „Човешки ресурси, финанси и административно обслужване“ е компетентен да подписва всяка декларация за ангажимент за защита на КИЕС, която следва да предоставя в контекста на извънредно *ad hoc* предоставяне на КИЕС.

6. Служителят по сигурността на информацията на Сметната палата действа в качеството на орган по сигурността на информацията. Служителят по сигурността на информацията и лицата, на които той може да делегира изцяло или частично своите задачи, имат подходящо разрешение за достъп. Органът по сигурността на информацията поема своите отговорности в близко сътрудничество с дирекция „Човешки ресурси, финанси и административно обслужване“, дирекция „Информация, работна среда и иновации“ и дирекция „Комитет за контрол на качеството на одита“ (вж. по-конкретно членове 4, 6 и 8). Органът по сигурността на информацията отговаря и за обученията и за срещите за повишаване на осведомеността относно сигурността на информацията, както и за периодичните проверки на спазването на настоящото решение, включително в случай на външна намеса, и за всички мерки, които следва да бъдат предприети, за да се гарантира спазването на изискванията.

7. Ръководителят по сигурността отговаря за мерките за физическа сигурност (по-конкретно член 5).

8. Служба „Документи“, създадена в рамките на Секретариата на Сметната палата, е входен и изходен пункт за информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, която Сметната палата може да обменя с други институции, агенции и органи на ЕС, държави членки. Тя е и входен и изходен пункт за еквивалентна информация на трети държави и международни организации. Служба „Документи“ е

организирана, както е определено в делегирано решение. Ръководителят на служба „Документи“ поема следните основни отговорности:

a) регистриране на влизането и излизането на информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED;

b) управление на специални за целта административни зони за регистриране на работата със, съхраняването и консултирането с КИЕС с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED.

9. Регистратура се създава съгласно СНО за използване на зоната за сигурност на друга институция на ЕС. Тази регистратура, организирана от Секретариата на Сметната палата в рамките на компетентност на директора на дирекция „Човешки ресурси, финанси и административно обслужване“, е входен и изходен пункт за информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, която Сметната палата може да обменя с други институции, агенции и органи на ЕС и държави членки. Тя е и входен и изходен пункт за еквивалентна информация на трети държави и международни организации. Тя е оборудвана с подходящи сейфове и друго оборудване за сигурност, подходящо за защита на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо. Регистратурата е организирана, както е определено в делегирано решение. Ръководителят на регистратурата има подходящо разрешение за достъп и поема следните основни отговорности:

а) управление на дейностите, свързани с регистрирането, консултирането, съхраняването, възпроизвеждането, превеждането, предаването, изпращането и, когато е целесъобразно, унищожаването на КИЕС;

б) изпълнение на всякакви други задачи, свързани със защитата на КИЕС, определени в делегирано решение.

10. Административният комитет приема делегирано решение за определяне на правила за прилагане на настоящото решение. Служителят по сигурността на информацията създава насоки относно сигурността на информацията. Комитетът за контрол на качеството на одита изготвя одитни насоки.

<u>Член 11.</u> **Влизане в сила**

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

Люксембург, 3 юни 2021 г.

За Сметната палата

Клаус-Хайнер Лене
Председател

Приложение: МЕРКИ ЗА ФИЗИЧЕСКА СИГУРНОСТ ПО ОТНОШЕНИЕ НА АДМИНИСТРАТИВНИТЕ ЗОНИ ЗА КИЕС

ПРИЛОЖЕНИЕ

МЕРКИ ЗА ФИЗИЧЕСКА СИГУРНОСТ ПО ОТНОШЕНИЕ НА АДМИНИСТРАТИВНИТЕ ЗОНИ ЗА КИЕС

1. В настоящото приложение се съдържат правилата за прилагане на член 5 от решението. Това са минимални правила за физическата защита на административни зони за информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED в Сметната палата: зони, които са определени за записването, съхранението и консултирането с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED.

2. Целта на мерките за физическа сигурност в административните зони е да се предотврати неразрешен достъп до тези зони, както следва:

   а) определя се видимо очертан периметър, който да позволява проверка на лицата;

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

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

3. Органът по сигурността на информацията на Сметната палата може по изключение да предоставя достъп на неоправомощени лица, включително за работа в административна зона, при условие че това не е свързано с достъп до КИЕС, която остава заключена. Такива лица могат да влизат само ако са придружени от органа по сигурността на информацията или от ръководителя на служба „Документи“ и непрекъснато се контролират от тях.

4. Органът по сигурността на информацията въвежда процедури за контрол на ключовете и/или цифровите комбинации за всички административни зони и заключващите се мебели. Целта на тези процедури е да се осигури защита срещу неразрешен достъп.

5. Шифровите комбинации се запаметяват от възможно най-малък брой лица на основание „необходимост да ги знаят“. Шифровите комбинации за заключващи се мебели, използвани за съхранение на информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, се променят:

   - при получаване на нова заключваща се мебел;
   - винаги когато има смяна на служител, на когото е известна комбинацията;
   - ако комбинацията е компрометирана или има подозрение за това;
   - ако дадена ключалка е преминала през поддръжка или ремонт;
   - най-малко на всеки 12 месеца.

6. Органът по сигурността на информацията и ръководителят по сигурността отговаря за спазването на тези правила.