



Съвет на
Европейския съюз

Брюксел, 29 март 2022 г.
(OR. en)

7670/22
ADD 3

Междуетноститутуционално досие:
2022/0084 (COD)

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

ПРЕДЛОЖЕНИЕ

От:	Генералния секретар на Европейската комисия, подписано от г-жа Martine DEPREZ, директор
Дата на получаване:	22 март 2022 г.
До:	Г-н Jeppe TRANHOLM-MIKKELSEN, генерален секретар на Съвета на Европейския съюз
№ док. Ком.:	COM(2022) 119 final - Annex 3
Относно:	ПРИЛОЖЕНИЕ към Предложение за РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА относно информационната сигурност в институциите, органите, службите и агенциите на Съюза

Приложено се изпраца на делегациите документ COM(2022) 119 final - Annex 3.

Приложение: COM(2022) 119 final - Annex 3



ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 22.3.2022 г.
COM(2022) 119 final

ANNEX 3

ПРИЛОЖЕНИЕ

към

**Предложение за РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА
СЪВЕТА**

**относно информационната сигурност в институциите, органите, службите и
агенциите на Съюза**

{SWD(2022) 65 final} - {SWD(2022) 66 final}

ПРИЛОЖЕНИЕ III

Мерки за физическата защита на класифицирана информация на Европейския съюз („КИЕС“)

Оборудване и организационни мерки за физическата защита на КИЕС

1. Всяка административна зона трябва да отговаря на следните изисквания:
 - а) да има видимо очертан периметър, който да позволява проверка на лицата и при възможност — на превозните средства;
 - б) прозорците в рамките на зоната, през които би могъл да се осъществи неразрешен визуален достъп до КИЕС, да са непрозрачни или оборудване с щори, завеси или друго средство за прикриване;
 - в) достъп без придружител се разрешава само на лица, надлежно оправомощени от органа по сигурността на съответната институция или орган на Съюза;
 - г) всички останали лица се придружават по всяко време или подлежат на равностойни проверки.
2. Освен на посочените в точка 1 изисквания, всяка зона за сигурност трябва да отговаря и на следните изисквания:
 - а) да има видимо очертан и защитен периметър, в който всички влизащи и излизащи винаги се проверяват;
 - б) да няма неразрешени линии за комуникации, неразрешени телефони или други неразрешени комуникационни средства и електрическо или електронно оборудване;
 - в) да е оборудвана с алармена система против проникване (IDS) и за контрол на достъпа и наблюдение в реално време, съчетана със служители за охрана и реагиране;
 - г) да се проверява в края на установеното работно време и на произволни интервали извън установеното работно време, когато не е заета от денонощно дежурен персонал и не е инсталирана система против проникване и за наблюдение в реално време;
 - д) да се управлява от обучени служители за охрана, подлежащи на надзор и надлежно проучени за надеждност;
 - е) да има оперативни процедури за сигурност, включващи следните елементи:
 - i) нивото на КИЕС, с която може да се борава в зоната и която може да се обсъжда и съхранява там;
 - ii) мерките за наблюдение и защита, които да се поддържат;
 - iii) лицата, които имат право на достъп без придружител до зоната на основание на разрешението им за достъп до КИЕС и „необходимост да се знае“;
 - iv) ако е уместно, процедури за придружаване или за защита на КИЕС, когато се разрешава достъп на други лица до зоната;
 - v) всякакви други подходящи мерки и процедури.

3. Когато влизането в зона за сигурност представлява пряк достъп до класифицираната информация в нея, зоната трябва да бъде определена като зона от клас I, а когато случаят не е такъв, зоната трябва да бъде определена като зона от клас II.

За зоните за сигурност и от двата класа, посочени в първа алинея, и в допълнение към посочените в точка 2 изисквания службата/служителят по сигурността на съответната институция или орган на Съюза трябва ясно да посочи най-високото ниво на класификация за сигурност на информацията, която обикновено се намира в зоната, и ясно да определи периметър, който дава възможност за проверка на лицата, а когато е възможно — и на превозните средства.

Институциите и органите на Съюза трябва да гарантират, че лицата, които влизат в зона за сигурност, изпълняват следните критерии:

- а) притежават специално разрешение за влизане в зоната;
 - б) придружават се непрекъснато;
 - в) преминали са през съответното проучване за надеждност, освен ако не са взети мерки да се гарантира, че достъпът до КИЕС е невъзможен.
4. За всяка техническа зона за сигурност се определя зона за сигурност, защитена срещу пасивно и активно подслушване. Прилагат се следните изисквания в допълнение към изискванията за зоните за сигурност:
- а) зоната трябва да е оборудвана със система против проникване, да бъде заключена, когато не се ползва, и да е под охрана, когато се ползва. Контролът на ключовете за зоната се осъществява в съответствие с член 29, параграф 3;
 - б) зоната трябва да се проверява редовно физически и/или технически от органа по сигурността на съответната институция или орган. Такива проверки трябва да се извършват и след всяко неразрешено влизане или при подозрение за такова влизане;
 - в) зоната трябва да има подходяща звукова защита и защита Tempest.
5. Всички лица, които влизат в технически зони за сигурност, трябва да отговарят на изискванията, посочени в точка 3.
6. Зони за сигурност и технически зони за сигурност могат да бъдат временно създадени в рамките на административна зона за целите на класифицирано заседание или други подобни цели.
7. В рамките на зоните за сигурност трябва да се изграждат блиндиращи помещения. Блиндиращото помещение представлява помещение с укрепена физическа конструкция, на което органът по сигурността на съответната институция или орган на Съюза одобрява стените, подовите, таваните, прозорците и вратите с ключалки. Такива помещения трябва да осигуряват защита, равностойна на тази на защитена каса от категорията, одобрена за съхранение на КИЕС със същото ниво на класификация за сигурност.

Физически защитни мерки за боравене с КИЕС и нейното съхранение

8. С КИЕС с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED трябва да се борава и тя да се съхранява в някоя от следните зони:
- а) в зона за сигурност;
 - б) в административна зона, при условие че КИЕС е защитена срещу достъп от страна на неоправомощени лица;
 - в) извън зона за сигурност или административна зона, при условие че притежателят се е ангажирал да спазва компенсаторните мерки, определени от органа по сигурността на всяка институция и орган на Съюза.
9. КИЕС с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED трябва да се съхранява в заключващи се офис мебели в административна зона или в зона за сигурност. Такава информация може да се съхранява временно извън административна зона или зона за сигурност, при условие че притежателят се е ангажирал да съхранява съответните документи в подходящи заключващи се офис мебели, когато те не се четат или обсъждат.
10. Институциите и органите на Съюза може да боравят с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED и да съхраняват такава информация извън своите обекти, при условие че съответната информация е защитена по подходящ начин. За целта институциите и органите на Съюза трябва да съблюдават мерките, предвидени в точка 8, буква в).
11. С информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET трябва да се борава и тя трябва да се съхранява в някоя от следните зони:
- а) в зона за сигурност;
 - б) в административна зона, при условие че КИЕС е защитена срещу достъп от страна на неоправомощени лица;
 - в) извън зона за сигурност или административна зона при ограничен обем на информацията и за ограничено време, при условие че притежателят се е ангажирал да спазва компенсаторните мерки, определени от органа по сигурността на съответната институция или орган на Съюза. В допълнение притежателят на КИЕС трябва да предприеме следните стъпки:
 - i) да уведоми съответната регистратура за факта, че с класифицираните документи се борава извън защитени зони;
 - ii) да държи документа под свой контрол през цялото време.
12. Информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET трябва да се съхранява в зона за сигурност, акредитирана за това ниво от компетентния орган по акредитиране на сигурността на съответната институция или орган на Съюза, в защитена каса или в блиндирано помещение.
13. Документи с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо може да се копират само от съответната регистратура.

14. С информация с ниво на класификация TRES SECRET UE/EU TOP SECRET трябва да се борави и тя трябва да се съхранява в зона за сигурност, акредитирана за това ниво. За целта институциите и органите на Съюза може да сключват необходимите договорености да използват зона за сигурност, на която домакин е органът по акредитиране на сигурността на друга институция или орган на Съюза и която е акредитирана от него за съответното ниво.
15. Информация с ниво на класификация TRÈS SECRET UE/EU TOP SECRET трябва да се съхранява в зона за сигурност, акредитирана за това ниво от органа по акредитиране на сигурността на компетентната институция или орган на Съюза, при някои от следните условия:
- а) в защитена каса, одобрена от органа по сигурността на всяка институция и орган на Съюза, с една или повече от следните допълнителни мерки за контрол:
 - i) постоянна защита или проверки от служители или дежурен персонал с разрешение за достъп;
 - ii) одобрена система против проникване, в съчетание със служители за охрана и реагиране;
 - б) в блиндирани помещения, оборудвани със системи против проникване, в съчетание със служители за охрана и реагиране.