



Europeiska
unionens råd

Bryssel den 29 mars 2022
(OR. en)

7670/22
ADD 3

**Interinstitutionellt ärende:
2022/0084(COD)**

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

FÖRSLAG

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	22 mars 2022
till:	Jeppe TRANHOLM-MIKKELSEN, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2022) 119 final - Annex 3
Ärende:	BILAGA till förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om informationssäkerhet i unionens institutioner, organ och byråer

För delegationerna bifogas dokument – COM(2022) 119 final - Annex 3.

Bilaga: COM(2022) 119 final - Annex 3



EUROPEISKA
KOMMISSIONEN

Bryssel den 22.3.2022
COM(2022) 119 final

ANNEX 3

BILAGA

till

förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om informationssäkerhet i unionens institutioner, organ och byråer

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

BILAGA III

Åtgärder för fysiskt skydd av säkerhetsskyddsklassificerade EU-uppgifter

Utrustning och organisatoriska åtgärder för fysiskt skydd av säkerhetsskyddsklassificerade EU-uppgifter

1. Ett administrativt utrymme ska uppfylla följande krav:
 - a) Ha en synlig yttre gräns som innebär att personer och, om möjligt, fordon kan kontrolleras.
 - b) Säkerställa att fönster som kan möjliggöra obehörig visuell tillgång till säkerhetsskyddsklassificerade EU-uppgifter inom området är ogenomskinliga eller försedda med persienn, gardiner eller andra täckande anordningar.
 - c) Obeledsagat tillträde ska endast beviljas personer som har lämpligt godkännande från säkerhetsmyndigheten vid den berörda EU-institutionen eller det berörda EU-organet.
 - d) Övriga personer ska alltid ledsagas eller genomgå likvärdiga kontroller.
2. Utöver kraven som anges i punkt 1 ska ett säkrat utrymme uppfylla följande krav:
 - a) Ha en synligt fastställd och skyddad yttre gräns genom vilken alla in- och utpasserande kontrolleras.
 - b) Vara fritt från otillåtna kommunikationslinjer, otillåtna telefoner eller annan otillåten kommunikationsutrustning och elektrisk eller elektronisk utrustning.
 - c) Vara utrustat med tillträdeskontroll och intrångsupptäcktssystem med övervakning i realtid i kombination med säkerhetspersonal.
 - d) Inspekteras i slutet av normal arbetstid, samt med slumpvisa intervall utanför normal arbetstid, om utrymmet inte är bemannat 24 timmar om dygnet och det inte finns något intrångsupptäcktssystem med övervakning i realtid.
 - e) Förvaltas av utbildad, övervakad säkerhetspersonal med lämpligt säkerhetsgodkännande.
 - f) Ha säkra driftsmetoder som omfattar följande:
 - i) Nivå av säkerhetsskyddsklassificerade EU-uppgifter som får hanteras, diskuteras och lagras i utrymmet.
 - ii) De övervaknings- och skyddsåtgärder som ska upprätthållas.
 - iii) Vilka personer som får ges obeledsagat tillträde till utrymmet i kraft av behovenlig behörighet för att få tillgång till säkerhetsskyddsklassificerade EU-uppgifter.
 - iv) Vid behov, förfaranden för ledsagare eller för skydd av säkerhetsskyddsklassificerade EU-uppgifter när eventuella andra personer beviljas tillträde till utrymmet.
 - v) Andra relevanta åtgärder och förfaranden.
3. Om inträde i ett säkrat utrymme innebär direkt tillgång till de säkerhetsskyddsklassificerade uppgifter som förvaras i det, ska området fastställas som ett utrymme av klass I, och om så inte är fallet ska området fastställas som ett utrymme av klass II.

För båda de klasser av säkrat utrymme som anges i första stycket och utöver de krav som anges i punkt 2 ska säkerhetsavdelningen/säkerhetsansvarig vid den berörda EU-institutionen eller det berörda EU-organet tydligt ange nivån på den högsta säkerhetsskyddsklassificeringen för de uppgifter som normalt förvaras i utrymmet och tydligt definiera en gräns som gör det möjligt att kontrollera personer och, om möjligt, fordon.

EU-institutioner och EU-organ måste säkerställa att personer som får tillträde till ett säkrat utrymme uppfyller följande kriterier:

- a) Har särskilt tillstånd för tillträde till utrymmet.
 - b) Alltid ledsagas.
 - c) Innehar lämpligt säkerhetsgodkännande, såvida inte åtgärder vidtas för att säkerställa att ingen tillgång till säkerhetsskyddsklassificerade EU-uppgifter är möjlig.
4. Ett säkrat utrymme som skyddas mot passiv och aktiv avlyssning ska markeras som ett tekniskt säkrat utrymme. Utöver kraven för säkrade utrymmen gäller följande krav:
- a) Utrymmet ska vara utrustat med ett intrångsupptäcktssystem, vara låst när det är tomt och bevakas när någon vistas där. Eventuella nycklar ska hanteras i enlighet med artikel 29.3.
 - b) Utrymmet ska inspekteras regelbundet, fysiskt eller tekniskt, eller bådadera, av säkerhetsmyndigheten vid den berörda EU-institutionen eller det berörda EU-organet. Sådana inspektioner ska också genomföras efter eventuellt obehörigt tillträde eller misstanke om sådant tillträde.
 - c) Utrymmet ska ha lämpligt akustiskt skydd och tempestskydd.
5. Alla personer som går in i tekniskt säkrade utrymmen ska uppfylla kraven i punkt 3.
6. Säkrade utrymmen och tekniskt säkrade utrymmen får tillfälligt inrättas inom ett administrativt utrymme för ett säkerhetsskyddsklassificerat möte eller liknande ändamål.
7. Skyddsvalv ska byggas inom det säkrade utrymmet. Ett skyddsvalv är ett rum med förstärkt fysisk konstruktion där säkerhetsmyndigheten vid den berörda EU-institutionen eller det berörda EU-organet godkänner väggar, golv, tak, fönster och låsbara dörrar. Sådana rum måste ge ett skydd som motsvarar ett säkerhetsskåp som godkänts för lagring av säkerhetsskyddsklassificerade EU-uppgifter med samma nivå av säkerhetsskyddsklassificering.

Fysiska skyddsåtgärder för hantering och lagring av säkerhetsskyddsklassificerade EU-uppgifter

8. Säkerhetsskyddsklassificerade EU-uppgifter med klassificeringen RESTREINT UE/EU RESTRICTED ska hanteras och lagras i något av följande utrymmen:
- a) I ett säkrat utrymme.
 - b) I ett administrativt utrymme, förutsatt att de säkerhetsskyddsklassificerade EU-uppgifterna skyddas från tillträde av obehöriga.
 - c) Utanför ett säkrat utrymme eller administrativt utrymme, förutsatt att innehavaren har åtagit sig att följa de kompensationsåtgärder som beslutats av säkerhetsmyndigheten för varje EU-institution och EU-organ.

9. Säkerhetsskyddsklassificerade EU-uppgifter med klassificeringen RESTREINT UE/EU RESTRICTED ska lagras i låsbara kontorsskåp i ett administrativt utrymme eller säkrat utrymme. De får tillfälligt lagras utanför ett administrativt utrymme eller säkrat utrymme, förutsatt att innehavaren har åtagit sig att lagra de berörda handlingarna i lämpliga låsta kontorsskåp när de inte läses eller diskuteras.
10. EU-institutioner och EU-organ får hantera och lagra uppgifter med klassificeringen RESTREINT UE/EU RESTRICTED utanför sina anläggningar, förutsatt att de relevanta uppgifterna skyddas på lämpligt sätt. För detta ändamål måste EU-institutioner och EU-organ följa de åtgärder som anges i punkt 8 c.
11. Uppgifter med klassificeringen CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET ska hanteras och lagras i något av följande utrymmen:
 - a) I ett säkrat utrymme.
 - b) I ett administrativt utrymme, förutsatt att de säkerhetsskyddsklassificerade EU-uppgifterna skyddas från tillträde av obehöriga.
 - c) Utanför ett säkrat utrymme eller administrativt utrymme där volymen och tiden är begränsad och förutsatt att innehavaren har åtagit sig att följa de kompensationsåtgärder som beslutats av säkerhetsmyndigheten vid den berörda EU-institutionen eller det berörda EU-organet. Dessutom ska innehavaren av säkerhetsskyddsklassificerade EU-uppgifter vidta följande åtgärder:
 - i) Underrätta den behöriga registreringsenheten om att säkerhetsskyddsklassificerade handlingar hanteras utanför skyddade utrymmen.
 - ii) Ständigt ha handlingen under sin kontroll.
12. Uppgifter med klassificeringen CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET ska lagras i ett säkrat utrymme som ackrediterats för den nivån av den behöriga ackrediteringsmyndigheten för säkerhet vid den berörda EU-institutionen eller det berörda EU-organet, antingen i ett säkerhetsskåp eller i ett skyddsvalv.
13. Handlingar med klassificeringen CONFIDENTIEL UE/EU CONFIDENTIAL eller högre får endast kopieras av relevant registreringsenhet.
14. Uppgifter med klassificeringen TRES SECRET UE/EU TOP SECRET ska hanteras och lagras i ett säkrat utrymme som är ackrediterat för den nivån. För detta ändamål får EU-institutioner och EU-organ ingå nödvändiga överenskommelser om att använda ett säkrat utrymme som förvaltas och ackrediteras på lämplig nivå av en annan EU-institutions eller ett annat EU-organs ackrediteringsmyndighet för säkerhet.
15. Uppgifter med klassificeringen TRES SECRET UE/EU TOP SECRET ska lagras i ett säkrat utrymme som ackrediterats för den nivån av ackrediteringsmyndigheten för säkerhet vid behörig berörd EU-institution eller berört EU-organ på något av följande villkor:
 - a) I ett säkerhetsskåp som godkänts av säkerhetsmyndigheten vid varje EU-institution och EU-organ med någon av följande kompletterande kontrollåtgärder:
 - i) Kontinuerligt skydd eller kontroll av godkänd säkerhetspersonal eller annan personal.

- ii) Ett godkänt intrångsupptäcktssystem i kombination med säkerhetspersonal redo att ingripa.
- b) Ett skyddsvalv utrustat med intrångsupptäcktssystem i kombination med säkerhetspersonal redo att ingripa.