DEN EUROPÆISKE REVISIONSRET

Revisionsrettens afgørelse nr. 041-2021 om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer (EUCI)

DEN EUROPÆISKE REVISIONSRET HAR -

UNDER HENVISNING TIL artikel 13 i traktaten om Den Europæiske Union,

UNDER HENVISNING TIL artikel 287 i traktaten om Den Europæiske Unions funktionsmåde,

UNDER HENVISNING TIL artikel 257 i Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046 af 18. juli 2018 om de finansielle regler vedrørende Unionens almindelige budget,

UNDER HENVISNING TIL artikel 1, stk. 6, i gennemførelsesbestemmelserne til Revisionsrettens forretningsorden (Revisionsrettens afgørelse nr. 21-2021),

UNDER HENVISNING TIL de andre EU-institutioners, -agenturers og -organers regler for sikkerhedsbeskyttelse af EU's klassificerede informationer,

UNDER HENVISNING TIL Revisionsrettens informationssikkerhedspolitik (DEC 127/15 FINAL) og politik for klassificering af oplysninger (personalemeddelelse nr. 123/2020), og

I BETRAGTNING AF at Revisionsretten i medfør af artikel 287, stk. 3, i TEUF har adgang til alle relevante dokumenter eller oplysninger, som den finder nødvendige for udøvelsen af sit mandat, herunder EU's klassificerede informationer (EUCI), og at den skal udøve sit mandat under fuld overholdelse af princippet om loyalt samarbejde mellem institutionerne og princippet om kompetencetildeling; den adgang til EUCI, som garanteres af TEUF, kan ikke drages i tvivl af udstederen af EUCI, men Revisionsretten kan blive anmodet om at indføre og overholde visse sikkerhedsforanstaltninger som nærmere beskrevet heri,

I BETRAGTNING AF at Revisionsrettens medlemmer samt dens tjenestemænd og øvrige ansatte selv efter at være udtrådt af tjenesten er underlagt tavshedspligt i henhold til artikel 339 i TEUF, artikel 17 i vedtægten og retsakter vedtaget i medfør heraf,

I BETRAGTNING AF at håndtering af EUCI på grund af deres følsomme art kræver, at overholdelse af fortrolighedsforpligtelsen sikres ved hjælp af passende sikkerhedsforanstaltninger, som kan garantere et højt beskyttelsesniveau for disse informationer, og som svarer til dem, der er fastsat i de regler for beskyttelse af EUCI, der er vedtaget af de andre EU-institutioner, -agenturer og -organer, idet det underforstås, at Revisionsretten, hvis den ikke finder sådanne sikkerhedsforanstaltninger berettigede i lyset af EUCI's art og type, forbeholder sig ret til at fremsætte de bemærkninger, som den anser for passende, idet den respekterer EUCI's klassifikationsgrad,

I BETRAGTNING AF at sikkerhedsforanstaltningerne til beskyttelse af fortroligheden, integriteten og tilgængeligheden af de informationer, der sendes til Revisionsretten, skal være passende for de pågældende informationers art og type,

I BETRAGTNING AF at Revisionsretten skal have adgang til klassificerede informationer efter "need-to-know"-princippet med henblik på udførelsen af de opgaver, den er pålagt ved traktaterne og ved retsakter vedtaget på grundlag af traktaterne,

I BETRAGTNING AF at det på grund af visse informationers art og følsomme indhold er passende at fastlægge en særlig procedure for Revisionsrettens håndtering af dokumenter, der indeholder EUCI, og

I BETRAGTNING AF at institutionen skal sikre, at denne afgørelse gennemføres i overensstemmelse med alle gældende regler, navnlig bestemmelserne om beskyttelse af personoplysninger, personers fysiske sikkerhed, bygninger og IT samt om aktindsigt -

VEDTAGET FØLGENDE AFGØRELSE:

Artikel 1. Genstand og anvendelsesområde

1) Denne afgørelse fastlægger grundprincipperne og minimumsstandarderne for sikkerhedsbeskyttelse af klassificerede informationer, som Revisionsretten håndterer i forbindelse med udøvelsen af sit mandat.

2) I denne afgørelse forstås ved klassificerede informationer en af eller alle de følgende typer informationer:

a) "EU's klassificerede informationer" (EUCI) som defineret i de andre EU-institutioners, -agenturers, -organers eller -kontorers sikkerhedsregler, forsynet med en af følgende EU-sikkerhedsklassifikationsmærkninger:

- TRÈS SECRET UE/EU TOP SECRET: informationer og materiale, hvis uautoriserede videregivelse kunne forvolde Den Europæiske Unions eller en eller flere af medlemsstaternes væsentlige interesser overordentlig alvorlig skade
- SECRET UE/EU SECRET: informationer og materiale, hvis uautoriserede videregivelse kunne forvolde Den Europæiske Unions eller en eller flere af medlemsstaternes væsentlige interesser alvorlig skade
- CONFIDENTIEL UE/EU CONFIDENTIAL: informationer og materiale, hvis uautoriserede videregivelse kunne forvolde Den Europæiske Unions eller en eller flere af medlemsstaternes væsentlige interesser skade
- RESTREINT UE/EU RESTRICTED: informationer og materiale, hvis uautoriserede videregivelse kunne have negativ indvirkning på Den Europæiske Unions eller en eller flere af medlemsstaternes interesser

b) klassificerede informationer, som videregives af medlemsstaterne, og som er forsynet med en national sikkerhedsklassifikationsmærkning svarende til en af de EUCI-sikkerhedsklassifikationsmærkninger[1], der er anført i litra a)

[1] Jf. aftalen af 4. maj 2011 mellem Den Europæiske Unions medlemsstater, forsamlet i Rådet, om beskyttelse af klassificerede informationer, der udveksles i Den Europæiske Unions interesse, og bilaget til denne aftale (EUT 2011/C 202/13).

c) klassificerede informationer, som videregives til Den Europæiske Revisionsret af tredjelande eller internationale organisationer, og som er forsynet med en sikkerhedsklassifikationsmærkning svarende til en af de EUCI-sikkerhedsklassifikationsmærkninger, der er anført i litra a), i overensstemmelse med de relevante aftaler eller administrative ordninger om informationssikkerhed.

3) Revisionsretten håndterer informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, i sine egne lokaliteter og træffer alle de nødvendige beskyttelsesforanstaltninger med henblik herpå. Der træffes foranstaltninger med henblik på at sikre, at ansatte i Revisionsretten, der har behov for adgang til EUCI på højere niveauer, kan få dette i egnede lokaliteter hos andre EU-institutioner, -organer eller -agenturer.

4) Denne afgørelse finder anvendelse på alle Revisionsrettens tjenester og lokaliteter.

5) Medmindre en bestemmelse vedrører specifikke personalegrupper, gælder denne afgørelse for medlemmerne af Revisionsretten, for de ansatte i Revisionsretten, der er omfattet af vedtægten for tjenestemænd og ansættelsesvilkårene for de øvrige ansatte i Den Europæiske Union[2], for udstationerede nationale eksperter i Revisionsretten, for tjenesteudbydere og deres personale, for praktikanter og for alle personer med adgang til Revisionsrettens bygninger og andre ejendomme eller til informationer, der forvaltes af Revisionsretten.

6) Medmindre andet er angivet, finder bestemmelserne om EUCI tilsvarende anvendelse på de klassificerede informationer, der er omhandlet i denne artikels stk. 2, litra b) og c).

Artikel 2. **Definitioner**

I denne afgørelse forstås ved:

a) "autorisation til at få adgang til EUCI": en afgørelse truffet af Revisionsrettens direktør for menneskelige ressourcer, finanser og generelle tjenester på grundlag af en sikkerhedskonklusion fra en kompetent myndighed i en medlemsstat om, at en tjenestemand, en anden ansat eller en udstationeret national ekspert i Revisionsretten, såfremt den pågældendes need-to-know er fastslået, og vedkommende er blevet behørigt orienteret om sit ansvar, kan autoriseres til at få adgang til EUCI op til en bestemt klassifikationsgrad (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere) indtil en bestemt dato; den pågældende person betegnes som "sikkerhedsautoriseret"

b) "klassificering": tildeling af en klassifikationsgrad til informationer baseret på den grad af skade, som deres uautoriserede videregivelse kunne forvolde

c) "kryptografisk materiale": algoritmer, kryptografiske hardware- og softwaremoduler samt produkter, der omfatter implementeringsdetaljer og tilhørende dokumentation, og nøglingsmateriale

d) "afklassificering": fjernelse af enhver sikkerhedsklassifikation

e) "dokument": registrerede informationer uanset deres form eller fysiske karakteristika

f) "nedklassificering": nedsættelse til en lavere klassifikationsgrad

g) "facilitetssikkerhedsgodkendelse": en administrativ afgørelse truffet af en kompetent myndighed om, at en facilitet ud fra et sikkerhedsmæssigt synspunkt kan yde tilstrækkelig beskyttelse af EUCI til en bestemt klassifikationsgrad

[2] Forordning nr. 31 (EØF) om vedtægten for tjenestemænd og om ansættelsesvilkårene for de øvrige ansatte, som ændret, EFT 01962R0031-1.1.2020-019.003-1 (https://eur-lex.europa.eu/eli/reg/1962/31 (1)/2020-01-01).

h) "håndtering" af EUCI: alle de foranstaltninger, som EUCI kan underkastes i hele deres livscyklus: udarbejdelse, registrering, behandling, transport, nedklassificering, afklassificering og destruktion. I forbindelse med kommunikations- og informationssystemer (CIS) omfatter det også indsamling, visning, transmission og opbevaring

i) "den, der er i besiddelse af": en behørigt autoriseret person med en fastslået need-to-know, der er i besiddelse af klassificerede informationer og derfor er ansvarlig for at beskytte dem

j) "informationssikkerhedsmyndighed": Revisionsrettens informationssikkerhedsansvarlige, som helt eller delvis kan uddelegere de opgaver, der er omhandlet i denne afgørelse

k) "informationer": alle skriftlige eller mundtlige informationer, uanset medium eller ophavsmand

l) "materiale": ethvert medium, enhver databærer, enhver maskine eller ethvert udstyr

m) "udsteder": en EU-institution eller et EU-organ eller -agentur, en medlemsstat, et tredjeland eller en international organisation, under hvis myndighed informationer er blevet udarbejdet og/eller bragt ind i EU's strukturer

n) "personelsikkerhedsgodkendelse" (PSC): en erklæring fra en medlemsstats kompetente myndighed på baggrund af en sikkerhedsundersøgelse udført af en medlemsstats kompetente myndigheder, hvorved det attesteres, at en person, forudsat at vedkommendes need-to-know er fastslået, og at vedkommende er blevet behørigt orienteret om sit ansvar, kan få adgang til EUCI op til en bestemt klassifikationsgrad (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere) indtil en bestemt dato

o) "certifikat for personelsikkerhedsgodkendelse" (PSCC): et certifikat udstedt af Revisionsrettens direktør for menneskelige ressourcer, finanser og generelle tjenester, som fastslår, at en person har en gyldig sikkerhedsgodkendelse eller sikkerhedsautorisation, og som viser den klassifikationsgrad for EUCI, som personen kan få adgang til (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere), den pågældende sikkerhedsgodkendelses eller sikkerhedsautorisations gyldighedsperiode og certifikatets udløbsdato

p) "myndigheden med ansvar for fysisk sikkerhed": Revisionsrettens sikkerhedschef, som er ansvarlig for gennemførelsen af de nødvendige foranstaltninger og procedurer vedrørende fysisk sikkerhed for at beskytte EUCI

q) "registerkontoret": et kontor, der administreres af Revisionsrettens Sekretariat og er placeret i et administrativt område, som hører under Revisionsrettens direktør for menneskelige ressourcer, finanser og generelle tjenester. Det er ansvarligt for ind- og udgående udveksling af informationer, der er klassificeret RESTREINT UE/EU RESTRICTED eller tilsvarende, med Revisionsretten

r) "EUCI-arkivet": et arkiv oprettet i et sikret område. Dette arkiv forvaltes af Revisionsrettens sikkerhedsgodkendte og autoriserede arkivansvarlige. Det er ansvarligt for ind- og udgående udveksling af informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, med Revisionsretten

s) "sikkerhedsakkrediteringsmyndighed": Revisionsrettens direktør for menneskelige ressourcer, finanser og generelle tjenester.

Artikel 3. **Foranstaltninger til beskyttelse af EUCI**

1) Revisionsretten sikrer, at alle klassificerede informationer, der videregives til den, beskyttes på en måde, der svarer til den klassifikationsgrad, som udstederen har fastsat, og i overensstemmelse med denne afgørelse.

2) Med henblik herpå underlægger Revisionsretten behandlingen af EUCI fysiske sikkerhedsforanstaltninger og, hvor det er relevant, personelsikkerhedsforanstaltninger, herunder tildeling af adgangsautorisationer til de identificerede personer, og foranstaltninger til beskyttelse af kommunikations- og informationssystemer. Disse foranstaltninger er beskrevet i artikel 4-6 og finder anvendelse i hele EUCI's livscyklus. De skal svare til EUCI's sikkerhedsklassifikation, formen og mængden af informationer eller materiale, placeringen og konstruktionen af de faciliteter, hvor EUCI opbevares, og den lokalt vurderede trussel fra ondsindet og/eller kriminel virksomhed, herunder spionage, sabotage og terrorisme.

3) EUCI beskyttes ved hjælp af fysiske sikkerhedsforanstaltninger, og informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, beskyttes desuden ved hjælp af personelsikkerhedsforanstaltninger.

4) EUCI må kun videregives til personer i institutionen med need-to-know. Den, der er i besiddelse af EUCI, skal beskytte dem som fastsat i denne afgørelse.

5) EUCI må ikke videregives, hverken mundtligt eller skriftligt. Revisionsrettens foreløbige bemærkninger, beretninger, udtalelser, pressemeddelelser og andre produkter, dens websted og intranet, mundtlige indlæg, svar på anmodninger om aktindsigt[3] og tale- eller videooptagelser må ikke indeholde eller henvise til EUCI eller uddrag heraf. Hvis udstederen har offentliggjort dokumenter eller informationer, der indeholder en henvisning til EUCI, kan denne henvisning dog nævnes.

6) Uanset stk. 5 kan Revisionsretten og udstederen aftale, at Revisionsretten i tilfælde af en specifik revision kan gengive eller anvende elementer af EUCI i et dokument. I så fald stiles dette dokument fra Revisionsretten i første omgang til udstederen af de pågældende EUCI før eller under den kontradiktoriske procedure. I denne situation aftaler Revisionsretten og ophavsmanden, om det dokument, der er udstedt af Revisionsretten, skal klassificeres. Hvis et ordførende medlem af Revisionsretten finder det nødvendigt at sende en helt eller delvis klassificeret revisionsberetning til bestemte adressater i Europa-Parlamentet eller Rådet - under hensyntagen til alle de sikkerhedsforanstaltninger, der er knyttet til denne afgørelse - kræver dette samtykke fra udstederen af de klassificerede informationer. De retlige rammer og proceduren for udveksling af sådanne dokumenter er fastlagt i artikel 7.

7) Når Revisionsrettens udøvelse af sit mandat kræver bredere udveksling af visse elementer i et klassificeret dokument eller klassificerede informationer, skal den under behørig hensyntagen til sikkerhedsklassifikationsmærkningen høre udstederen, før den beslutter at anvende disse elementer eller informationer, hvis den finder, at der er en tungtvejende offentlig interesse i at gøre dette. Informationerne må kun anvendes i beretningen på en sådan måde, at udstederens interesser ikke kan skades. Dette kan sikres på en passende måde ved at anmode udstederen om at fremsætte bemærkninger med henblik på at nå til enighed om, hvordan informationerne kan anonymiseres, kondenseres, generaliseres osv. med respekt for de parters interesser, der primært er berørt af de offentliggjorte oplysninger.

---

[3] Jf. Revisionsrettens afgørelse nr. 12/2005 om aktindsigt i Revisionsrettens dokumenter, som ændret ved Revisionsrettens afgørelse nr. 14/2009 (EUT 2009/C 67/1).

8) Revisionsretten videregiver ikke EUCI til andre EU-institutioner, -agenturer, -organer eller -kontorer, en medlemsstat, et tredjeland eller en international organisation uden forudgående høring af udstederen og dennes udtrykkelige skriftlige samtykke.

9) Medmindre udstederen af et dokument, der er klassificeret SECRET UE/EU SECRET eller lavere, har fastlagt begrænsninger med hensyn til kopiering eller oversættelse, kan den, der er i besiddelse af et sådant dokument, få det kopieret eller oversat i overensstemmelse med de praktiske arbejdsinstruktioner fra Revisionsrettens informationssikkerhedsmyndighed. De sikkerhedsforanstaltninger, der gælder for det oprindelige dokument, gælder også for kopier og oversættelser af det.

10) Hvis Revisionsretten har brug for nedklassificering eller afklassificering af et klassificeret dokument, som den har modtaget eller har adgang til, skal den høre udstederen og spørge, om denne kan videregive en nedklassificeret eller afklassificeret udgave af dokumentet.

Artikel 4. **Personelsikkerhed**

1) I kraft af deres funktioner er Revisionsrettens medlemmer autoriseret til at få adgang til alle EUCI og til at deltage i møder, hvor EUCI håndteres. Medlemmerne oplyses om deres sikkerhedsforpligtelser med hensyn til beskyttelse af EUCI og anerkender skriftligt deres ansvar med hensyn til beskyttelse af sådanne informationer.

2) En ansat i Revisionsretten, det være sig en tjenestemand, en ansat omfattet af ansættelsesvilkårene for de øvrige ansatte eller en udstationeret national ekspert, kan kun få adgang til EUCI, efter at:

   i. vedkommendes need-to-know er fastslået

   ii. vedkommende er blevet oplyst om regler og procedurer for sikkerhedsbeskyttelse af EUCI og de relevante sikkerhedsstandarder og sikkerhedsretningslinjer og skriftligt har anerkendt sit ansvar med hensyn til beskyttelse af sådan informationer, og

   iii. vedkommende i forbindelse med informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, er blevet sikkerhedsgodkendt og autoriseret til at få adgang.

3) Proceduren for fastlæggelse af, om en tjenestemand eller en anden ansat i Revisionsretten kan autoriseres til at få adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, under hensyntagen til vedkommendes loyalitet, integritet og pålidelighed og efter indhentning af en sikkerhedskonklusion fra en kompetent myndighed i en medlemsstat som omhandlet i artikel 2, litra n), fastlægges i en delegeret afgørelse, der træffes i overensstemmelse med artikel 10, stk. 10. Afgørelser om tildeling af adgangsautorisation træffes af Revisionsrettens direktør for menneskelige ressourcer, finanser og generelle tjenester.

4) Revisionsrettens direktør for menneskelige ressourcer, finanser og generelle tjenester kan udstede et PSCC med angivelse af den klassifikationsgrad for EUCI, som personen kan få adgang til (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere), den pågældende adgangsautorisations gyldighedsperiode og PSCC'ets udløbsdato.

5) Kun personer med den i stk. 2, nr. iii), omhandlede autorisation og medlemmer af Revisionsretten, jf. stk. 1, kan deltage i møder, hvor informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, håndteres. Revisionsretten og udstederen træffer de praktiske foranstaltninger i forbindelse med sådanne møder fra sag til sag.

6) De tjenester i Revisionsretten, der har ansvar for at afholde møder, hvor informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, skal behandles, underretter i god tid informationssikkerhedsmyndigheden om mødedatoer, mødetidspunkter og mødesteder samt fremsender deltagerlister.

7) Enhver, der er i besiddelse af EUCI uden behørig autorisation og/eller uden dokumenteret need-to-know, skal rapportere situationen til informationssikkerhedsmyndigheden så hurtigt som muligt og sikre, at EUCI beskyttes som fastsat i denne afgørelse.

Artikel 5. **Fysiske sikkerhedsforanstaltninger til beskyttelse af klassificerede informationer**

1) Ved "fysisk sikkerhed" forstås anvendelse af fysiske og tekniske beskyttelsesforanstaltninger for at forhindre uautoriseret adgang til EUCI.

2) De fysiske sikkerhedsforanstaltninger udformes med henblik på at forhindre, at en indtrænger skaffer sig hemmelig adgang eller tiltvinger sig adgang, at afværge, vanskeliggøre og afsløre uautoriserede handlinger samt at muliggøre personalemæssig adskillelse for så vidt angår adgang til EUCI på en need-to-know-basis. Disse foranstaltninger fastlægges på grundlag af en risikostyringsproces i overensstemmelse med denne afgørelse.

3) Områder, hvor EUCI håndteres eller opbevares, underkastes regelmæssig inspektion af Revisionsrettens sikkerhedsmyndighed.

4) Kun udstyr eller anordninger, der lever op til de gældende regler for beskyttelse af EUCI i EU-institutionerne, -agenturerne eller -organerne, må anvendes til at håndtere og opbevare EUCI.

5) Ansatte i Revisionsretten kan få adgang til EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, eller tilsvarende, i sikrede områder uden for Revisionsrettens lokaliteter.

6) Revisionsretten kan indgå en serviceleveranceaftale med en anden EU-institution i Luxembourg med henblik på at kunne håndtere og opbevare informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, i et sikret område i den pågældende institution. Medmindre udstederen udtrykkeligt har givet sit samtykke hertil, må disse EUCI ikke håndteres eller opbevares i Revisionsrettens lokaliteter og ikke kopieres eller oversættes af Revisionsretten.

7) Informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, registreres af Revisionsretten. Søgning i informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, eller tilsvarende, uden for Revisionsrettens lokaliteter, sikkerhedsregistreres.

8) EUCI, der er klassificeret RESTREINT UE/EU RESTRICTED, kan opbevares i passende aflåste kontormøbler i et administrativt område eller et sikret område. EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, opbevares i henhold til en serviceleveranceaftale i en sikkerhedscontainer i et sikret område tilhørende en anden EU-institution i Luxembourg.

9) Uden for arkivet transporteres EUCI på følgende måde mellem tjenester og lokaliteter:

   a) Generelt transporteres EUCI ved elektronisk transmission beskyttet af kryptoprodukter, der er godkendt i overensstemmelse med artikel 6, stk. 8.

   b) Hvis EUCI ikke overføres som beskrevet i litra a), overføres de ved hjælp af en databærer (f.eks. en USB-hukommelsesnøgle, en CD, en harddisk) beskyttet af kryptoprodukter, der

er godkendt i overensstemmelse med artikel 6, stk. 8, eller som papirkopi i en ugennemsigtig forseglet kuvert.

10) Informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, kan destrueres af den, der er i besiddelse af dem, under overholdelse af de arkiveringsregler, der gælder i Revisionsretten. Informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, må kun destrueres af den arkivansvarlige på anmodning fra den, der er i besiddelse af dem, eller fra en kompetent myndighed i overensstemmelse med de arkiveringsregler, der gælder i Revisionsretten. Dokumenter, der er klassificeret SECRET UE/EU SECRET, destrueres i overværelse af et vidne, der er sikkerhedsgodkendt til mindst samme klassifikationsgrad som de dokumenter, der skal destrueres. Den arkivansvarlige og vidnet, hvis et vidnes tilstedeværelse er påkrævet, underskriver en destruktionsattest, der opbevares i arkivet. Den arkivansvarlige opbevarer i mindst fem år optegnelser over destruktion af dokumenter, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET.

11) Myndigheden med ansvar for fysisk sikkerhed og informationssikkerhedsmyndigheden udarbejder under hensyntagen til lokale forhold en fælles plan for sikker opbevaring af EUCI i krisesituationer, herunder om nødvendigt planer for nøddestruktion eller nødflytning. De udsteder sådanne instruktioner, som de finder hensigtsmæssige, for at forhindre, at EUCI falder i hænderne på uautoriserede personer.

12) Hvis det er nødvendigt at transportere EUCI fysisk, overholder Revisionsretten de foranstaltninger, som udstederen har foreskrevet med henblik på at beskytte dem mod uautoriseret videregivelse under transporten.

13) De fysiske sikkerhedsforanstaltninger, der finder anvendelse i administrative områder, hvor informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, håndteres og opbevares, er fastsat i bilaget.

Artikel 6. Beskyttelse af EUCI i kommunikations- og informationssystemer

1) I denne artikel forstås ved "kommunikations- og informationssystem" et system, der muliggør håndtering af EUCI i elektronisk form. Et kommunikations- og informationssystem omfatter alle aktiver, der er nødvendige for dets drift, herunder infrastruktur, organisation, personale og informationsressourcer.

2) Ved "legitim bruger" forstås et medlem af Revisionsretten eller en tjenestemand, en anden ansat eller en udstationeret national ekspert i Revisionsretten med et fastslået og anerkendt behov for adgang til et specifikt informationssystem.

3) Revisionsretten giver sikkerhed for, at dens systemer i passende omfang beskytter de informationer, de håndterer, og at de fungerer, som de skal, når de skal, under de legitime brugeres kontrol. Med henblik herpå sikrer de et passende niveau af:

- autenticitet: sikkerhed for, at informationer er ægte og fra bona fide-kilder
- tilgængelighed: det forhold, at informationerne er tilgængelige og kan anvendes på anmodning fra en autoriseret enhed
- fortrolighed: det forhold, at informationerne ikke videregives til uautoriserede personer, enheder eller processer
- integritet: sikkerhed for, at informationerne og aktiverne er korrekte og fuldstændige
- uafviselighed: det forhold, at det kan bevises, at en handling eller begivenhed har fundet sted, så denne handling eller begivenhed ikke senere kan benægtes.

Denne sikkerhed baseres på en risikostyringsproces. Ved "risiko" forstås muligheden for, at en given trussel vil udnytte indre og ydre sårbarheder i en organisation eller i nogen af de systemer, den benytter, og derved skade organisationen og dens materielle eller immaterielle aktiver. Den måles som en kombination af sandsynligheden for, at trusler indtræffer, og deres virkning. Risikostyringsprocessen består af følgende skridt: identifikation af trusler og sårbarhed, risikovurdering, risikobehandling, risikoaccept og risikokommunikation.

- "Risikovurdering" er identifikation af trusler og sårbarheder og udførelse af den dertil knyttede risikoanalyse, dvs. vurdering af sandsynlighed og virkning.
- "Risikobehandling" er afbødning, fjernelse, reduktion (gennem en passende kombination af tekniske, fysiske, organisatoriske eller proceduremæssige foranstaltninger), flytning eller overvågning af risikoen.
- "Risikoaccept" er beslutningen om at acceptere, at der fortsat findes en residualrisiko efter risikobehandlingen.
- "Residualrisiko" er den risiko, der fortsat eksisterer, efter at der er gennemført sikkerhedsforanstaltninger, idet ikke alle trusler kan imødegås, og ikke alle sårbarheder kan fjernes.
- "Risikokommunikation" er fremme af bevidstheden om risici blandt brugere af kommunikations- og informationssystemer, underretning af godkendelsesmyndigheder om sådanne risici og indberetning af dem til driftsmyndigheder.

4) Alt elektronisk udstyr og alle elektroniske anordninger, der anvendes til at håndtere EUCI, skal leve op til de gældende regler for beskyttelse af EUCI. Der gives fortrinsret til elektroniske anordninger og elektronisk udstyr, der allerede er akkrediteret af en anden EU-institution, et andet EU-agentur eller et andet EU-organ. Anordningerne skal være garanteret sikre i hele deres livscyklus.

5) Revisionsrettens kommunikations- og informationssystem til håndtering af EUCI akkrediteres af en kompetent myndighed. Med henblik herpå søger Revisionsretten at indgå en serviceleveranceaftale med en sikkerhedsakkrediteringsmyndighed i en EU-institution, som har beføjelser til at akkreditere CIS, der håndterer EUCI, for at få en akkrediteringsudredning med angivelse af, at informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, kan håndteres i Revisionsrettens CIS, og med fastsættelse af de betingelser og vilkår, der svarer hertil. Serviceleveranceaftalen henviser også til de standarder, der skal anvendes i forbindelse med akkrediteringsprocessen, og aftalen indgås efter proceduren i artikel 10, stk. 3.

6) Hvis Revisionsretten skal fastlægge sin egen for akkrediteringsproces for sit CIS, skal en delegeret afgørelse som omhandlet i denne afgørelses artikel 10, stk. 10, fastlægge processen i overensstemmelse med standarderne for akkrediteringsprocessen for CIS, der håndterer EUCI i andre EU-institutioner, -agenturer og -organer.

7) Ansvaret for at forberede akkrediteringssager og -dokumentation i overensstemmelse med de gældende standarder, påhviler udelukkende CIS-systemejeren.

8) Hvis EUCI er beskyttet af kryptoprodukter, giver Revisionsretten fortrinsret til produkter, der er godkendt af Rådet eller af generalsekretæren for Rådet som kryptogodkendelsesmyndighed, eller til produkter, der af andre EU-institutioner, -agenturer og -organer er godkendt til beskyttelse af EUCI.

9) Informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, må kun behandles på elektroniske anordninger (såsom arbejdsstationer, printere og fotokopieringsmaskiner), der befinder sig i et administrativt område eller et sikret område. Elektroniske anordninger, som håndterer informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, adskilles fra andre computernetværk og beskyttes ved hjælp af passende fysiske eller tekniske foranstaltninger.

10) Alt personale i Revisionsretten, der er involveret i udformningen, udviklingen, testningen, driften, forvaltningen eller brugen af CIS, som håndterer EUCI, skal meddele informationssikkerhedsmyndigheden alle potentielle sikkerhedssvagheder, hændelser og sikkerhedsbrud eller -kompromittering, som kan have indflydelse på beskyttelsen af CIS og/eller de EUCI, det indeholder.

Artikel 7. **Procedure for udveksling af og adgang til klassificerede informationer**

1) Når EU-institutionerne, -agenturerne, -organerne og -kontorerne og de nationale myndigheder er retligt forpligtet hertil i medfør af traktaterne eller retsakter vedtaget på grundlag af traktaterne, giver de på eget initiativ eller på skriftlig anmodning fra formanden, fra det eller de ordførende medlemmer eller fra generalsekretæren Revisionsretten adgang til EUCI efter nedenstående procedure.

2) Anmodninger om adgang sendes til de berørte institutioner via Revisionsrettens registerkontor.

3) Hvis det er nødvendigt, indgår Revisionsretten en administrativ ordning vedrørende de praktiske aspekter ved udveksling af EUCI eller tilsvarende informationer.

4) Med henblik på indgåelsen af sådanne administrative ordninger giver Revisionsretten udstederen alle nødvendige oplysninger om sit informationssikkerhedssystem. Om nødvendigt kan der arrangeres et vurderingsbesøg.

5) Sådanne administrative ordninger indgås under fuld overholdelse af principperne om kompetencetildeling og loyalt samarbejde i artikel 13 i traktaten om Den Europæiske Union. De indgås efter proceduren i artikel 10, stk. 4.

6) Hvis der med en given EU-institution, et givet EU-organ eller -agentur, et givet tredjeland eller en given international organisation ikke er indgået en administrativ ordning om videregivelse af klassificerede informationer til Revisionsretten, undertegner Revisionsretten en erklæring om, at den forpligter sig til at beskytte de klassificerede informationer, den modtager.

Artikel 8. **Brud på sikkerheden og bortkomst eller kompromittering af klassificerede informationer**

1) Ved brud på sikkerheden forstås en persons handling eller forsømmelse, der er i strid med sikkerhedsreglerne i denne afgørelse og dens gennemførelsesbestemmelser.

2) EUCI anses for at være kompromitteret, hvis de som følge af et brud på sikkerheden helt eller delvist er videregivet til uautoriserede personer.

3) Ethvert brud på og enhver mistanke om brud på sikkerheden skal straks meldes til Revisionsrettens informationssikkerhedsmyndighed.

4) Hvis det konstateres, eller hvis der er rimelig grund til at formode, at EUCI er kompromitteret eller bortkommet, underretter informationssikkerhedsmyndigheden Revisionsrettens direktør for menneskelige ressourcer, finanser og generelle tjenester og Revisionsrettens generalsekretær. Revisionsrettens direktør for menneskelige ressourcer, finanser og generelle tjenester underretter straks udstederens sikkerhedsmyndighed. Ovennævnte direktør i Revisionsretten foretager en undersøgelse og underretter Revisionsrettens generalsekretær og udstederens sikkerhedsmyndighed om resultaterne og om de foranstaltninger, der er truffet for at forhindre, at situationen opstår igen. Hvis et medlem af Revisionsretten er

involveret, er Revisionsrettens formand ansvarlig for at træffe foranstaltninger i samarbejde med Revisionsrettens generalsekretær.

5) Enhver tjenestemand eller anden ansat ved Revisionsretten, der er ansvarlig for brud på de sikkerhedsregler, der er fastsat i denne afgørelse og dens gennemførelsesbestemmelser, kan pålægges de sanktioner, der er fastsat i vedtægten for tjenestemænd og ansættelsesvilkårene for de øvrige ansatte i Den Europæiske Union.

6) Ethvert medlem af Revisionsretten, der ikke overholder bestemmelserne i denne afgørelse, kan blive genstand for de foranstaltninger og sanktioner, der er fastsat i traktatens artikel 286, stk. 6.

7) Enhver, der er ansvarlig for bortkomst eller kompromittering af EUCI, kan pålægges disciplinære foranstaltninger og/eller retsforfølges i overensstemmelse med de gældende love, regler og bestemmelser.

Artikel 9. **Sikkerhed i tilfælde af intervention udefra**

1) Revisionsretten kan i medfør af kontrakter overdrage opgaver, der indebærer eller medfører adgang til EUCI, til kontrahenter, som er registreret i en medlemsstat. Dette kan navnlig ske i forbindelse med vedligeholdelse af kommunikations- og informationssystemer og computernetværket.

2) I tilfælde af intervention udefra træffer Revisionsretten alle nødvendige sikkerhedsforanstaltninger som omhandlet i denne artikels stk. 3 og anmoder herunder om en facilitetssikkerhedsgodkendelse for at sikre, at EUCI beskyttes af kandidater og tilbudsgivere i hele udbuds- og kontraktindgåelsesproceduren og af kontrahenter og underkontrahenter i hele kontraktens løbetid. Den kontraherende myndighed sikrer, at de minimumssikkerhedsstandarder, der er fastsat i denne afgørelse, angives i kontrakter, så kontrahenterne forpligtes til at overholde dem.

3) Sikkerhedsregler, udbudsprocedurer, skabeloner til og modeller for kontrakter og underkontrakter, der indebærer adgang til EUCI, udbudsbekendtgørelser, vejledning om forhold, der forudsætter facilitetssikkerhedsgodkendelser og personalesikkerhedsgodkendelser, program- eller projektsikkerhedsinstruktioner, særlige sikkerhedsbetingelser, besøg og transmission og transport af EUCI, som er omfattet af sådanne kontrakter og underkontrakter, skal være i overensstemmelse med de regler, skabeloner og modeller, som Europa-Kommissionen har fastsat for klassificerede kontrakter i afgørelse (EU, Euratom) 2015/444 af 13. marts 2015 om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer.

Artikel 10. **Gennemførelse af afgørelsen og ansvar i forbindelse hermed**

1) Revisionsrettens tjenester træffer alle fornødne foranstaltninger, der henhører under deres ansvarsområde, til at sikre, at de anvender denne afgørelse og de relevante gennemførelsesbestemmelser i forbindelse med håndtering eller opbevaring af EUCI eller andre klassificerede informationer.

2) Generalsekretæren er ansættelsesmyndighed og myndighed med beføjelse til at indgå ansættelseskontrakter vedrørende alle tjenestemænd og andre ansatte. Generalsekretæren kan overdrage direktøren for menneskelige ressourcer, finanser og generelle tjenester ansvaret for at give tjenestemænd og andre ansatte autorisation til at få adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, for at

fungere som sikkerhedsakkrediteringsmyndighed og for at føre tilsyn med Revisionsrettens Sekretariat hvad angår håndtering af EUCI.

3) Generalsekretæren har kompetence til at indgå serviceleveranceaftaler om akkreditering af Revisionsrettens kommunikations- og informationsudstyr og -systemer, om anvendelse af et sikret område i en anden EU-institution og om proceduren vedrørende anmodninger om personnelsikkerhedsgodkendelser i forbindelse med adgang til EUCI.

4) Direktøren for menneskelige ressourcer, finanser og generelle tjenester har kompetence til at indgå administrative ordninger med EU's institutioner, agenturer og andre organer om udveksling af de EUCI, som Revisionsretten skal bruge for at udøve sit mandat. Direktøren kan også indgå administrative ordninger med tredjelande eller internationale organisationer om beskyttelse af de klassificerede informationer, der modtages.

5) Direktøren for menneskelige ressourcer, finanser og generelle tjenester har kompetence til at underskrive enhver erklæring om beskyttelse af EUCI, der skal afgives i forbindelse med en ekstraordinær ad hoc-videregivelse.

6) Revisionsrettens informationssikkerhedsansvarlige fungerer som informationssikkerhedsmyndighed. Den informationssikkerhedsansvarlige og de personer, som vedkommende uddelegerer alle eller en del af sine opgaver til, skal have en relevant sikkerhedsgodkendelse. Informationssikkerhedsmyndigheden varetager sit ansvar i tæt samarbejde med Direktoratet for Menneskelige Ressourcer, Finanser og Generelle Tjenester, Direktoratet for Information, Arbejdsplads og Innovation og Direktoratet under Udvalget for Kvalitetskontrol af Revisionen (jf. navnlig artikel 4, 6 og 8). Informationssikkerhedsmyndigheden er også ansvarlig for uddannelse og oplysningsmøder om informationssikkerhed samt for at foretage periodiske inspektioner for at kontrollere overholdelsen af denne afgørelse, herunder i tilfælde af intervention udefra, og for at træffe foranstaltninger med henblik på at sikre overholdelse.

7) Sikkerhedschefen er ansvarlig for fysiske sikkerhedsforanstaltninger (jf. navnlig artikel 5).

8) Et registerkontor oprettet i Revisionsrettens Sekretariat er kanal for ind- og udgående udveksling af informationer, som er klassificeret RESTREINT UE/EU RESTRICTED, og som Revisionsretten kan udveksle med andre EU-institutioner, -agenturer og -organer samt medlemsstater. Det er også kanal for ind- og udgående udveksling af tilsvarende informationer fra tredjelande og internationale organisationer. Registerkontoret organiseres som fastsat i en delegeret afgørelse. Den ansvarlige for registerkontoret varetager følgende hovedopgaver:

   a) registrering af ind- og udgående udveksling af informationer, der er klassificeret RESTREINT UE/EU RESTRICTED

   b) forvaltning af særlige administrative områder med henblik på registrering af håndtering og opbevaring af samt søgning i EUCI, der er klassificeret RESTREINT UE/EU RESTRICTED.

9) Et arkiv oprettes under en serviceleveranceaftale om anvendelse af en anden EU-institutions sikrede område. Dette arkiv, som organiseres af Revisionsrettens Sekretariat under ansvar af Revisionsrettens direktør for menneskelige ressourcer, finanser og generelle tjenester, er kanal for ind- og udgående udveksling af informationer, som er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, og som Revisionsretten kan udveksle med andre EU-institutioner, -agenturer og -organer samt medlemsstater. Det er også kanal for ind- og udgående udveksling af tilsvarende informationer fra tredjelande og internationale organisationer. Det udstyres med passende bokse og andet sikkerhedsudstyr, som er egnet til at beskytte informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere. Arkivet organiseres som fastsat i en delegeret afgørelse. Den arkivansvarlige skal have en relevant sikkerhedsgodkendelse og varetager følgende hovedopgaver:

a) forvaltning af operationer i forbindelse med registrering af og søgning i samt bevarelse, reproduktion, oversættelse, transmission, afsendelse og, hvor det er relevant, destruktion af EUCI

b) andre opgaver med tilknytning til beskyttelsen af EUCI som fastlagt i en delegeret afgørelse.

10) Administrationsudvalget vedtager en delegeret afgørelse om gennemførelsesbestemmelser til denne afgørelse. Den informationssikkerhedsansvarlige udarbejder retningslinjer for informationssikkerhed. Udvalget for Kvalitetskontrol af Revisionen udarbejder revisionsretningslinjer.

Artikel 11. **Ikrafttræden**

Denne afgørelse træder i kraft dagen efter offentliggørelsen i Den Europæiske Unions Tidende.

Udfærdiget i Luxembourg, den 3. juni 2021.

På Revisionsrettens vegne

Klaus-Heiner Lehne
Formand

Bilag: FYSISKE SIKKERHEDSFORANSTALTNINGER VEDRØRENDE ADMINISTRATIVE OMRÅDER FOR EUCI

BILAG

FYSISKE SIKKERHEDSFORANSTALTNINGER VEDRØRENDE ADMINISTRATIVE OMRÅDER FOR EUCI

1) Dette bilag indeholder regler for gennemførelse af afgørelsens artikel 5. Der er tale om minimumsregler for fysisk beskyttelse af administrative områder for informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, i Revisionsretten: områder, som er udpeget til registrering og opbevaring af samt søgning i informationer, der er klassificeret RESTREINT UE/EU RESTRICTED.

2) Formålet med de fysiske sikkerhedsforanstaltninger i administrative områder er at forhindre uautoriseret adgang til disse områder på følgende måde:

   a) Der skal etableres en synligt afgrænset perimeter, der muliggør kontrol af personer.

   b) Uledsaget adgang tillades kun for personer, der er behørigt autoriseret af Revisionsrettens informationssikkerhedsmyndighed eller af en anden kompetent myndighed.

   c) Alle andre personer skal til stadighed ledsages eller underkastes tilsvarende kontrol.

3) Revisionsrettens informationssikkerhedsmyndighed kan undtagelsesvis give uautoriserede personer adgang, herunder til at arbejde i et administrativt område, forudsat at dette ikke indebærer adgang til EUCI - som skal forblive låst væk. Sådanne personer må kun komme ind, hvis de ledsages og holdes under konstant opsyn af informationssikkerhedsmyndigheden eller den arkivansvarlige.

4) Informationssikkerhedsmyndigheden fastlægger procedurer for forvaltning af nøgler og/eller koder til alle administrative områder og sikrede møbler. Procedurerne skal beskytte mod uautoriseret adgang.

5) Koder skal læres udenad af færrest mulige personer, der har behov for at kende dem. Koder til sikrede møbler, som anvendes til opbevaring af informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, skal ændres:

   - når der modtages et nyt sikret møbel
   - når der sker en ændring i det personale, der kender koden
   - hvis der er konstateret en kompromittering af koden, eller der er mistanke herom
   - hvis der er foretaget vedligeholdelse eller reparation af en lås
   - mindst hver 12. måned.

6) Informationssikkerhedsmyndigheden og sikkerhedschefen er ansvarlig for overholdelsen af disse regler.