EUROPEISKA REVISIONSRÄTTEN

Revisionsrättens beslut nr 041-2021 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter

EUROPEISKA REVISIONSRÄTTEN HAR FATTAT DETTA BESLUT

med beaktande av artikel 13 i fördraget om Europeiska unionen,

med beaktande av artikel 287 i fördraget om Europeiska unionens funktionssätt,

med beaktande av artikel 257 i Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046 av den 18 juli 2018 om finansiella regler för unionens allmänna budget,

med beaktande av artikel 1.6 i tillämpningsföreskrifterna för revisionsrättens arbetsordning (revisionsrättens beslut nr 21–2021),

med beaktande av övriga EU-institutioners, EU-byråers och EU-organs säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter,

med beaktande av revisionsrättens informationssäkerhetspolicy (DEC 127/15 FINAL) och policy för informationsklassificering (Staff Notice 123/2020), och

av följande skäl:

Enligt artikel 287.3 i EUF-fördraget har revisionsrätten rätt att få tillgång till alla relevanta handlingar och uppgifter som den anser sig behöva för att utföra sitt uppdrag, inbegripet säkerhetsskyddsklassificerade EU-uppgifter, vilket ska ske i full överensstämmelse med principen om lojalt samarbete mellan institutionerna och principen om tilldelade befogenheter. Denna rätt till tillgång till säkerhetsskyddsklassificerade EU-uppgifter, som garanteras i EUF-fördraget, kan inte ifrågasättas av upphovsmannen till säkerhetsskydds-klassificerade EU-uppgifter, medan revisionsrätten kan uppmanas att införa och respektera vissa säkerhetsåtgärder, såsom beskrivs närmare i detta beslut.

Revisionsrättens ledamöter, tjänstemän och övriga anställda är, även efter det att de har lämnat sin tjänst, bundna av tystnadsplikt enligt artikel 339 i EUF-fördraget, artikel 17 i tjänsteföreskrifterna och rättsakter som antagits med stöd av dessa.

Med tanke på uppgifternas känsliga karaktär kräver hanteringen av säkerhetsskyddsklassificerade EU-uppgifter att sekretesskravet efterlevs genom lämpliga säkerhetsåtgärder som kan garantera en hög skyddsnivå för dessa uppgifter och som är likvärdiga med dem som fastställs i de bestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter som antagits av EU:s övriga institutioner, byråer och organ, varvid revisionsrätten,

om den anser att sådana säkerhetsåtgärder inte är motiverade med hänsyn till uppgifternas art och typ, förbehåller sig rätten att göra de iakttagelser som den finner lämpliga, samtidigt som den respekterar de säkerhetsskydds-klassificerade EU-uppgifternas säkerhetsskyddsklassificeringsnivå.

Säkerhetsåtgärder för att skydda konfidentialiteten, riktigheten och tillgängligheten för de uppgifter som överlämnas till revisionsrätten måste vara lämpliga för den art och typ av uppgifter som berörs.

Tillgång till säkerhetsskyddsklassificerade uppgifter måste ges till revisionsrätten i enlighet med principen om behovsenlig behörighet för att revisionsrätten ska kunna utföra det uppdrag som anförtrotts den genom fördragen och genom rättsakter som antagits på grundval av fördragen.

Med tanke på vissa uppgifters art och känsliga innehåll är det lämpligt att inrätta ett särskilt förfarande för revisionsrättens hantering av handlingar som innehåller säkerhetsskyddsklassificerade EU-uppgifter.

Institutionen ska se till att detta beslut genomförs i enlighet med alla tillämpliga regler, särskilt bestämmelserna om skydd av personuppgifter, fysisk säkerhet för personer, byggnader och informationsteknik samt allmänhetens tillgång till handlingar.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

<u>Artikel 1</u> **Syfte och tillämpningsområde**

1. I detta beslut fastställs grundläggande principer och minimisäkerhetsnormer för skydd av säkerhetsskyddsklassificerade uppgifter som revisionsrätten behandlar i samband med utövandet av sitt uppdrag.

2. I detta beslut avses med *säkerhetsskyddsklassificerade uppgifter* någon eller alla av följande typer av uppgifter:

   a) ”Säkerhetsskyddsklassificerade EU-uppgifter” enligt definitionen i andra EU-institutioners, EU-byråers eller EU-organs säkerhetsbestämmelser som är försedda med någon av följande säkerhetsskyddsmarkeringar:

      - *TRES SECRET UE/EU TOP SECRET*: uppgifter och materiel vars obehöriga röjande skulle kunna medföra synnerligt men för Europeiska unionens eller en eller flera medlemsstaters väsentliga intressen.

      - *SECRET UE/EU SECRET*: uppgifter och materiel vars obehöriga röjande skulle kunna medföra betydande men för Europeiska unionens eller en eller flera medlemsstaters väsentliga intressen.

      - *CONFIDENTIEL UE/EU CONFIDENTIAL*: uppgifter och materiel vars obehöriga röjande skulle kunna medföra ett inte obetydligt men för Europeiska unionens eller en eller flera medlemsstaters väsentliga intressen.

      - *RESTREINT UE/EU RESTRICTED*: uppgifter och materiel vars obehöriga röjande skulle kunna medföra endast ringa men för Europeiska unionens eller en eller flera medlemsstaters intressen.

b) Säkerhetsskyddsklassificerade uppgifter som lämnas av medlemsstater, med en nationell säkerhetsskyddsmarkering som motsvarar någon av de säkerhetsskyddsmarkeringar[1] som används för säkerhetsskyddsklassificerade EU-uppgifter som förtecknas i led a.

c) Säkerhetsskyddsklassificerade uppgifter som lämnas till Europeiska revisionsrätten av tredjestater eller internationella organisationer, med en säkerhetsskyddsmarkering som motsvarar någon av de säkerhetsskyddsmarkeringar som används för säkerhetsskydds-klassificerade EU-uppgifter som förtecknas i led a i enlighet med vad som fastställs i relevanta avtal eller administrativa överenskommelser om informationssäkerhet.

3. Revisionsrätten ska hantera uppgifter på nivån *RESTREINT UE/EU RESTRICTED* i sina lokaler och vidta alla nödvändiga skyddsåtgärder i detta syfte. Arrangemang ska utarbetas för att den personal vid revisionsrätten som behöver få tillgång till säkerhetsskyddsklassificerade EU-uppgifter med en högre säkerhetsskyddsnivå ska kunna få detta i lämpliga lokaler vid andra EU-institutioner, EU-organ eller EU-byråer.

4. Detta beslut ska tillämpas på alla revisionsrättens avdelningar och lokaler.

5. Utom när en bestämmelse avser särskilda grupper av anställda, ska detta beslut tillämpas på ledamöterna av revisionsrätten, revisionsrättens personal som omfattas av tjänsteföreskrifterna och anställningsvillkoren för övriga anställda i Europeiska gemenskaperna[2], nationella experter som är utstationerade vid revisionsrätten, tjänsteleverantörer och deras anställda, praktikanter samt var och en som har tillträde till revisionsrättens byggnader eller andra tillgångar eller till uppgifter som hanteras av revisionsrätten.

6. Om inte något annat anges ska bestämmelserna om säkerhetsskyddsklassificerade EU-uppgifter tillämpas på ett likvärdigt sätt på de säkerhetsskyddsklassificerade uppgifter som avses i punkt 2 b och c i denna artikel.

Artikel 2 **Definitioner**

I detta beslut gäller följande definitioner:

a) *bemyndigande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter*: ett beslut som revisionsrättens direktör för personalfrågor och ekonomi och allmänna tjänster har fattat på grundval av en positiv bedömning från en behörig myndighet i en medlemsstat om att en tjänsteman eller en annan anställd vid revisionsrätten eller en nationell expert, under förutsättning att deras behovsenliga behörighet har fastställts och de har fått vederbörlig information om sitt ansvar, ska ha tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till en angiven säkerhetsskyddsklassificeringsnivå (*CONFIDENTIEL UE/EU CONFIDENTIAL* eller högre) till och med ett angivet datum. Sådana personer är då ”säkerhetsbemyndigade”.

b) *säkerhetsskyddsklassificering*: tilldelning av en säkerhetsskyddsklassificeringsnivå för uppgifter på grundval av graden av skada som skulle kunna orsakas av obehörigt röjande av dessa uppgifter.

---

[1] Se avtalet mellan Europeiska unionens medlemsstater, församlade i rådet, om skydd av säkerhetsskyddsklassificerade uppgifter som utbyts i Europeiska unionens intresse av den 4 maj 2011 och bilagan till detta OJ 2011/C 202/13.

[2] Förordning nr 31 (EEG) om tjänsteföreskrifter för tjänstemän och anställningsvillkor för övriga anställda, i dess ändrade lydelse, EGT 01962R0031-1.1.2020-019.003-1 (https://eur-lex.europa.eu/eli/reg/1962/31_(1)/2020-01-01).

c) *kryptoprodukter*: kryptoalgoritmer, maskinvara för kryptering och programvarumoduler och produkter som innehåller tillämpningsdetaljer med tillhörande dokumentation samt nyckelmateriel.

d) *beslut att uppgifter inte längre ska vara säkerhetsskyddsklassificerade*: borttagande av varje säkerhetsskyddsklassificering.

e) *handling*: registrerad information, oavsett form eller fysiska egenskaper.

f) *inplacering på lägre säkerhetsskyddsklassificeringsnivå*: sänkning av nivån på säkerhetsskyddsklassificeringen.

g) *säkerhetsgodkännande av verksamhetsställe*: administrativt beslut av en nationell säkerhetsmyndighet om att ett verksamhetsställe ur säkerhetsperspektiv kan erbjuda tillräckligt säkerhetsskydd av säkerhetsskyddsklassificerade EU-uppgifter på en angiven säkerhetsskyddsklassificeringsnivå.

h) *hantering av säkerhetsskyddsklassificerade EU-uppgifter*: all hantering som säkerhetsskyddsklassificerade EU-uppgifter kan utsättas för under hela sin livscykel: upprättande, registrering, behandling, befordran, inplacering på lägre säkerhetsskydds-klassificeringsnivå samt beslut om att uppgifterna inte längre ska vara säkerhetsskydds-klassificerade och förstöring. I samband med kommunikations- och informationssystem omfattar detta också insamling, visning, överföring och förvaring.

i) *innehavare*: vederbörligen bemyndigad person som konstaterats ha behovsenlig behörighet och som förfogar över en säkerhetsskyddsklassificerad uppgift och därmed ansvarar för dess skydd.

j) *informationssäkerhetsmyndighet*: informationssäkerhetsansvarig vid revisionsrätten, som helt eller delvis får delegera de arbetsuppgifter som anges i detta beslut.

k) *uppgifter*: alla skriftliga eller muntliga uppgifter, oavsett på vilket lagringsmedium de finns eller från vem de härrör.

l) *materiel*: varje medium, databärare eller maskin eller utrustning.

m) *upphovsman*: EU-institution, EU-byrå eller EU-organ, medlemsstat, tredjestat eller internationell organisation under vars behörighet säkerhetsskyddsklassificerade uppgifter har upprättats och/eller införts i unionens strukturer.

n) *personalsäkerhetsgodkännande*: ett utlåtande från en medlemsstats behöriga myndighet vilket görs efter genomförande av en säkerhetsprövning som utförs av en medlemsstats behöriga myndigheter och i vilket det intygas att en person får beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till en angiven nivå (*CONFIDENTIEL UE/EU CONFIDENTIAL* eller högre) till och med ett angivet datum.

o) *intyg om personalsäkerhetsgodkännande*: ett intyg utfärdat av revisionsrättens direktör för personalfrågor, ekonomi och allmänna tjänster där det fastställs att en person är säkerhetsprövad och innehar ett giltigt nationellt personalsäkerhetsgodkännande eller ett säkerhetsbemyndigande som visar vilken nivå av säkerhetsskyddsklassificerade EU-uppgifter som personen kan få tillgång till (*CONFIDENTIEL UE/EU CONFIDENTIAL* eller högre), giltighetsdatum för personalsäkerhetsgodkännandet eller personalsäkerhets-bemyndigandet samt vilket datum själva intyget löper ut.

p) *myndighet för fysisk säkerhet*: revisionsrättens säkerhetschef, som ska ansvara för genomförandet av nödvändiga fysiska säkerhetsåtgärder och förfaranden för att skydda säkerhetsskyddsklassificerade EU-uppgifter.

q) *registratorskontoret*: kontor som ska förvaltas av revisionsrättens sekretariat, vara beläget i ett administrativt utrymme och lyda under revisionsrättens direktör för personalfrågor,

ekonomi och allmänna tjänster. Det ansvarar för in- och utförsel av uppgifter klassificerade som *RESTREINT UE/EU RESTRICTED*, eller motsvarande, som utbyts med revisionsrätten.

r) *registreringsenhet för säkerhetsskyddsklassificerade EU-uppgifter*: ett område som upprättas inom ett säkrat utrymme. Enheten ska förvaltas av revisionsrättens säkerhetsgodkända och bemyndigade kontrolltjänsteman för registreringsenheten. Det ansvarar för in- och utförsel av uppgifter klassificerade som *CONFIDENTIEL UE/EU CONFIDENTIAL*, eller motsvarande, som utbyts med revisionsrätten.

s) *myndighet för säkerhetsackreditering*: revisionsrättens direktör för personalfrågor, ekonomi och allmänna tjänster.

Artikel 3 **Åtgärder för att skydda säkerhetsskyddsklassificerade EU-uppgifter**

1. Revisionsrätten ska se till att alla säkerhetsskyddsklassificerade uppgifter som lämnas till den skyddas på ett sätt som står i proportion till den säkerhetsskyddsklassificeringsnivå som fastställts av upphovsmannen och i enlighet med detta beslut.

2. I detta syfte ska revisionsrätten låta hanteringen av säkerhetsskyddsklassificerade EU-uppgifter omfattas av fysiska säkerhetsåtgärder och, vid behov, personalsäkerhetsåtgärder, inbegripet åtkomstbehörighet för identifierade personer och åtgärder för skydd av kommunikations- och informationssystem. Dessa åtgärder beskrivs i artiklarna 4–6 och ska gälla under de säkerhetsskyddsklassificerade EU-uppgifternas hela livscykel. De ska motsvara de säkerhetsskyddsklassificerade EU-uppgifternas eller materielens säkerhetsskydds-klassificeringsnivå, form och volym, läge och konstruktion för de utrymmen där de säkerhetsskyddsklassificerade EU-uppgifterna förvaras och det lokalt bedömda hotet från fientlig och/eller brottslig verksamhet, inklusive spionage, sabotage och terroristverksamhet.

3. Säkerhetsskyddsklassificerade EU-uppgifter ska skyddas genom fysiska säkerhetsåtgärder, och uppgifter på säkerhetsskyddsklassificeringsnivån *CONFIDENTIEL UE/EU CONFIDENTIAL* eller högre ska dessutom skyddas genom personalsäkerhetsåtgärder.

4. Säkerhetsskyddsklassificerade EU-uppgifter får endast lämnas ut till personer med behovsenlig behörighet inom institutionen. En innehavare av säkerhetsskyddsklassificerade EU-uppgifter ska skydda dem i enlighet med detta beslut.

5. Säkerhetsskyddsklassificerade EU-uppgifter får inte lämnas ut muntligen eller skriftligen. Revisionsrättens preliminära iakttagelser, rapporter, yttranden, pressmeddelanden och andra produkter, dess webbplats och intranät, muntliga inlägg, svar på begäranden om tillgång till handlingar[3] och röst- eller videoinspelningar får inte innehålla eller hänvisa till säkerhetsskyddsklassificerade EU-uppgifter eller utdrag ur dessa. Om upphovsmannen har offentliggjort handlingar eller information som innehåller en hänvisning till säkerhetsskydds-klassificerade EU-uppgifter, får dock denna hänvisning nämnas.

6. Trots vad som sägs i punkt 5 får revisionsrätten och upphovsmannen komma överens om att revisionsrätten vid en särskild revision får mångfaldiga eller använda delar av säkerhetsskyddsklassificerade EU-uppgifter i en handling. I sådana fall ska denna handling från revisionsrätten först skickas till upphovsmannen för de säkerhetsskyddsklassificerade EU-uppgifterna i fråga före eller under det kontradiktoriska förfarandet. I detta fall ska revisionsrätten och upphovsmannen komma överens om huruvida den handling som utfärdats av revisionsrätten ska säkerhetsskyddsklassificeras. Om en föredragande ledamot av

[3] I enlighet med revisionsrättens beslut nr 12/2005 om allmänhetens tillgång till revisionsrättens handlingar, ändrat genom beslut nr 14/2009 (EUT 2009/C 67, s. 1).

revisionsrätten anser det nödvändigt att översända en granskningsrapport som helt eller delvis har säkerhetsskyddsklassificerats till vissa mottagare vid Europaparlamentet eller rådet – med beaktande av alla säkerhetsåtgärder som fastställs i detta beslut – ska detta kräva samtycke från upphovsmannen till de säkerhetsskyddsklassificerade uppgifterna. Den rättsliga ramen och förfarandet för utbyte av sådana handlingar fastställs i artikel 7.

7. Om utövandet av revisionsrättens uppdrag kräver att vissa delar av en säkerhetsskyddsklassificerad handling eller säkerhetsskyddsklassificerade uppgifter ska delas i större utsträckning, ska revisionsrätten, med vederbörlig hänsyn till säkerhetsskydds-markeringen, samråda med upphovsmannen innan den beslutar att använda dessa delar eller uppgifter, om den anser att det finns ett övervägande allmänintresse av att göra detta. Uppgifterna ska endast användas i rapporten på ett sådant sätt att upphovsmannens intressen inte kan skadas. Detta skulle kunna säkerställas på lämpligt sätt genom att man ber upphovsmannen att lämna synpunkter för att nå en överenskommelse om hur uppgifterna ska anonymiseras, koncentreras eller generaliseras med mera, samtidigt som man respekterar intresset hos dem som främst berörs av den offentliggjorda informationen.

8. Revisionsrätten får inte lämna ut säkerhetsskyddsklassificerade EU-uppgifter till någon annan av EU:s institutioner, byråer, organ eller kontor, en medlemsstat, en tredjestat eller en internationell organisation utan föregående samråd med och uttryckligt skriftligt medgivande från upphovsmannen.

9. Om inte upphovsmannen till en handling på säkerhetsskyddsklassificeringsnivån *SECRET UE/EU SECRET* eller lägre har angett begränsning för kopiering eller översättning av handlingen, får en sådan handling kopieras eller översättas på innehavarens begäran och i enlighet med de praktiska arbetsanvisningarna från revisionsrättens myndighet för informationssäkerhet. De säkerhetsåtgärder som ska tillämpas på originalhandlingen ska även tillämpas på kopior och översättningar av denna.

10. Om revisionsrätten har behov av att en säkerhetsskyddsklassificerad handling som den har mottagit eller har rätt att få tillgång till inplaceras på en lägre säkerhetsskydds-klassificeringsnivå, eller att säkerhetsskyddsklassificeringen för handlingen tas bort, ska den samråda med upphovsmannen för att fråga om upphovsmannen kan tillhandahålla en version av handlingen på en lägre säkerhetsskyddsklassificeringsnivå eller en version av handlingen som inte längre är säkerhetsskyddsklassificerad.

Artikel 4 Personalsäkerhet

1. Revisionsrättens ledamöter ska i kraft av sina uppdrag ha rätt att få tillgång till alla säkerhetsskyddsklassificerade EU-uppgifter och att delta i möten där säkerhetsskydds-klassificerade EU-uppgifter behandlas. Ledamöterna ska informeras om sina säkerhets-skyldigheter när det gäller skyddet av säkerhetsskyddsklassificerade EU-uppgifter och ska skriftligen bekräfta sitt ansvar för skyddet av sådana uppgifter.

2. En anställd vid revisionsrätten ska, oavsett om det är en tjänsteman, personal som omfattas av anställningsvillkoren för övriga anställda eller en nationell expert, endast beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter

   i. när personens behovsenliga behörighet fastställts,

   ii. när personen har informerats om säkerhetsbestämmelserna för skydd av säkerhetsskyddsklassificerade EU-uppgifter och relevanta säkerhetsnormer och riktlinjer samt bekräftat sitt ansvar i fråga om skyddet av sådana uppgifter,

iii. för uppgifter på säkerhetsskyddsklassificeringsnivån *CONFIDENTIEL UE/EU CONFIDENTIAL* eller högre, när vederbörande har genomgått säkerhetsprövning och beviljats bemyndigande för tillgång.

3. Förfarandet för att avgöra om en tjänsteman eller annan anställd vid revisionsrätten kan få bemyndigande för tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån *CONFIDENTIEL UE/EU CONFIDENTIAL* eller högre, med beaktande av personens lojalitet, integritet och pålitlighet, och efter försäkran från de behöriga myndigheterna i en medlemsstat i enlighet med artikel 2 n, ska fastställas i ett delegerat beslut som fattas i enlighet med artikel 10.10. Beslut om beviljande av bemyndigande för tillgång ska fattas av revisionsrättens direktör för personalfrågor, ekonomi och allmänna tjänster.

4. Revisionsrättens direktör för personalfrågor, ekonomi och allmänna tjänster får utfärda intyg om personalsäkerhetsgodkännande som anger vilken nivå av säkerhetsskyddsklassificerade EU-uppgifter som enskilda personer kan få tillgång till (*CONFIDENTIEL UE/EU CONFIDENTIAL* eller högre), giltighetsperioden för motsvarande bemyndigande och datum då intyget löper ut.

5. Endast personer med det bemyndigande som avses i punkt 2 iii ovan och ledamöter av revisionsrätten enligt punkt 1 ovan får delta i möten där uppgifter på säkerhetsskydds-klassificeringsnivån *CONFIDENTIEL UE/EU CONFIDENTIAL* eller högre behandlas. Revisionsrätten och upphovsmannen ska besluta om de praktiska arrangemangen för sådana möten i varje enskilt fall.

6. De avdelningar vid revisionsrätten som ansvarar för att anordna möten där uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ska behandlas ska i god tid informera myndigheten för informationssäkerhet om datum, tidpunkt och plats för dessa möten samt om vilka som kommer att delta vid mötena.

7. Varje person som utan vederbörligt tillstånd och/eller utan bevisad behovsenlig behörighet förfogar över säkerhetsskyddsklassificerade EU-uppgifter ska rapportera situationen till myndigheten för informationssäkerhet så snart som möjligt och se till att de säkerhetsskyddsklassificerade EU-uppgifterna skyddas i enlighet med detta beslut.

Artikel 5 **Fysiska säkerhetsåtgärder för att skydda säkerhetsskyddsklassificerade uppgifter**

1. Med *fysisk säkerhet* avses användningen av fysiska och tekniska skyddsåtgärder för att hindra obehörig tillgång till säkerhetsskyddsklassificerade EU-uppgifter.

2. Fysiska säkerhetsåtgärder ska utformas för att förhindra intrång i smyg eller genom tvång, för att avskräcka, hindra och avslöja otillåtet agerande och för att möjliggöra åtskillnad mellan personal med avseende på deras tillgång till säkerhetsskyddsklassificerade EU-uppgifter utifrån principen om behovsenlig behörighet. Sådana åtgärder ska fastställas utifrån ett riskhanteringsförfarande i enlighet med detta beslut.

3. Utrymmen inom vilka säkerhetsskyddsklassificerade EU-uppgifter hanteras eller förvaras ska inspekteras med jämna mellanrum av revisionsrättens behöriga säkerhetsmyndighet.

4. Endast utrustning eller anordningar som uppfyller gällande regler inom EU:s institutioner, byråer eller organ för skydd av säkerhetsskyddsklassificerade EU-uppgifter ska användas för att hantera och lagra säkerhetsskyddsklassificerade EU-uppgifter.

5. Revisionsrättens personal kan få tillgång till EU-uppgifter med en säkerhetsskydds-klassificeringsnivå motsvarande *CONFIDENTIEL UE/EU CONFIDENTIAL* eller högre i säkrade utrymmen utanför revisionsrättens lokaler.

6. Revisionsrätten får ingå ett servicenivåavtal med en annan EU-institution i Luxemburg för att kunna hantera och lagra uppgifter på säkerhetsskyddsklassificeringsnivån *CONFIDENTIEL UE/EU CONFIDENTIAL* eller högre i ett säkrat utrymme inom den institutionen. Dessa säkerhetsskyddsklassificerade EU-uppgifter får inte hanteras eller lagras i revisionsrättens lokaler och får inte dupliceras eller översättas av revisionsrätten, såvida inte detta specifikt medgivits av upphovsmannen.

7. Revisionsrätten ska registrera alla mottagna uppgifter som är säkerhetsskyddsklassificerade på nivån RESTREINT UE/EU RESTRICTED. Konsultation av uppgifter med en säkerhetsskyddsklassificeringsnivå motsvarande *CONFIDENTIEL UE/EU CONFIDENTIAL* eller högre utanför revisionsrättens lokaler ska registreras av säkerhetsskäl.

8. Säkerhetsskyddsklassificerade EU-uppgifter på nivån *RESTREINT UE/EU RESTRICTED* får förvaras i lämpliga låsbara kontorsmöbler i ett administrativt eller säkrat utrymme. Säkerhetsskyddsklassificerade EU-uppgifter på nivåerna *CONFIDENTIEL UE/EU CONFIDENTIAL* eller *SECRET UE/EU SECRET* ska förvaras enligt ett servicenivåavtal i ett säkerhetsskåp i ett säkrat utrymme vid en annan EU-institution i Luxemburg.

9. Säkerhetsskyddsklassificerade EU-uppgifter som finns utanför registreringsenheten ska överföras mellan avdelningar och lokaler på följande sätt:

   a) Som allmän regel ska säkerhetsskyddsklassificerade EU-uppgifter överföras elektroniskt med kryptoprodukter som godkänts i enlighet med artikel 6.8.

   b) Om säkerhetsskyddsklassificerade EU-uppgifter inte överförs enligt led a ska de överföras med hjälp av en databärare (t.ex. USB-minnen, cd-skivor, hårddiskar) som skyddas med kryptoprodukter som godkänts i enlighet med artikel 6.8, eller som papperskopia i ett ogenomskinligt förslutet kuvert.

10. Uppgifter på säkerhetsskyddsklassificeringsnivån *RESTREINT UE/EU RESTRICED* får förstöras av innehavaren i enlighet med revisionsrättens arkiveringsregler. Uppgifter på säkerhetsskydds-klassificeringsnivån *CONFIDENTIEL UE/EU CONFIDENTIAL* eller högre får endast förstöras av kontrolltjänstemannen för registreringsenheten på instruktion från innehavaren eller en behörig myndighet i enlighet med revisionsrättens arkiveringsregler. Handlingar på säkerhetsskyddsklassificeringsnivån *SECRET UE/EU SECRET* ska förstöras i närvaro av ett vittne med säkerhetsgodkännande som minst motsvarar säkerhetsskyddsklassificeringsnivån för den handling som ska förstöras. Kontrolltjänstemannen för registreringsenheten och vittnet, om närvaro av ett sådant krävs, ska underteckna ett förstöringsintyg, som ska arkiveras vid registreringsenheten. Kontrolltjänstemannen för registreringsenheten ska bevara förstöringsintyg för handlingar på säkerhetsskyddsklassificeringsnivån *CONFIDENTIEL UE/EU CONFIDENTIAL* och *SECRET UE/EU SECRET* i minst fem år.

11. Myndigheten för den fysiska säkerheten och informationssäkerhetsmyndigheten ska upprätta en gemensam plan, med beaktande av lokala förhållanden, för skydd av säkerhetsskyddsklassificerade EU-uppgifter i kristider, inbegripet, vid behov, planer för att förstöra eller evakuera dem i händelse av en nödsituation. De ska utfärda sådana instruktioner som de anser lämpliga för att förhindra att säkerhetsskyddsklassificerade EU-uppgifter hamnar i händerna på obehöriga personer.

12. Om säkerhetsskyddsklassificerade EU-uppgifter måste transporteras fysiskt ska revisionsrätten följa de åtgärder som upphovsmannen fastställt för att skydda dem mot obehörigt röjande under transporten.

13. De fysiska säkerhetsåtgärder som ska tillämpas i administrativa utrymmen där uppgifter på säkerhetsskyddsklassificeringsnivån *RESTREINT UE/EU RESTRICTED* hanteras och lagras anges i bilagan.

<u>Artikel 6</u> Skydd av säkerhetsskyddsklassificerade EU-uppgifter i kommunikations- och informationssystem

1. I denna artikel avses med *kommunikations- och informationssystem* varje system som gör det möjligt att hantera säkerhetsskyddsklassificerade EU-uppgifter i elektronisk form. Ett kommunikations- och informationssystem ska innefatta alla de resurser som krävs för att det ska fungera, inklusive infrastruktur, organisation, personal och informationsresurser.

2. Med *behörig användare* avses en ledamot av revisionsrätten eller en tjänsteman, en annan anställd eller en nationell expert vid revisionsrätten med ett fastställt och konstaterat behov av tillgång till ett särskilt informationssystem.

3. Revisionsrätten ska avge en försäkran om att dess system i tillräcklig utsträckning kommer att skydda den information de hanterar och fungera som de ska när det krävs, under kontroll av behöriga användare. För detta ändamål ska systemen garantera lämpliga nivåer för följande:

   - Autenticitet: garanti för att uppgifterna är riktiga och härrör från pålitliga källor.
   - Tillgänglighet: egenskapen att vara tillgängliga och användbara för behöriga enheter.
   - Konfidentialitet: egenskapen att uppgifter skyddas mot insyn av obehöriga personer, enheter eller processer.
   - Riktighet: egenskapen att säkerställa att uppgifter och tillgångar är exakta och fullständiga.
   - Oavvislighet: möjlighet att bevisa att en åtgärd eller händelse har ägt rum så att denna åtgärd eller händelse inte senare kan förnekas.

   Denna försäkran ska grundas på en riskhanteringsprocess. Med *risk* avses potentialen för att ett givet hot kommer att utnyttja intern och extern sårbarhet hos en organisation eller något av de system den använder och därigenom skada organisationen och dess materiella eller immateriella tillgångar. Risken kan mätas som en kombination av sannolikheten att hot uppträder och följderna därav. En riskhanteringsprocess ska bestå av följande åtgärder: identifiering av hot och sårbarhet, riskbedömning, riskhantering, riskacceptans och riskkommunikation.

   - Med *riskbedömning* avses identifiering av hot och sårbarheter och utförande av en därmed sammanhängande riskanalys, det vill säga en analys av sannolikhet och konsekvenser.
   - Med *riskhantering* avses att mildra, undanröja, reducera (genom en lämplig kombination av tekniska, fysiska, organisatoriska eller procedurmässiga åtgärder), överföra eller övervaka risken.
   - Med *riskacceptans* avses ett beslut efter riskhanteringen om att godta att en kvarstående risk fortfarande existerar.
   - Med *kvarstående risk* avses den risk som kvarstår efter det att säkerhetsåtgärder har vidtagits, med tanke på att alla hot inte kan motverkas och alla sårbarheter inte kan elimineras.

- Med *riskkommunikation* avses åtgärder för att öka medvetenheten om risker bland systemanvändargrupper, information till tillståndsmyndigheter om dessa risker och rapportering av dem till driftsmyndigheter.

4. Alla elektroniska anordningar och all elektronisk utrustning som används för hantering av säkerhetsskyddsklassificerade EU-uppgifter ska följa gällande regler för skydd av säkerhetsskyddsklassificerade EU-uppgifter. Företräde ska ges till elektroniska anordningar och elektronisk utrustning som redan har ackrediterats av en annan EU-institution, en annan EU-byrå eller ett annat EU-organ. Anordningarna ska garanteras vara säkra under hela sin livscykel.

5. Revisionsrättens kommunikations- och informationssystem för hantering av säkerhetsskyddsklassificerade EU-uppgifter ska ackrediteras av en lämplig myndighet. I detta syfte avser revisionsrätten teckna ett servicenivåavtal med en myndighet för säkerhetsackreditering vid någon EU-institution som har kapacitet att ackreditera kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter, i syfte att erhålla ett ackrediteringsutlåtande för uppgifter på säkerhetsskydds-klassificeringsnivån *RESTREINT UE/EU RESTRICTED* som kan hanteras i revisionsrättens kommunikations- och informationssystem, och motsvarande driftsvillkor. I servicenivåavtalet ska också de standarder som ska tillämpas för ackrediteringsförfarandet anges, och det ska ingås i enlighet med förfarandet i artikel 10.3.

6. Om revisionsrätten behöver upprätta ett eget ackrediteringsförfarande för sina kommunikations- och informationssystem ska ett delegerat beslut enligt artikel 10.10 i detta beslut fastställa förfarandet i enlighet med standarderna för ackrediteringsförfarandet för kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter vid andra EU-institutioner, EU-byråer och EU-organ.

7. Ansvaret för att förbereda ackrediteringsakter och ackrediteringsunderlag i enlighet med gällande standarder ska helt och hållet åligga ägaren av det berörda kommunikations- och informationssystemet.

8. Om de säkerhetsskyddsklassificerade EU-uppgifterna skyddas med hjälp av kryptoprodukter ska revisionsrätten ge företräde till produkter som har godkänts av rådet eller rådets generalsekreterare i dess funktion som kryptogodkännande myndighet eller, i annat fall, till produkter som godkänts av andra EU-institutioner, EU-byråer och EU-organ för skydd av säkerhetsskyddsklassificerade EU-uppgifter.

9. Uppgifter på säkerhetsskyddsklassificeringsnivån *RESTREINT UE/EU RESTRICTED* får endast hanteras på elektronisk utrustning (t.ex. arbetsstationer, skrivare, kopieringsapparater) som är placerade i ett administrativt utrymme eller ett säkrat utrymme. Elektronisk utrustning som hanterar uppgifter på säkerhetsskyddsklassificeringsnivån *RESTREINT UE/EU RESTRICTED* ska åtskiljas från andra datornät och skyddas med hjälp av lämpliga fysiska eller tekniska åtgärder.

10. All personal vid revisionsrätten som arbetar med utformning, utveckling, testning, drift, förvaltning eller användning av kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter ska underrätta informationssäkerhetsansvarig vid revisionsrätten om alla potentiella säkerhetsbrister, incidenter, överträdelser av säkerhetsbestämmelser eller röjanden som kan påverka skyddet av kommunikations- och informationssystemet och/eller säkerhetsskyddsklassificerade EU-uppgifter i systemet.

Artikel 7 **Förfarande för utbyte och tillgängliggörande av säkerhetsskyddsklassificerade uppgifter**

1. När EU:s institutioner, byråer, organ och kontor samt nationella myndigheter är skyldiga enligt fördragen eller rättsakter som antagits på grundval av fördragen att ge revisionsrätten tillgång till säkerhetsskyddsklassificerade EU-uppgifter gör de detta på eget initiativ eller på skriftlig begäran från revisionsrättens ordförande, den föredragande ledamoten eller de föredragande ledamöterna eller generalsekreteraren i enlighet med nedanstående förfarande.

2. En begäran om tillgång till handlingar ska lämnas till de berörda institutionerna via revisionsrättens registratorskontor.

3. Vid behov ska revisionsrätten ingå en administrativ överenskommelse om de praktiska arrangemangen för utbyte av säkerhetsskyddsklassificerade EU-uppgifter eller motsvarande information.

4. I syfte att ingå sådana administrativa överenskommelser ska revisionsrätten förse upphovsmannen med all nödvändig information om sitt informationssäkerhetssystem. Vid behov kan ett utvärderingsbesök anordnas.

5. Dessa administrativa överenskommelser ska ingås i full överensstämmelse med principerna om tilldelade befogenheter och lojalt samarbete som anges i artikel 13 i fördraget om Europeiska unionen. De ska ingås enligt det förfarande som fastställs i artikel 10.4.

6. Om det saknas administrativa överenskommelser med några av EU:s institutioner, organ eller byråer, ett tredjeland eller en internationell organisation om tillhandahållande av säkerhetsskyddsklassificerade uppgifter till revisionsrätten, ska revisionsrätten underteckna en åtagandeförklaring om att skydda de säkerhetsskyddsklassificerade uppgifter som den tar emot.

Artikel 8 **Överträdelse av säkerhetsbestämmelserna, förlust eller röjande av säkerhetsskyddsklassificerade uppgifter**

1. Med en *överträdelse av säkerhetsbestämmelserna* avses ett agerande eller en försummelse som begåtts av en person och som står i strid med säkerhetsbestämmelserna i detta beslut och dess tillämpningsföreskrifter.

2. Röjande av säkerhetsskyddsklassificerade EU-uppgifter inträffar när dessa som resultat av en säkerhetsöverträdelse helt eller delvis har lämnats ut till obehöriga.

3. Överträdelser av säkerhetsbestämmelserna eller misstänkta överträdelser av säkerhets-bestämmelserna ska omedelbart rapporteras till revisionsrättens informationssäkerhets-myndighet.

4. Om det är känt eller om det föreligger rimliga skäl att anta att säkerhetsskyddsklassificerade EU-uppgifter har röjts eller förlorats, ska informationssäkerhetsmyndigheten informera revisionsrättens direktör för personalfrågor, ekonomi och allmänna tjänster samt revisionsrättens generalsekreterare. Direktören för personalfrågor, ekonomi och allmänna tjänster ska omedelbart underrätta den berörda upphovsmannens säkerhetsmyndighet. Ovannämnda direktör för revisionsrätten ska genomföra en undersökning och underrätta revisionsrättens generalsekreterare och upphovsmannens säkerhetsmyndighet om resultaten och om de åtgärder som vidtagits för att förhindra att situationen upprepas. Om en ledamot

av revisionsrätten berörs ska revisionsrättens ordförande ansvara för att vidta åtgärder i samarbete med revisionsrättens generalsekreterare.

5. Varje tjänsteman eller annan anställd vid revisionsrätten som är ansvarig för en överträdelse av säkerhetsbestämmelserna i detta beslut och dess tillämpningsföreskrifter ska bli föremål för de påföljder som föreskrivs i tjänsteföreskrifterna och anställningsvillkoren för övriga anställda i Europeiska unionen.

6. Varje ledamot av revisionsrätten som inte följer bestämmelserna i detta beslut ska underkastas de åtgärder och påföljder som föreskrivs i artikel 286.6 i EUF-fördraget.

7. Den som är ansvarig för förlust eller röjande av säkerhetsskyddsklassificerade EU-uppgifter kan komma att underkastas disciplinära och/eller rättsliga åtgärder enligt tillämpliga lagar och andra författningar.

Artikel 9 **Säkerhet vid externa ingripanden**

1. Revisionsrätten får, i enlighet med ingångna kontrakt, anförtro utförandet av arbetsuppgifter som inbegriper eller kräver tillgång till säkerhetsskyddsklassificerade EU-uppgifter till entreprenörer som är registrerade i en medlemsstat. Detta kan ske särskilt i samband med underhåll av kommunikations- och informationssystem och datornätet.

2. Vid externa ingripanden ska revisionsrätten vidta alla nödvändiga säkerhetsåtgärder som avses i punkt 3 i denna artikel och bland annat begära ett säkerhetsgodkännande av verksamhetsstället för att säkerställa att säkerhetsskyddsklassificerade EU-uppgifter skyddas av anbudssökande och anbudsgivare under hela anbuds- och upphandlingsförfarandet samt av entreprenörer och underleverantörer under kontraktets hela löptid. Den upphandlande myndigheten ska se till att de minimisäkerhetsnormer som föreskrivs i detta beslut anges i kontrakten för att ålägga entreprenörerna att följa dem.

3. Säkerhetsbestämmelser, upphandlingsförfaranden samt mallar och standarder för kontrakt och underleverantörskontrakt som innebär tillgång till säkerhetsskyddsklassificerade EU-uppgifter, meddelanden om upphandling, vägledning om under vilka omständigheter säkerhetsgodkännande av verksamhetsställe och personal krävs, säkerhetsanvisningar för program eller projekt, säkerhetsskyddsöverenskommelser, besök samt överföring och transport av säkerhetsskyddsklassificerade EU-uppgifter inom ramen för sådana kontrakt och underleverantörskontrakt, ska överensstämma med de regler, mallar och standarder som Europeiska kommissionen fastställt för säkerhetsskyddsklassificerade kontrakt i kommissionens beslut (EU, Euratom) 2015/444 av den 13 mars 2015 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter.

Artikel 10 **Genomförande av beslutet och ansvarsfördelning**

1. Revisionsrättens avdelningar ska vidta alla nödvändiga åtgärder inom sitt ansvarsområde för att säkerställa att detta beslut och relevanta tillämpningsföreskrifter tillämpas i samband med hantering eller lagring av säkerhetsskyddsklassificerade EU-uppgifter eller andra säkerhetsskyddsklassificerade uppgifter.

2. Generalsekreteraren ska vara tillsättningsmyndighet och myndighet med befogenhet att sluta anställningsavtal för alla tjänstemän och övriga anställda. Generalsekreteraren får delegera ansvaret till direktören för personalfrågor, ekonomi och allmänna tjänster för att bevilja tjänstemän och annan personal behörighet att få tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån *CONFIDENTIEL UE/EU CONFIDENTIAL* eller högre, att

utöva dennes funktion som myndighet för säkerhetsackreditering för säkerhet och att utöva tillsyn över revisionsrättens sekretariat när det gäller hanteringen av säkerhetsskydds-klassificerade EU-uppgifter.

3. Generalsekreteraren ska vara behörig att ingå servicenivåavtal om ackreditering av revisionsrättens kommunikations- och informationsutrustning och kommunikations- och informationssystem, om användningen av ett säkrat utrymme i en annan EU-institution och om förfarandet för begäran om säkerhetsgodkännande av personal för tillgång till säkerhetsskyddsklassificerade EU-uppgifter.

4. Direktören för personalfrågor, ekonomi och allmänna tjänster ska vara behörig att ingå administrativa överenskommelser med EU:s institutioner, byråer och andra organ om utbyte av säkerhetsskyddsklassificerade EU-uppgifter som revisionsrätten behöver för att utföra sitt uppdrag. Direktören får också ingå administrativa överenskommelser med tredjestater eller internationella organisationer om skydd av säkerhetsskyddsklassificerade uppgifter som revisionsrätten tar emot.

5. Direktören för personalfrågor, ekonomi och allmänna tjänster ska vara behörig att underteckna varje åtagandeförklaring för skydd av säkerhetsskyddsklassificerade EU-uppgifter som ska tillhandahållas i samband med ett exceptionellt *ad hoc*-utlämnande.

6. Informationssäkerhetsansvarig vid revisionsrätten ska fungera som informationssäkerhets-myndighet. Den informationssäkerhetsansvariga och de personer till vilka han eller hon delegerar hela eller delar av sina uppdrag ska inneha ett lämpligt säkerhetsgodkännande. Informationssäkerhetsmyndigheten ska utöva sitt ansvar i nära samarbete med direktoratet för personalfrågor, ekonomi och allmänna tjänster, direktoratet för informationsteknik, arbetsmiljö och innovation samt direktoratet för kommittén för kontroll av revisionskvaliteten (se särskilt artiklarna 4, 6 och 8). Informationssäkerhetsmyndigheten ska också ansvara för utbildning och möten för att öka medvetenheten om informationssäkerhet och för regelbundna inspektioner för att kontrollera efterlevnaden av detta beslut, inbegripet vid externa ingripanden och eventuella åtgärder som ska vidtas för att säkerställa efterlevnaden.

7. Säkerhetschefen ska ansvara för de fysiska säkerhetsåtgärderna (särskilt de som anges i artikel 5).

8. Ett registratorskontor som inrättats vid revisionsrättens sekretariat ska vara in- och utförselställe för uppgifter på säkerhetsskyddsklassificeringsnivån *RESTREINT UE/EU RESTRICTED* och som revisionsrätten får utbyta med andra av EU:s institutioner, byråer och organ samt med medlemsstaterna. Det ska också vara in- och utförselställe för tredjestaters och internationella organisationers motsvarande uppgifter. Registratorskontoret ska organiseras i enlighet med ett delegerat beslut. Registratorn ska ansvara för följande:

   a) Registrering av in- och utförsel av uppgifter på säkerhetsskyddsklassificeringsnivån *RESTREINT UE/EU RESTRICTED*.

   b) Förvaltning av särskilda administrativa utrymmen för registrering av hantering, lagring och konsultation av säkerhetsskyddsklassificerade EU-uppgifter på nivån *RESTREINT UE/EU RESTRICTED*.

9. En registreringsenhet ska inrättas inom ramen för ett servicenivåavtal om användningen av en annan EU-institutions säkrade utrymme. Registreringsenheten, som ska organiseras av revisionsrättens sekretariat under ansvar av revisionsrättens direktör för personalfrågor, ekonomi och allmänna tjänster, ska vara in- och utförselställe för uppgifter på säkerhetsskyddsklassificeringsnivån *CONFIDENTIEL UE/EU CONFIDENTIAL* eller högre och som revisionsrätten får utbyta med andra av EU:s institutioner, byråer och organ samt med

medlemsstaterna. Den ska också vara in- och utförselställe för tredjestaters och internationella organisationers motsvarande uppgifter. Registreringsenheten ska vara utrustad med lämpliga säkerhetsskåp och annan säkerhetsutrustning som är lämplig för att skydda uppgifter på säkerhetsskyddsklassificeringsnivån *CONFIDENTIEL UE/EU CONFIDENTIAL* eller högre. Registreringsenheten ska organiseras i enlighet med ett delegerat beslut. Kontrolltjänstemannen för registreringsenheten ska inneha ett lämpligt säkerhetsgodkännande och ansvara för följande:

a) Ledning av verksamhet som avser registrering, bevarande, konsultation, mångfaldigande, översättning, överföring, avsändande och, i tillämpliga fall, förstöring av säkerhetsskyddsklassificerade EU-uppgifter.

b) Utförande av eventuella andra arbetsuppgifter i samband med skyddet av säkerhetsskyddsklassificerade EU-uppgifter som fastställs i ett delegerat beslut.

10. Förvaltningskommittén ska anta ett delegerat beslut om tillämpningsföreskrifterna för detta beslut. Den informationssäkerhetsansvariga ska fastställa riktlinjer för informationssäkerhet. Kommittén för kontroll av revisionskvaliteten ska utarbeta riktlinjer för revision.

Artikel 11 **Ikraftträdande**

Detta beslut träder i kraft dagen efter det att det har offentliggjorts i Europeiska unionens officiella tidning.

Utfärdat i Luxemburg den 3 juni 2021

För revisionsrätten

Klaus-Heiner Lehne
ordförande

Bilaga: FYSISKA SÄKERHETSÅTGÄRDER AVSEENDE ADMINISTRATIVA UTRYMMEN FÖR SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

BILAGA

FYSISKA SÄKERHETSÅTGÄRDER AVSEENDE ADMINISTRATIVA UTRYMMEN FÖR SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

1. Denna bilaga innehåller tillämpningsföreskrifter till artikel 5 i beslutet. Dessa är minimiregler för det fysiska skyddet av revisionsrättens administrativa utrymmen för uppgifter på säkerhetsskyddsklassificeringsnivån *RESTREINT UE/EU RESTRICTED*. Dessa utrymmen är avsedda för registrering, lagring och konsultation av uppgifter på säkerhetsskydds-klassificeringsnivån *RESTREINT UE/EU RESTRICTED*.

2. Syftet med fysiska säkerhetsåtgärder i administrativa utrymmen är att hindra obehörigt tillträde till dessa utrymmen med hjälp av följande åtgärder:

   a) En synlig yttre gräns upprättas som gör att personer kan kontrolleras.

   b) Obeledsagat tillträde ska endast beviljas personer som har fått vederbörligt tillstånd av revisionsrättens informationssäkerhetsmyndighet eller någon annan behörig myndighet.

   c) Övriga personer ska alltid ledsagas eller genomgå likvärdiga kontroller.

3. Revisionsrättens informationssäkerhetsmyndighet får undantagsvis bevilja tillträde för obehöriga, även för arbete i ett administrativt utrymme, förutsatt att detta inte medför tillgång till säkerhetsskyddsklassificerade EU-uppgifter, som ska förbli inlåsta. Sådana personer får endast vistas i utrymmet om de åtföljs och ständigt övervakas av informationssäkerhetsmyndigheten eller kontrolltjänstemannen för registreringsenheten.

4. Informationssäkerhetsmyndigheten ska fastställa förfaranden för hantering av nycklar och/eller kombinationer till alla administrativa utrymmen och all säkerhetsanpassad inredning. Syftet med dessa förfaranden ska vara att skydda mot obehörigt tillträde.

5. Kombinationer ska memoreras av lägsta möjliga antal personer som behöver känna till dem. Kombinationer för säkerhetsanpassad inredning som används för lagring av uppgifter på säkerhetsskyddsklassificeringsnivån *RESTREINT UE/EU RESTRICTED* ska ändras

   - vid mottagande av ny säkerhetsanpassad inredning,
   - vid varje byte av personal som känner till kombinationen,
   - om kombinationen har röjts eller misstänks ha röjts,
   - om ett lås har genomgått underhållsarbete eller reparation,
   - minst var tolfte månad.

6. Informationssäkerhetsmyndigheten och säkerhetschefen ska ansvara för att dessa regler följs.