Europeiska unionens
officiella tidning

SV
L-serien

2024/1418

24.5.2024

Delegerat beslut nr 19/2024 om genomförandebestämmelser för hantering av uppgifter på säkerhetsskydds-klassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET

EUROPEISKA REVISIONSRÄTTENS FÖRVALTNINGSKOMMITTÉ HAR ANTAGIT DETTA BESLUT,

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

med beaktande av revisionsrättens beslut nr 41/2021 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter ([1]), nedan kallat *beslut nr 41/2021*,

med beaktande av revisionsrättens informationssäkerhetspolicy (för närvarande DEC 127/15 FINAL) och policy för informationsklassificering (personalmeddelande nr 123/20) ([2]),

med beaktande av diskussionerna vid förvaltningskommitténs sammanträde den 18 mars 2024, och

av följande skäl: Beslut nr 41/2021 är tillämpligt med avseende på alla revisionsrättens avdelningar och lokaler.

I artikel 1.3 i beslut nr 41/2021 föreskrivs att 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.

I artiklarna 1.3 och 5.6 i beslut nr 41/2021 föreskrivs att 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, och ett samförståndsavtal undertecknades med kommissionens generaldirektorat för personal och säkerhet den 25 september 2023 om användningen av säkerhetsdirektoratets säkrade utrymmen i Luxemburg.

Säkerhetsåtgärder för att skydda säkerhetsskyddsklassificerade EU-uppgifter under hela deras livscykel ska särskilt anpassas till uppgifternas säkerhetsskyddsklassificering.

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

Enligt artikel 3.3 i beslut nr 41/2021 ska alla säkerhetsskyddsklassificerade EU-uppgifter skyddas genom fysiska säkerhetsåtgärder, och uppgifter på säkerhetsskydds-klassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ska dessutom skyddas genom personalsäkerhetsåtgärder.

I artikel 10.10 i beslut nr 41/2021 föreskrivs att förvaltningskommittén ska anta ett delegerat beslut om tillämpningsföreskrifter, vilka enligt artiklarna 8.1 och 10.1 i beslut nr 41/2021 ska avse frågor som hantering och lagring av säkerhetsskyddsklassificerade EU-uppgifter samt överträdelser av säkerhetsbestämmelserna.

Revisionsrätten har genom beslut nr 41/2021 säkerställt att dess säkerhetsåtgärder för att garantera en hög skyddsnivå för säkerhetsskyddsklassificerade EU-uppgifter 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.

En förenklad administrativ överenskommelse mellan revisionsrätten och kommissionen, rådet och Europeiska utrikestjänsten trädde i kraft den 27 januari 2023.

([1]) EUT L 256, 19.7.2021, s. 106.
([2]) Finns på https://www.eca.europa.eu/sv/legal-framework.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL 1

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte och tillämpningsområde

1. I detta beslut fastställs villkoren för hantering av säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL ([3]) och SECRET UE/EU SECRET ([4]) i enlighet med revisionsrättens beslut nr 41/2021.

2. Detta beslut ska vara tillämpligt med avseende på alla revisionsrättens avdelningar och lokaler. Det är också tillämpligt med avseende på revisionsrättens revisionsavdelningar och kommittéer, vilka omfattas av termen ”avdelningar” i detta beslut.

Artikel 2

Kriterier för tillgång till uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET

1. Tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET får beviljas efter att följande har gjorts:

a) Det har fastställts att en person måste ha tillgång till vissa uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET för att kunna utöva en yrkesfunktion eller utföra uppgifter för revisionsrätten.

b) Personen har informerats om reglerna och relevanta säkerhetsstandarder och riktlinjer för skydd av uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET.

c) Personen har skriftligen bekräftat sitt ansvar för att skydda de berörda uppgifterna.

d) Personen har av revisionsrättens direktör för personalfrågor, ekonomi och allmänna tjänster fått ett säkerhetsgodkännande och beviljats tillgång upp till den angivna nivån och till och med ett angivet datum, i enlighet med artikel 4.4 i beslut nr 41/2021.

2. Revisionsrättens praktikanter ska inte tilldelas arbetsuppgifter som kräver tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET.

3. För andra personalkategorier ska tillgång vägras eller tillåtas i enlighet med tabellen i bilagan.

([3]) Enligt artikel 1.2 a i revisionsrättens beslut nr 41/2021 avses med uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL ”uppgifter och materiel vars obehöriga röjande skulle kunna medföra endast ringa men för Europeiska unionens eller en eller flera medlemsstaters intressen”.

([4]) Enligt artikel 1.2 a i revisionsrättens beslut nr 41/2021 avses med uppgifter på säkerhetsskyddsklassificeringsnivån 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”.

KAPITEL 2

UPPRÄTTANDE AV UPPGIFTER PÅ SÄKERHETSSKYDDSKLASSIFICERINGSNIVÅERNA CONFIDENTIEL UE/EU CONFIDENTIAL OCH SECRET UE/EU SECRET

Artikel 3

Upphovsman

Även om upphovsmannen i den mening som avses i artikel 2 m i beslut nr 41/2021 är en EU-institution, en EU-byrå eller ett EU-organ, en medlemsstat, en tredjestat eller en internationell organisation under vars behörighet säkerhetsskyddsklassificerade uppgifter har upprättats och/eller införts i unionens strukturer, är den som utarbetar uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET inte nödvändigtvis densamma.

Artikel 4

Fastställande av säkerhetsskyddsklassificeringsnivå

1. En handling ska säkerhetsskyddsklassificeras minst på nivån CONFIDENTIEL UE/EU CONFIDENTIAL om dess obehöriga röjande bland annat skulle kunna

a) påtagligt skada diplomatiska förbindelser, det vill säga förorsaka formella protester eller andra sanktioner,

b) äventyra enskilda personers säkerhet och frihet,

c) vålla skada på den operativa effektiviteten eller säkerheten hos medlemsstaternas eller andra medverkande staters utstationerade personal, eller på effektiviteten hos värdefulla säkerhets- eller underrättelseoperationer,

d) avsevärt undergräva den finansiella bärkraftigheten hos större organisationer,

e) hindra brottsutredningar eller göra det lättare att begå allvarliga brott,

f) väsentligt motarbeta unionens eller medlemsstaternas finansiella, monetära, ekonomiska och kommersiella intressen,

g) allvarligt hindra utvecklingen eller genomförandet av unionens viktigare strategier,

h) innebära ett avbrott för eller på annat sätt väsentligt störa betydelsefull unionsverksamhet,

i) leda till upptäckt av uppgifter som placerats på en högre säkerhetsskyddsklassificeringsnivå.

2. Uppgifter ska säkerhetsskyddsklassificeras minst på nivån SECRET UE/EU SECRET om dess obehöriga röjande bland annat skulle kunna

a) skapa internationella spänningar,

b) allvarligt skada förbindelserna med tredjestater eller internationella organisationer,

c) utgöra ett direkt hot mot liv eller allvarligt skada den allmänna ordningen eller den enskildes säkerhet eller frihet,

d) vålla allvarlig skada på den operativa effektiviteten eller säkerheten hos medlemsstaternas eller andra medverkande staters utstationerade personal, eller på den fortsatta effektiviteten hos ytterst värdefulla säkerhets- eller underrättelseoperationer,

e) vålla väsentlig materiell skada på unionens eller medlemsstaternas finansiella, monetära, ekonomiska eller kommersiella intressen,

f) leda till upptäckt av uppgifter som placerats på en högre säkerhetsskyddsklassificeringsnivå.

3. Upphovsmän får besluta att tilldela en standardiserad säkerhetsskyddsklassificeringsnivå till de kategorier av uppgifter som de regelbundet upprättar. De ska dock se till att enskilda uppgifter ges lämplig säkerhetsskyddsklassificeringsnivå.

Artikel 5

Utarbetande av utkast

1. Uppgifter ska säkerhetsskyddsklassificeras så snart de har upprättats. Personliga meddelanden, preliminära utkast eller meddelanden som innehåller uppgifter som motiverar en säkerhetsskyddsklassificering på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska märkas som sådana från början och ska framställas och hanteras i enlighet med detta beslut.

2. Om den ursprungliga säkerhetsskyddsklassificeringsnivån inte längre är motiverad för den slutgiltiga handlingen ska handlingen inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller säkerhetsskyddsklassificeringen hävas efter det att handlingens upphovsman bekräftat att det kan göras utan säkerhetsrisk.

Artikel 6

Register över källmaterial

För att kunna utöva upphovsmannens kontroll i enlighet med artikel 14 nedan ska upphovsmän till handlingar på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET föra register över alla säkerhetsskyddsklassificerade källor som använts för framställning av säkerhetsskyddsklassificerade handlingar, inbegripet uppgifter om källor som ursprungligen kommer från EU:s medlemsstater, internationella organisationer eller tredjeländer. När så är lämpligt ska säkerhetsskyddsklassificerade uppgifter i aggregerad form märkas på ett sådant sätt att uppgifter som identifierar upphovsmännen till säkerhetsskyddsklassificerat källmaterial bevaras.

Artikel 7

Säkerhetsskyddsklassificering av delar av en handling

1. I enlighet med punkt 12 i revisionsrättens policy för informationsklassificering ska en handlings övergripande säkerhetsskyddsklassificeringsnivå minst motsvara den högsta säkerhetsskyddsklassificeringsnivå som tilldelats någon av handlingens delar. När uppgifter från olika källor sammanställs, ska den slutliga handlingen i aggregerad form ses över och dess övergripande säkerhetsskyddsklassificeringsnivå fastställas, eftersom det kan vara motiverat med en högre säkerhetsskyddsklassificeringsnivå för handlingen som helhet än för de enskilda delarna.

2. Handlingar som innehåller både säkerhetsskyddsklassificerade och icke-säkerhetsskyddsklassificerade delar ska struktureras och märkas så att delar på olika klassificerings- och/eller känslighetsnivå vid behov lätt kan identifieras och avskiljas. På så sätt möjliggörs att varje del hanteras på lämpligt sätt när den skilts från de övriga delarna.

Artikel 8

Fullständig säkerhetsskyddsmarkering

1. Uppgifter som motiverar säkerhetsskyddsklassificering ska märkas och hanteras som sådana oberoende av deras fysiska form. Säkerhetsskyddsklassificeringsnivån ska tydligt meddelas till mottagarna, antingen genom en säkerhetsskyddsmarkering, om uppgifterna tillhandahålls i skriftlig form (oavsett om så sker i pappersform, på flyttbara lagringsmedier eller i ett kommunikations- och informationssystem) eller genom ett tillkännagivande, om uppgifterna lämnas i muntlig form (till exempel i ett samtal eller en presentation). Säkerhetsskyddsklassificerat material ska märkas fysiskt så att dess säkerhetsskyddsklassificering lätt kan identifieras.

2. På handlingar ska den fullständiga säkerhetsskyddsmarkeringen CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET skrivas med versaler, på franska och engelska (med franska först), i enlighet med punkt 3. Markeringen ska inte översättas till andra språk.

3. Säkerhetsskyddsmarkeringen CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska placeras

a) centrerat högst upp och längst ned på varje sida i handlingen,

b) med fullständig säkerhetsskyddsmarkering på en rad, utan mellanslag på någondera sidan av snedstrecket,

c) med versaler, i svart, med teckensnittet Times New Roman, storlek 16 (om möjligt, men minst 14) i fetstil, och omgivet av en ram på alla sidor.

4. Vid upprättandet av en handling på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska

a) varje sida tydligt märkas med säkerhetsskyddsklassificeringsnivån,

b) varje sida numreras,

c) handlingen förses med ett referensnummer, ett registreringsnummer och en ämnesuppgift som inte i sig är en säkerhetsskyddsklassificerad uppgift, om den inte getts en sådan märkning,

d) alla bilagor och bifogade handlingar förtecknas, om möjligt på första sidan,

e) datum för upprättande anges på handlingen.

5. Om möjligt ska markeringen SECRET UE/EU SECRET vara röd.

Artikel 9

Förkortade säkerhetsskyddsmarkeringar C-UE/EU-C och S-EU/EU-S

Förkortningarna C-UE/EU-C och S-UE/EU-S får användas för att ange säkerhetsskyddsklassificeringsnivån för enskilda delar av en handling respektive en handling klassificerad som CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET eller där den fullständiga säkerhetsskyddsmarkeringen inte kan placeras, till exempel på ett mindre, flyttbart lagringsmedium. Den får användas i brödtext där upprepad användning av fullständiga säkerhetsskyddsmarkeringar skulle bli svårhanterlig. Förkortningen får inte användas i stället för den fullständiga säkerhetsskyddsmarkeringen i sidhuvudet och sidfoten i handlingen.

Artikel 10

Andra säkerhetsbeteckningar

1. Handlingar på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET får förses med andra markeringar, eller ”säkerhetsbeteckningar”, med uppgift om till exempel det område till vilket handlingen hör eller en särskild spridning på grundval av principen om behovsenlig behörighet. Ett exempel:

RELEASABLE TO LIECHTENSTEIN

2. Handlingar på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET får förses med en säkerhetsvarning med särskilda anvisningar om hur handlingarna ska hanteras och förvaltas.

Om det är möjligt ska alla uppgifter om hävande av säkerhetsskyddsklassificering anges på första sidan i handlingen vid den tidpunkt då den upprättas. Exempelvis kan följande märkning användas:

SECRET UE/EU SECRET until [dd.mm.yyyy] and RESTREINT UE/EU RESTRICTED thereafter

Artikel 11

Elektronisk behandling

1. Handlingar på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET ska upprättas med hjälp av elektroniska medel om sådana finns tillgängliga.

2. Vid upprättandet av uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska revisionsrättens personal använda ett ackrediterat kommunikations- och informationssystem som minst motsvarar säkerhetsskyddsklassificeringsnivån. Om det råder tvivel om vilket kommunikations- och informationssystem som får användas ska revisionsrättens informationssäkerhetsansvariga frågas om råd.

3. Handlingar på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET, inklusive utkast (se artikel 5), får inte sändas med e-post, tryckas eller skannas på standardskrivare eller skannrar, eller hanteras på personliga enheter som tillhör personalen. Endast skrivare eller kopiatorer som är anslutna till fristående datorer med skydd mot elektromagnetisk strålning eller till ett ackrediterat system får användas för att skriva ut handlingar på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET.

Artikel 12

Registrering för säkerhetsändamål

1. Uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska registreras för säkerhetsändamål innan de lämnas ut och när de tas emot. De ska registreras

— när de kommer till eller lämnar det säkrade utrymmet vid kommissionen i Luxemburg för vars användning revisionsrätten har ingått ett samförståndsavtal,

— när de kommer till eller lämnar ett kommunikations- och informationssystem.

2. Registreringen får göras på papper eller i elektroniska loggböcker.

3. Om uppgifterna hanteras elektroniskt i ett kommunikations- och informationssystem kan registreringen också utföras som en del av processer inom själva systemet. I så fall måste kommunikations- och informationssystemet omfatta åtgärder som garanterar registrens integritet.

4. Kontrolltjänstemannen för registreringsenheten ska föra ett register över åtminstone följande uppgifter för varje handling:

a) Datumet när den slutliga säkerhetsskyddsklassificerade handlingen registrerades.

b) Säkerhetsskyddsklassificeringsnivå.

c) I tillämpliga fall, datumet då säkerhetsskyddsklassificeringsnivån upphör att gälla.

d) Namnet på den avdelning där handlingen har sitt ursprung.

e) Mottagaren eller mottagarna.

f) En ämnesuppgift.

g) Referensnummer för handlingen från den avdelning där den har sitt ursprung.

h) Registreringsnummer.

i) Antal distribuerade exemplar.

j) Om möjligt, en logg över de källor som använts för att upprätta handlingen.

k) Datumet för inplacering på lägre säkerhetsskyddsklassificeringsnivå eller då handlingen inte längre är säkerhetsskyddsklassificerad.

l) Uppgifter om förstöring (ort, datum, metod, övervakning, intyg över förstöring).

Artikel 13

Spridning

Sändaren av handlingar på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska besluta till vem uppgifterna ska spridas, på grundval av behovsenlig behörighet. En distributionslista ska upprättas för att se till att principen om behovsenlig behörighet tillämpas korrekt.

KAPITEL 3

ARBETE MED BEFINTLIGA UPPGIFTER PÅ SÄKERHETSSKYDDSKLASSIFICERINGSNIVÅERNA CONFIDENTIEL UE/EU CONFIDENTIAL OCH SECRET UE/EU SECRET

Artikel 14

Upphovsmannens kontroll

1. Upphovsmannen ska ha ”upphovsmannens kontroll” över uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET som han eller hon har upprättat. Upphovsmannens skriftliga förhandsmedgivande ska inhämtas innan

a) uppgifters säkerhetsskyddsklassificering får hävas eller uppgifter inplaceras på lägre säkerhetsskyddsklassificeringsnivå,

b) uppgifter får användas för andra ändamål än dem som fastställts av upphovsmannen,

c) uppgifter får lämnas ut till ett tredjeland eller en internationell organisation,

d) uppgifter får röjas för en part utanför revisionsrätten men inom EU.

2. Innehavare av uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET är vederbörligen bemyndigade personer som har fått tillgång till de säkerhetsskyddsklassificerade uppgifterna för att kunna utföra sina arbetsuppgifter. De ansvarar för att sådana uppgifter hanteras, lagras och skyddas korrekt i enlighet med beslut nr 41/2021. Till skillnad från upphovsmannen har innehavaren av säkerhetsskyddsklassificerade uppgifter inte befogenhet att besluta om att uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska inplaceras på lägre säkerhetsskyddsklassificeringsnivå, inte längre ska vara säkerhetsskyddsklassificerade eller kan lämnas ut.

3. Om upphovsmannen till en uppgift på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET inte kan identifieras, ska den avdelning vid revisionsrätten som innehar de säkerhetsskyddsklassificerade uppgifterna utöva upphovsmannens kontroll. Om innehavaren anser att det är nödvändigt att lämna ut uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET till ett tredjeland eller en internationell organisation, ska revisionsrätten rådgöra med en av parterna i ett informationssäkerhetsavtal med det aktuella tredjelandet eller den aktuella internationella organisationen ([5]).

Artikel 15

Lämpligt kommunikations- och informationssystem för hantering av uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET

1. Uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET ska om möjligt hanteras och överföras elektroniskt. I enlighet med artikel 6 i beslut nr 41/2021 får endast kommunikations- och informationssystem som har ackrediterats av en annan EU-institution, en annan EU-byrå eller ett annat EU-organ eller av revisionsrätten användas för detta ändamål.

Artikel 16

Särskilda åtgärder avseende uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET som lagrats på flyttbara lagringsmedier

1. Användningen av flyttbara lagringsmedier, såsom usb-minnen, cd-skivor, dvd-skivor eller minneskort (inbegripet SSD ([6])), ska hållas strikt kontrollerad och redovisas. Endast flyttbara lagringsmedier som tillhandahållits av revisionsrätten eller av en annan EU-institution, en annan EU-byrå eller ett annat EU-organ och godkänts av revisionsrättens informationssäkerhetsansvariga och krypterats med en produkt som godkänts av de informationssäkerhetsansvariga får användas. Personliga flyttbara lagringsmedier och sådana som delats ut fritt vid konferenser, seminarier osv. får inte användas för överföring av säkerhetsskyddsklassificerade uppgifter. I enlighet med riktlinjerna från revisionsrättens informationssäkerhetsansvariga bör om möjligt Tempest-säkra flyttbara lagringsmedier användas.

([5]) Se artikel 35 för närmare information.

([6]) Solid-state drive, lagringsminne som enbart består av halvledarminne, vanligtvis flashminne.

2. Om en säkerhetsskyddsklassificerad handling hanteras eller lagras elektroniskt på ett flyttbart lagringsmedium, ska säkerhetsskyddsmarkeringen framgå tydligt i själva handlingen, liksom i filnamnet och på det flyttbara lagringsmediet.

3. Personalen ska ha i åtanke att en högre säkerhetsskyddsklassificeringsnivå kan vara motiverad när stora mängder säkerhetsskyddsklassificerade uppgifter lagras på flyttbara lagringsmedier.

4. Endast vederbörligen ackrediterade kommunikations- och informationssystem får användas för att överföra uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET till eller från flyttbara lagringsmedier.

5. Innan sådana uppgifter laddas ner till ett flyttbart lagringsmedium ska särskild omsorg ägnas åt att se till att lagringsmediet inte innehåller virus eller sabotageprogram.

6. Flyttbara lagringsmedier ska i förekommande fall hanteras i enlighet med de säkra driftsmetoder som gäller för det krypteringssystem som används.

7. Handlingar på flyttbara lagringsmedier som antingen inte längre behövs eller som har överförts till ett lämpligt kommunikations- och informationssystem ska avlägsnas eller raderas säkert med hjälp av godkända produkter eller metoder. Om de flyttbara lagringsmedierna inte förvaras i lämpliga säkerhetsskåp ska de förstöras när de inte längre behövs. All förstöring eller radering ska ske i enlighet med revisionsrättens säkerhetsbestämmelser. En inventarieförteckning ska upprättas över flyttbara lagringsmedier, och förstöringen av dem ska registreras.

Artikel 17

Hantering och lagring av uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET

1. I enlighet med artiklarna 5.5 och 5.6 i beslut nr 41/2021 ska uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET hanteras i ett säkrat utrymme ([7]). Revisionsrättens personal kan också få tillgång till sådana uppgifter i säkrade utrymmen vid en annan EU-institution.

2. Enligt artikel 5.6 i beslut nr 41/2021, och om detta specifikt medgivits av upphovsmannen, får dessa uppgifter i undantagsfall hanteras i revisionsrättens administrativa utrymmen ([8]), förutsatt att de säkerhetsskyddsklassificerade EU-uppgifterna skyddas från att obehöriga personer får tillgång till dem.

3. I kristider eller i en nödsituation får dessa uppgifter hanteras utanför ett säkrat eller administrativt utrymme, förutsatt att innehavaren har åtagit sig att vidta kompensationsåtgärder som minst ska omfatta följande:

— Handlingar på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET får inte läsas på offentliga platser.

— Säkerhetsskyddsklassificerade EU-uppgifter ska alltid förvaras under innehavarens personliga kontroll.

— När det gäller handlingar i pappersform måste innehavaren anmäla till registreringsenheten med ansvar för säkerhetsskyddsklassificerade EU-uppgifter, så snart som möjligt och beroende på krisens eller nödsituationens karaktär, att de säkerhetsskyddsklassificerade handlingarna hanteras utanför ett säkrat eller administrativt utrymme.

— Handlingarna ska förvaras i lämpliga säkerhetsskåp när de inte läses eller diskuteras.

— Dörrarna till lokalen ska vara stängda när handlingarna läses eller diskuteras.

— Detaljerna i handlingarna får inte diskuteras på en icke-säkrad telefonlinje eller via e-post.

— Innehavaren får inte kopiera eller skanna handlingarna. Endast registreringsenheten med ansvar för säkerhetsskyddsklassificerade EU-uppgifter får tillhandahålla ytterligare kopior.

([7]) Enligt definitionen i artikel 18 i kommissionens beslut (EU, Euratom) 2015/444 av den 13 mars 2015 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (EUT L 72, 17.3.2015, s. 53).

([8]) Enligt definitionen i bilagan till beslut nr 41/2021.

— Handlingar får hanteras och tillfälligt hållas utanför ett administrativt eller säkrat utrymme endast så länge som det är absolut nödvändigt, och därefter ska de returneras till registreringsenheten med ansvar för säkerhetsskyddsklassificerade EU-uppgifter.

— När handlingarna lämnas tillbaka ska de kvitteras.

— Innehavaren får varken kasta bort de säkerhetsskyddsklassificerade handlingarna eller förstöra dem.

4. Uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET ska förvaras i ett säkrat utrymme, antingen i ett säkerhetsskåp eller i ett valv.

5. Ytterligare rådgivning kan begäras från revisionsrättens informationssäkerhetsansvariga.

6. Alla misstänkta eller faktiska säkerhetsincidenter som inbegriper en handling ska rapporteras till den informationssäkerhetsansvariga så snart som möjligt.

Artikel 18

Kopiering och översättning av uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET

1. Uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET får kopieras eller översättas på uppdrag av innehavaren, förutsatt att upphovsmannen specifikt medgivit detta och inte har angett några begränsningar. Det får dock inte göras fler kopior än vad som är absolut nödvändigt. Revisionsrätten får också be upphovsmannen om att tillhandahålla en kopia som översatts till engelska.

2. Om endast en del av en säkerhetsskyddsklassificerad handling återges ska samma villkor gälla som för kopior av handlingen i sin helhet. Utdrag ska också klassificeras på samma nivå, såvida inte upphovsmannen särskilt har klassificerat dem på en lägre nivå eller markerat att de inte är säkerhetsskyddsklassificerade.

3. De säkerhetsåtgärder som är tillämpliga på de ursprungliga uppgifterna ska också tillämpas på kopior och översättningar av dessa.

Artikel 19

Allmänna principer för befordran av uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET

1. När så är möjligt ska uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET som behöver tas utanför ett säkrat utrymme, eller administrativt utrymme i enlighet med artikel 17.2, överföras på elektronisk väg med hjälp av vederbörligen ackrediterade medel och/eller skyddas med godkända kryptoprodukter.

2. Beroende på de tillgängliga medlen och de särskilda omständigheterna får uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET befordras fysiskt genom personligt överlämnande i pappersform eller på flyttbara lagringsmedier. För att överföra uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET ska användning av flyttbara lagringsmedier ges företräde framför att skicka pappersdokument.

3. I enlighet med artikel 6.8 i beslut nr 41/2021 ska flyttbara lagringsmedier krypteras med en produkt som godkänts för att skydda säkerhetsskyddsklassificerade EU-uppgifter antingen av rådet eller rådets generalsekreterare i dess funktion som kryptogodkännande myndighet eller av en annan EU-institution, en annan EU-byrå eller ett annat EU-organ. Uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET på flyttbara lagringsmedier som inte skyddas av en kryptoprodukt som har godkänts på detta sätt ska hanteras på samma sätt som uppgifter i pappersform.

4. Försändelser får innehålla mer än en säkerhetsskyddsklassificerad EU-uppgift, förutsatt att principen om behovsenlig behörighet följs.

5. De förpackningar som används ska förhindra att innehållet går att se. Uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET ska befordras i dubbla ogenomskinliga förpackningar, till exempel kuvert, ogenomskinliga mappar eller en portfölj. Den yttre förpackningen ska vara försluten och får inte vara försedd med någon uppgift om innehållets karaktär eller dess säkerhetskyddsklassificeringsnivå. Den inre förpackningen ska märkas CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET. På båda förpackningarna anges den avsedda mottagarens namn, tjänstetitel och adress samt en returadress om leveransen inte kan utföras.

6. Personal eller kurirer som befordrar uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska vara säkerhetsbemyndigade och ha ett kuririntyg som utfärdats för dem.

7. Kuvert och förpackningar får inte öppnas under befordran. Säkerhetsgodkännandet för kuriren bemyndigar inte honom eller henne att få tillgång till de säkerhetsskyddsklassificerade uppgifterna i försändelsen.

8. Enligt artikel 5.12 i revisionsrättens beslut 41/2021 får upphovsmannen också ange ytterligare fysiska åtgärder som ska vidtas för att skydda uppgifterna från obehörigt röjande under transporten.

9. Alla misstänkta eller faktiska säkerhetsincidenter som inbegriper uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET som befordras av personal eller kurirer ska rapporteras till den informationssäkerhetsansvariga för vidare utredning så snart som möjligt.

Artikel 20

Personligt överlämnande av flyttbara lagringsmedier

1. Flyttbara lagringsmedier som används för att transportera uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET ska åtföljas av en fraktsedel med uppgifter om de flyttbara lagringsmedierna samt alla filer som finns på dem, så att mottagaren kan göra nödvändiga kontroller och bekräfta mottagandet.

2. Enheterna ska endast lagra de säkerhetsskyddsklassificerade EU-uppgifter som transporteras. Exempelvis måste alla säkerhetsskyddsklassificerade uppgifter på en enskild enhet vara avsedda för en och samma mottagare. Avsändarna bör ha i åtanke att en högre säkerhetsskyddsklassificeringsnivå kan vara motiverad för enheten som helhet när stora mängder säkerhetsskyddsklassificerade uppgifter lagras på sådana enheter.

3. Endast flyttbara lagringsmedier med vederbörlig säkerhetsskyddsmarkering får användas för att befordra uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET.

4. Alla uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET som sparas på flyttbara lagringsmedier ska registreras för säkerhetsändamål.

Artikel 21

Befordran av handlingar på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET inom avdelningar och i revisionsrättens lokaler

1. Säkerhetsbemyndigad personal får befordra handlingar på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET inom avdelningar och i revisionsrättens lokaler, men handlingarna får inte lämnas utan uppsikt av den person som befordrar dem eller läsas offentligt.

2. Handlingar på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET får inte skickas med intern post.

Artikel 22

Befordran av handlingar på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET inom Europeiska unionen

1. Uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET får befordras av personal vid revisionsrätten eller den EU-institution, den EU-byrå eller det EU-organ där handlingen har sitt ursprung eller deras kurirer vart som helst inom unionen, förutsatt att följande anvisningar följs:

a) För befordran av uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET ska ogenomskinliga dubbla kuvert eller förpackningar användas. Den yttre förpackningen ska vara försluten och ska inte vara försedd med någon uppgift om innehållets karaktär eller dess säkerhetsskyddsklassificeringsnivå.

b) Handlingar på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET får inte lämnas utan uppsikt av den person som befordrar dem.

c) Kuvertet eller förpackningen får inte öppnas under befordran och uppgifterna får inte läsas offentligt.

2. Personal vid registreringsenheten som vill skicka uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL till andra platser inom unionen får göra det på ett av följande sätt:

a) Med nationella posttjänster som spårar försändelserna eller kommersiella kurirtjänster som garanterar personlig befordran, förutsatt att de uppfyller kraven i artikel 24 i detta beslut.

b) Med militär-, regerings- eller diplomatkurir, i samarbete med registratorskontorets personal.

3. Personal som vill skicka uppgifter på säkerhetsskyddsklassificeringsnivån SECRET UE/EU SECRET till andra EU-medlemsstater måste komma överens med kontrolltjänstemannen för registreringsenheten om att de skickas med militär-, regerings- eller diplomatkurir och inte med post eller kommersiella kurirer.

4. All personal vid revisionsrätten eller alla officiella kurirer som befordrar uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska medföra ett kuririntyg för varje försändelse. Intyget ska utfärdas av kontrolltjänstemannen för registreringsenheten och ange att personen är bemyndigad att befordra försändelsen.

Artikel 23

Befordran av uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET från eller till ett tredjelands territorium

1. Uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET får befordras av personal vid revisionsrätten eller den EU-institution där handlingen har sitt ursprung mellan unionens territorium och ett tredje lands territorium genom personligt överlämnande.

2. Registreringsenhetens personal får sörja för befordran med militär- eller diplomatkurir.

3. Personal som befordrar pappersdokument eller flyttbara lagringsmedier på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET genom personligt överlämnande, ska vidta samtliga följande ytterligare åtgärder:

— När de reser med kollektivtrafik ska de placera de säkerhetsskyddsklassificerade uppgifterna i en portfölj eller väska över vilken de har personlig uppsikt. Portföljen eller väskan får inte befordras som lastrumsbagage.

— Den inre förpackningen ska vara försedd med en officiell försegling som visar att det rör sig om en officiell försändelse som inte ska genomgå säkerhetskontroll.

— Den person som befordrar försändelsen ska medföra ett kuririntyg, utfärdat av kontrolltjänstemannen för registreringsenheten, som anger att han eller hon har tillstånd att befordra försändelsen med säkerhetsskyddsklassificeringen CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET.

Artikel 24

Befordran med kommersiella kurirer

1. I detta beslut avses med ”kommersiella kurirer” nationella posttjänster och kommersiella kurirföretag som tillhandahåller en tjänst med hjälp av vilken uppgifter levereras mot en avgift, antingen med personligt överlämnande eller med spårning.

2. Kommersiella kurirer får överföra uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL inom en EU-medlemsstat eller mellan två medlemsstater. Kommersiella kurirer får överföra uppgifter på säkerhetsskyddsklassificeringsnivån SECRET UE/EU SECRET inom en medlemsstat men inte utomlands.

3. Kommersiella kurirtjänster ska uppmanas att leverera försändelser på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET endast till kontrolltjänstemannen för registreringsenheten, deras vederbörligen bemyndigade ersättare eller till den avsedda mottagaren.

4. Kommersiella kurirer får använda sig av en underleverantörs tjänster. Ansvaret för att följa detta beslut ska dock kvarstå hos kurirföretaget.

Artikel 25

Förberedelse av säkerhetsskyddsklassificerade EU-uppgifter för befordran med kommersiella kurirtjänster

1. När säkerhetsskyddsklassificerade försändelser förbereds ska avsändarna ha i åtanke att kommersiella kurirtjänster endast får leverera försändelser på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET till kontrolltjänstemannen för registreringsenheten, dennes vederbörligen bemyndigade ersättare eller till den avsedda mottagaren.

2. Försändelser med uppgifter som skickas via en godkänd kommersiell kurirtjänst ska förberedas och förpackas enligt följande:

a) Uppgifterna ska vara placerade i ett ogenomskinligt dubbelt kuvert (innerkuvertet ska vara sådant att eventuella försök att öppna det blir uppenbara) eller annat lämpligt säkert emballage.

b) Säkerhetsskyddsklassificeringsnivån ska vara tydligt märkt på innerkuvertet eller på innerförpackningen.

c) Den yttre förpackningen ska vara försluten och ska inte vara försedd med någon säkerhetskyddsmarkering.

d) Både inner- och ytterkuvertet eller inner- och ytterförpackningen ska vara tydligt adresserade till en namngiven person hos den avsedda mottagaren och vara försedda med en returadress.

e) En blankett för mottagningsbevis ska placeras inuti innerkuvertet eller innerförpackningen för mottagaren att fylla i och returnera. Mottagningsbeviset, som inte ska säkerhetsskyddsklassificeras, ska vara försett med handlingens referensnummer, datum och exemplarnummer, men får inte ange ämnet.

f) Ytterkuvertet eller ytterförpackningen måste förses med ett leveranskvitto. Leveranskvittot, som inte ska säkerhetsskyddsklassificeras, ska vara försett med handlingens referensnummer, datum och exemplarnummer, men får inte ange ämnet.

g) Kurirtjänsten måste på en särskild blankett inhämta och förse avsändaren med bevis på att försändelsen har levererats, eller införskaffa kvitton eller försändelsenummer.

3. Innan försändelsen skickas iväg ska avsändaren komma överens med den namngivna mottagaren om ett lämpligt datum och klockslag för leverans.

4. Avsändaren är ensam ansvarig för försändelser som sänds via en kommersiell kurirtjänst. Om försändelsen kommer bort eller inte levereras i tid ska avsändaren informera den informationssäkerhetsansvariga och kontrolltjänstemannen för registreringsenheten, som följer upp säkerhetsincidenten.

Artikel 26

Andra särskilda hanteringsvillkor

1. Alla ytterligare villkor för befordran som anges i ett informationssäkerhetsavtal eller i administrativa överenskommelser ska uppfyllas. I tveksamma fall ska personalen samråda med den informationssäkerhetsansvariga eller kontrolltjänstemannen för registreringsenheten.

2. Kravet på dubbla förpackningar får frångås för säkerhetsskyddsklassificerade uppgifter som skyddas med godkända kryptoprodukter. För adresseringen, och eftersom flyttbara lagringsmedier ska vara försedda med en uttrycklig säkerhetsskyddsmarkering, ska de dock transporteras i minst ett förslutet ogenomskinligt kuvert med, i förekommande fall, ytterligare fysiska skyddsåtgärder, till exempel kuvert av bubbelplast.

KAPITEL 4

SÄKERHETSSKYDDSKLASSIFICERADE MÖTEN

Artikel 27

Förbereda ett möte där uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska behandlas

1. Möten vid vilka uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIEL eller SECRET UE/EU SECRET ska diskuteras får endast hållas i en möteslokal som har godkänts på vederbörlig eller högre säkerhetsskyddsklassificeringsnivå. Revisionsrätten får använda möteslokaler i säkrade utrymmen vid en annan EU-institution. Om sådana inte är tillgängliga ska personalen rådgöra med revisionsrättens informationssäkerhetsansvariga.

2. Som regel bör dagordningarna inte säkerhetsskyddsklassificeras. Om en dagordning för ett möte innehåller uppgifter om säkerhetsskyddsklassificerade handlingar, ska själva dagordningen inte automatiskt säkerhetsskyddsklassificeras. Punkterna på dagordningen ska formuleras på ett sådant sätt att unionens eller medlemsstaternas intressen inte äventyras.

3. Mötesarrangörerna ska påminna deltagarna om att alla synpunkter som lämnas in rörande en punkt på dagordningen där uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET behandlas inte får skickas med e-post eller på något annat sätt som inte har ackrediterats på vederbörligt sätt i enlighet med artikel 11 i detta beslut.

4. Mötesarrangörerna ska sträva efter att gruppera punkter där uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET behandlas efter varandra på dagordningen för att mötet ska fungera smidigt. Endast personer med behovsenlig behörighet, som har ett personalsäkerhetsgodkännande på vederbörlig säkerhetsskyddsklassificeringsnivå och är vederbörligen bemyndigade, får närvara vid diskussioner om säkerhetsskyddsklassificerade punkter.

5. I mötesinbjudningar måste deltagarna förvarnas om att säkerhetsskyddsklassificerade ämnen kommer att tas upp på dagordningen och att lämpliga säkerhetsåtgärder kommer att tillämpas.

6. Mötesarrangörerna ska påminna deltagarna om att bärbara elektroniska enheter ska lämnas utanför möteslokalen vid diskussioner om punkter på dagordningen där uppgifter på säkerhetsskyddsklassificeringsnivå CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET behandlas.

7. Mötesarrangörerna ska i förväg utarbeta en fullständig förteckning över deltagare. I enlighet med artikel 4.6 i beslut nr 41/2021 ska de också i god tid informera den informationssäkerhetsansvariga om datum, tidpunkt och plats för dessa möten samt om vilka som kommer att delta vid mötena.

Artikel 28

Deltagarnas tillträde till ett möte där uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET behandlas

1. Mötesarrangörerna ska underrätta revisionsrättens informationssäkerhetsansvariga och kontrolltjänstemannen för registreringsenheten om eventuella externa besökare som kommer att närvara vid ett möte som revisionsrätten arrangerar där uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET behandlas.

2. Deltagarna måste bevisa att de innehar ett giltigt personalsäkerhetsgodkännande på vederbörlig säkerhetsskyddsklassificeringsnivå för att tillåtas närvara vid behandlingen av punkter där uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET behandlas.

Artikel 29

Elektronisk utrustning i möteslokaler där uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET behandlas

Endast ackrediterade it-system i enlighet med artikel 11 i detta beslut får användas om uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET förmedlas till exempel inom ramen för en presentation eller en videokonferens.

Artikel 30

Förfaranden som ska följas vid ett möte där uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET behandlas

1. När en diskussion rörande säkerhetsskyddsklassificerade uppgifter inleds ska ordföranden tillkännage att mötet övergår till att behandla säkerhetsskyddsklassificerade uppgifter. Dörrarna ska vara stängda.

2. Endast det nödvändiga antalet handlingar ska kvitteras och ges till deltagare och, i förekommande fall, tolkar, vid början av diskussionen.

3. Handlingar på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET får inte lämnas utan uppsikt under avbrott i mötet.

4. Vid mötets slut ska deltagarna och tolkarna påminnas om att inte lämna några säkerhetsskyddsklassificerade handlingar eller säkerhetsskyddsklassificerade anteckningar som de kan ha gjort obevakade i lokalen. Eventuella handlingar på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET som deltagarna inte behöver efter mötets slut, och alla handlingar som använts av tolkarna, ska kvitteras och returneras till kontrolltjänstemannen för registreringsenheten för förstöring i vederbörliga dokumentförstörare ([9]).

5. En deltagarförteckning och en sammanfattning av alla säkerhetsskyddsklassificerade uppgifter som delats med medlemsstaterna och muntligen lämnats ut till tredjeländer eller internationella organisationer ska sammanställas under mötet och inkluderas i lägesrapporten från mötet.

Artikel 31

Tolkar och översättare

Endast tolkar och översättare som har säkerhetsgodkännande och bemyndigande samt omfattas av tjänsteföreskrifterna eller anställningsvillkoren för övriga anställda i Europeiska unionen ([10]) eller som har ett avtalsförhållande med revisionsrätten eller en annan EU-institution ska ha tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET.

([9]) Se artikel 42.6 för närmare information.

([10]) Förordning nr 31 (EEG) om tjänsteföreskrifter för tjänstemän och anställningsvillkor för övriga anställda, i dess ändrade lydelse (EGT 45, 14.6.1962, s. 1385/62) (ELI: http://data.europa.eu/eli/reg/1962/31(1)/2023-01-01).

KAPITEL 5

DELNING OCH UTBYTE AV UPPGIFTER PÅ SÄKERHETSSKYDDSKLASSIFICERINGSNIVÅN CONFIDENTIEL UE/EU CONFIDENTIAL OCH SECRET UE/EU SECRET

Artikel 32

Upphovsmannens medgivande

Om det inte är revisionsrätten som är upphovsman till de säkerhetsskyddsklassificerade uppgifter som är föremål för en begäran om utlämning eller delning, eller eventuellt källmaterial de kan innehålla, ska den avdelning vid revisionsrätten som innehar de säkerhetsskyddsklassificerade uppgifterna först söka upphovsmannens skriftliga medgivande till att lämna ut uppgifterna. Om upphovsmannen till en uppgift inte kan identifieras ska den avdelning vid revisionsrätten som innehar dessa säkerhetsskyddsklassificerade uppgifter utöva upphovsmannens kontroll.

Artikel 33

Delning av uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET med andra unionsenheter

1. Uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET får endast delas med en annan EU-institution, en annan EU-byrå eller ett annat EU-organ om mottagaren har behovsenlig behörighet och enheten har en motsvarande juridisk överenskommelse med revisionsrätten.

2. Inom revisionsrätten ska registreringsenheten med ansvar för säkerhetsskyddsklassificerade EU-uppgifter som regel fungera som huvudsaklig kontaktpunkt för in- och utpassering när det gäller utbyte av säkerhetsskyddsklassificerade EU-uppgifter med andra EU-institutioner, EU-byråer och EU-organ.

Artikel 34

Utbyte av uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET med medlemsstater

1. Uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET får delas med medlemsstaterna om mottagaren har behovsenlig behörighet och har fått ett säkerhetsgodkännande.

2. Säkerhetsskyddsklassificerade uppgifter från medlemsstater som har en motsvarande nationell säkerhetsskyddsmarkering ([11]) och som tillhandahållits revisionsrätten ska ha samma skyddsnivå som uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET.

Artikel 35

Utbyte av uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET med tredjeländer och internationella organisationer

1. Uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET får endast lämnas ut till ett tredjeland eller en internationell organisation om mottagaren har behovsenlig behörighet och landet eller den internationella organisationen har upprättat en lämplig rättslig eller administrativ ram, till exempel ett informationssäkerhetsavtal eller en administrativ överenskommelse med revisionsrätten. Bestämmelserna i varje sådant avtal eller sådan överenskommelse ska ha företräde framför bestämmelserna i detta beslut.

2. Registreringsenheten med ansvar för säkerhetsskyddsklassificerade EU-uppgifter ska som regel fungera som huvudsaklig kontaktpunkt för in- och utpassering när det gäller utbyte av alla uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET mellan revisionsrätten och tredjeländer eller internationella organisationer.

([11]) En jämförelsetabell över medlemsstaternas säkerhetsskyddsmarkeringar återfinns i bilaga I till beslut (EU, Euratom) 2015/444.

3. Alla säkerhetsskyddsklassificerade uppgifter som mottas från ett tredjeland eller en internationell organisation ska registreras för säkerhetsändamål. Personalen ska därför kontakta registreringsenheten med ansvar för säkerhetsskyddsklassificerade EU-uppgifter om de tar emot säkerhetsskyddsklassificerade uppgifter via andra än registreringsenhetens vanliga kanaler.

4. För att säkerställa spårbarhet ska uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET registreras

— när de kommer till eller lämnar ett säkrat utrymme,

— när de kommer till eller lämnar ett kommunikations- och informationssystem.

5. Registreringen får göras på papper eller i elektroniska loggböcker.

6. Registreringsförfaranden för säkerhetsskyddsklassificerade uppgifter som hanteras i ett ackrediterat kommunikations- och informationssystem kan ingå som en del av processer inom själva systemet. I så fall ska kommunikations- och informationssystemet omfatta åtgärder som garanterar loggregistrens integritet.

7. Säkerhetsskyddsklassificerade uppgifter som mottas från ett tredjeland eller en internationell organisation ska ges en motsvarande skyddsnivå som säkerhetsskyddsklassificerade EU-uppgifter som har motsvarande säkerhetsskyddsmarkering i enlighet med relevanta informationssäkerhetsavtal eller administrativa överenskommelser.

Artikel 36

ad hoc-utlämning i undantagsfall av uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET

1. Om revisionsrätten eller någon av dess avdelningar fastställer att det finns ett exceptionellt behov av att lämna ut uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET till ett tredjeland, en internationell organisation eller en EU-enhet, men det saknas ett informationssäkerhetsavtal eller en administrativ överenskommelse, ska förfarandet för *ad hoc*-utlämning i undantagsfall följas.

2. Revisionsrättens avdelningar ska kontakta revisionsrättens informationssäkerhetsansvariga och upphovsmannen. Revisionsrätten ska rådgöra med en av parterna i ett informationssäkerhetsavtal med det aktuella tredjelandet, den aktuella internationella organisationen eller den aktuella EU-enheten.

3. Efter denna rådfrågning får revisionsrättens kollegium, på grundval av ett förslag från generalsekreteraren, tillåta att de berörda uppgifterna lämnas ut.

KAPITEL 6

UPPHÖRANDE AV UPPGIFTERS SÄKERHETSSKYDDSKLASSIFICERING PÅ NIVÅERNA CONFIDENTIEL UE/EU CONFIDENTIAL OCH SECRET UE/EU SECRET

Artikel 37

Beslut att uppgifter ska inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre vara säkerhetsskyddsklassificerade

1. Uppgifter ska vara säkerhetsskyddsklassificerade endast så länge de kräver skydd. Inplacering på lägre säkerhetsskyddsklassificeringsnivå innebär en sänkning av nivån på säkerhetsskyddsklassificeringen. Beslut att uppgifter inte längre ska vara säkerhetsskyddsklassificerade innebär att de inte längre ska betraktas som säkerhetsskyddsklassificerade över huvud taget. I samband med upprättandet av säkerhetsskyddsklassificerade EU-uppgifter ska upphovsmannen om möjligt ange huruvida uppgifterna kan inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre ska vara säkerhetsskyddsklassificerade från ett visst datum eller efter en särskild händelse. Annars ska upphovsmannen se över uppgifterna och bedöma riskerna minst vart femte år för att avgöra om den ursprungliga säkerhetsskyddsklassificeringsnivån fortfarande är lämplig.

2. Även för revisionsrättens handlingar kan beslut fattas från fall till fall att de ska inplaceras på lägre säkerhetsskyddsklassificeringsnivå eller inte längre vara säkerhetsskyddsklassificerade, till exempel efter en begäran om tillgång till en handling från allmänheten.

Artikel 38

Ansvar för beslut att uppgifter ska inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre vara säkerhetsskyddsklassificerade

1. Beslut att uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET ska inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre vara säkerhetsskyddsklassificerade får inte fattas utan medgivande från upphovsmannen.

2. Den avdelning vid revisionsrätten som upprättade en säkerhetsskyddsklassificerad handling ska ansvara för att besluta huruvida den kan inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre ska vara säkerhetsskyddsklassificerad. Vid revisionsrätten ska en begäran om beslut om att en handling ska inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre ska vara säkerhetsskyddsklassificerad föregås av samråd med avdelningschefen eller direktören för den avdelning där den har sitt ursprung, eller den uppgiftsansvariga. Om avdelningen har sammanställt säkerhetsskyddsklassificerade uppgifter från olika källor ska den först inhämta samtycke från alla andra parter som tillhandahållit källmaterial, inbegripet i medlemsstaterna, andra EU-organ, tredjeländer eller internationella organisationer.

3. Om den avdelning inom revisionsrätten där handlingen har sitt ursprung inte längre finns och dess ansvar har överförts till en annan avdelning, ska beslutet att uppgifter ska inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre vara säkerhetsskyddsklassificerade fattas av denna avdelning. Om den avdelning där handlingen har sitt ursprung inte längre finns och dess ansvar inte har överförts, ska beslutet att uppgifter ska inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre vara säkerhetsskyddsklassificerade fattas gemensamt av revisionsrättens direktörer.

4. Den avdelning som ansvarar för uppgifters inplacering på en lägre säkerhetsskyddsklassificeringsnivå eller för att de inte längre ska vara säkerhetsskyddsklassificerade ska samarbeta med registreringsenheten med ansvar för säkerhetsskyddsklassificerade EU-uppgifter om de praktiska arrangemangen för detta.

Artikel 39

Känsliga uppgifter som inte är säkerhetsskyddsklassificerade

När en översyn av en handling leder till ett beslut att den inte längre ska vara säkerhetsskyddsklassificerad ska hänsyn tas till huruvida handlingen ska markeras som innehållande känsliga icke-säkerhetsskyddsklassificerade uppgifter i den mening som avses i punkt 16 i revisionsrättens policy för informationsklassificering ([12]) och punkt 4 i riktlinjerna för klassificering och hantering av icke-säkerhetsskyddsklassificerade
EU-uppgifter.

Artikel 40

Angivande av att en handling har placerats in på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre är säkerhetsskyddsklassificerad

1. Den ursprungliga säkerhetsskyddsmarkeringen högst upp och längst ned på varje sida ska tydligt strykas över (inte tas bort) med hjälp av funktionen ”genomstrykning” för elektroniska format eller manuellt för utskrifter.

2. Första sidan (försättsbladet) ska förses med en markering att handlingen har placerats in på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre är säkerhetsskyddsklassificerad, kompletterad med uppgifter om den myndighet som ansvarar för beslutet om detta och datum.

3. De ursprungliga mottagarna av uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET ska underrättas om att uppgifterna har placerats in på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre är säkerhetsskyddsklassificerade. De ursprungliga mottagarna ska ansvara för att underrätta eventuella efterföljande mottagare till vilka de har översänt eller för vilka de har kopierat de ursprungliga uppgifterna på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET.

4. Revisionsrättens arkivtjänst ska underrättas om alla beslut om att EU-uppgifter eller handlingar inte längre ska vara säkerhetsskyddsklassificerade.

5. Alla översättningar av säkerhetsskyddsklassificerade uppgifter ska omfattas av samma förfaranden för att uppgifterna ska placeras in på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre ska vara säkerhetsskyddsklassificerade som den ursprungliga språkversionen.

([12]) Finns på https://www.eca.europa.eu/sv/legal-framework.

Artikel 41

Partiell inplacering på lägre säkerhetsskyddsklassificeringsnivå eller partiellt hävande av säkerhetsskyddsklassificeringen för uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET

1. Det är också möjligt att besluta om partiell inplacering på lägre säkerhetsskyddsklassificeringsnivå eller partiellt hävande av säkerhetsskyddsklassificeringen (till exempel bilagor eller endast vissa punkter). Förfarandet ska vara identiskt med förfarandet för inplacering på lägre säkerhetsskyddsklassificeringsnivå eller för att en handling i sin helhet inte längre ska vara säkerhetsskyddsklassificerad.

2. När ett beslut har fattats om partiellt borttagande av säkerhetsskyddsklassificeringen för uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska ett utdrag göras av de delar av handlingen som omfattas av beslutet om partiellt hävande av säkerhetsskyddsklassificeringen

3. I det utdrag som inte längre ska vara säkerhetsskyddsklassificerat ska de delar som förblir säkerhetsskyddsklassificerade ersättas med följande:

PART NOT TO BE DECLASSIFIED

antingen i brödtexten, om den del som förblir säkerhetsskyddsklassificerad är en del av en punkt, eller som en punkt, om den del som förblir klassificerad omfattar en eller mer än en hel punkt.

4. Ett särskilt omnämnande ska göras i texten om säkerhetsskyddsklassificeringen för en hel bilaga inte kan hävas och denna därför inte ingår i utdraget.

Artikel 42

Rutinmässig förstöring och radering av uppgifter på säkerhetsskydds klassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET

1. Revisionsrätten ska inte ansamla stora mängder säkerhetsskyddsklassificerade uppgifter.

2. De avdelningar där uppgifterna har sitt ursprung ska se över handlingarna minst vart femte år för förstöring eller radering. Detta ska tillämpas med jämna mellanrum både på uppgifter i pappersform och på uppgifter som lagras i kommunikations- och informationssystem.

3. Personalen får inte förstöra handlingar i pappersformat på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET som de inte längre behöver, utan ska i stället be kontrolltjänstemannen för registreringsenheten förstöra handlingarna, med förbehåll för eventuella arkiveringsbestämmelser för originalhandlingen.

4. Personalen behöver inte informera upphovsmannen om de raderar kopior av handlingar på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET.

5. Utkast till material som innehåller säkerhetsskyddsklassificerade uppgifter ska omfattas av samma metoder för bortskaffande som slutliga säkerhetsskyddsklassificerade handlingar.

6. Endast godkända dokumentförstörare ska användas för att förstöra handlingar på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET. Dokumentförstörare i säkerhetsklass 5 enligt standarden DIN 66399 är lämpliga för att förstöra handlingar på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL. Dokumentförstörare i säkerhetsklass 6 enligt standarden DIN 66399 är lämpliga för att förstöra handlingar på säkerhetsskyddsklassificeringsnivån SECRET UE/EU SECRET.

7. Avfallet från godkända dokumentförstörare får bortskaffas som vanligt kontorsavfall.

8. Kontrolltjänstemannen för registreringsenheten ska upprätta intyg om förstöring och uppdatera loggböckerna och andra registreringsuppgifter i enlighet med detta.

9. Alla medier och enheter som innehåller uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska saneras på vederbörligt sätt när de blivit uttjänta. Elektroniska uppgifter ska förstöras eller raderas från it-resurser och tillhörande lagringsmedier på ett sätt som ger rimliga garantier för att uppgifterna inte kan återvinnas. Genom saneringen avlägsnas all data från lagringsenheterna liksom alla märkningar, markeringar och aktivitetsloggar.

10. Lagringsmedier för datorer ska ges till den informationssäkerhetsansvariga för förstöring och bortskaffande efter att kontrolltjänstemannen för registreringsenheten har informerats.

Artikel 43

Evakuering och förstöring av uppgifter på säkerhetsskydd sklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET i en nödsituation

1. I enlighet med samförståndsavtalet mellan revisionsrätten och kommissionens generaldirektorat för personal och säkerhet om användningen av säkerhetsdirektoratets säkrade utrymmen ska kommissionens fastställda förfarande för skyddande av säkerhetsskyddsklassificerade uppgifter i en nödsituation tillämpas. Vid behov kommer den lokala säkerhetsansvariga vid kommissionens säkerhetsdirektorat i Luxemburg att ha tillgång till revisionsrättens säkerhetsskåp för att tillämpa kommissionens fastställda förfarande i en nödsituation och aktivera planer för evakuering och förstöring i nödsituationer för att skydda säkerhetsskyddsklassificerade EU-uppgifter som vid en kris löper stor risk att falla i händerna på obehöriga. I prioritetsordning och beroende på nödsituationens karaktär ska följande åtgärder beaktas:

i) Flytta säkerhetsskyddsklassificerade EU-uppgifter till en alternativ säker plats, om möjligt ett säkrat utrymme i samma byggnad.

ii) Evakuera säkerhetsskyddsklassificerade EU-uppgifter till en alternativ säker plats, om möjligt ett säkrat utrymme i en annan byggnad, om möjligt en EU-institution.

iii) Förstöra säkerhetsskyddsklassificerade EU-uppgifter, om möjligt med användning av godkända metoder för förstöring.

2. Om planerna i händelse av en nödsituation har aktiverats ska prioritet ges åt att flytta eller förstöra uppgifter på säkerhetsskyddsklassificeringsnivå SECRET UE/EU SECRET först och därefter CONFIDENTIEL UE/EU CONFIDENTIAL.

3. De operativa detaljerna i planerna för evakuering och förstöring i nödsituationer ska vara säkerhetsskyddsklassificerade på nivån RESTREINT UE/EU RESTRICTED. En kopia ska finnas i varje säkerhetsskåp där uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET brukar förvaras, så att den är tillgänglig i en nödsituation.

Artikel 44

Arkivering

1. Beslut om huruvida och när arkivering ska ske, och vilka motsvarande praktiska åtgärder som ska vidtas, ska fattas i enlighet med revisionsrättens informationssäkerhetspolicy, policy för informationsklassificering och arkiveringspolicy.

2. Handlingar på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET får inte skickas till Europeiska unionens historiska arkiv i Florens.

KAPITEL 7

SLUTBESTÄMMELSER

Artikel 45

Öppenhet

Revisionsrättens personal och övriga personer som berörs ska informeras om detta beslut, som ska offentliggöras i *Europeiska unionens officiella tidning*.

Artikel 46

Ikraftträdande

När förvaltningskommittén har antagit detta beslut träder det i kraft dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Luxemburg den 19 mars 2024.

På revisionsrättens förvaltningskommittés vägnar
Tony MURPHY
Ordförande

BILAGA

Personalkategorier som vid behov kan få tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET för att utföra sina arbetsuppgifter

Kategorier av personal vid revisionsrätten	Tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET	Villkor
Ledamöter	ja	Information + bekräftelse
Tjänstemän	ja	Säkerhetsprövning + information + bekräftelse + bemyndigande + behovsenlig behörighet
Tillfälligt anställda	ja	Säkerhetsprövning + information + bekräftelse + bemyndigande + behovsenlig behörighet
Kontraktsanställda	ja	Säkerhetsprövning + information + bekräftelse + bemyndigande + behovsenlig behörighet
Utstationerade nationella experter från EU:s medlemsstater	ja	Endast om de godkänts av ursprungsmedlemsstaterna innan de tillträder sin tjänst + information från revisionsrätten + bekräftelse + bemyndigande av revisionsrätten + behovsenlig behörighet
Praktikanter	nej	Inga undantag möjliga
Övriga personalkategorier (anställda via bemanningsföretag, extern personal som arbetar internt osv.)	nej	Inga undantag möjliga