

BESLUT

DOMSTOLENS BESLUT (EU) 2016/2386

av den 20 september 2016

om säkerhetsbestämmelser för upplysningar eller handlingar som har getts in till tribunalen enligt artikel 105 i dess rättegångsregler

DOMSTOLEN HAR BESLUTAT FÖLJANDE

med beaktande av rättegångsreglerna, särskilt artikel 190a.5, och

av följande skäl:

- (1) En part kan enligt artikel 105.1 och 105.2 i tribunalens rättegångsregler, på eget initiativ eller till följd av en åtgärd för bevisupptagning som beslutats av tribunalen, ge in upplysningar och handlingar som berör unionens säkerhet eller en eller flera av dess medlemsstaters säkerhet eller deras internationella förbindelser. Det förfarande som föreskrivs i artikel 105.3–105.10 ska tillämpas på sådana upplysningar eller handlingar.
- (2) Mot bakgrund av att de berörda upplysningarna eller handlingarna är av känslig eller konfidentiell natur kräver tillämpningen av artikel 105 i tribunalens rättegångsregler att det införs lämpliga säkerhetsbestämmelser som garanterar en hög skyddsnivå för dessa upplysningar eller handlingar.
- (3) Säkerhetsbestämmelserna ska tillämpas på samtliga upplysningar eller handlingar som har getts in enligt artikel 105.1 eller 105.2 i tribunalens rättegångsregler, när dessa utgör säkerhetsskyddsklassificerade EU-uppgifter eller när den part som har gett in dem har angett att det skulle skada unionens säkerhet eller dess medlemsstaters säkerhet eller deras internationella förbindelser om dessa upplysningar eller handlingar kommunicerades med den andra parten, även om de inte utgör säkerhetsskyddsklassificerade EU-uppgifter.
- (4) För att säkerställa en hög skyddsnivå för dessa upplysningar eller handlingar, ska de grundläggande principer och miniminormer för säkerhet som gäller för skydd av nämnda upplysningar eller handlingar grunda sig på de principer och normer som gäller för skydd av uppgifter på säkerhetsskyddsklassificeringsnivån SECRET UE/EU SECRET enligt EU-institutionernas bestämmelser om skydd för säkerhetsskyddsklassificerade EU-uppgifter, särskilt de bestämmelser som antagits av Europeiska unionens råd, Europaparlamentet och Europeiska kommissionen.
- (5) Upplysningar eller handlingar som har getts in enligt artikel 105.1 eller 105.2 i tribunalens rättegångsregler ska förses med en markering som är specifik för Europeiska unionens domstol. Denna ska vara "FIDUCIA". Markeringen bestämmer vilka säkerhetsbestämmelser som ska gälla för upplysningarna eller handlingarna under hela rättegången vid tribunalen och, om avgörandet överklagas, vid domstolen. Anbringandet av FIDUCIA-markeringen och borttagandet av densamma ska inte påverka klassificeringen av uppgifter som lämnas till tribunalen.
- (6) Tillgång till FIDUCIA-uppgifter ska ges i överensstämmelse med behovsprincipen.

Artikel 1

Definitioner

I detta beslut avses med

- a) *säkerhetsmyndighet*: den myndighet som är ansvarig för säkerheten vid Europeiska unionens domstol och som utsetts av denna, vilken helt eller delvis får delegera utförandet av de uppgifter som föreskrivs i detta beslut,
- b) *FIDUCIA-enheten*: den enhet vid Europeiska unionens domstol som har ansvar för att hantera FIDUCIA-uppgifter,
- c) *innehavare*: vederbörligen behörig person som på grundval av ett konstaterat behov förfogar över en FIDUCIA-uppgift och därmed ansvarar för dess skydd,

- d) *handling*: alla slags uppgifter, oavsett fysisk form eller fysiska egenskaper,
- e) *uppgift*: alla slags skriftliga eller muntliga uppgifter, oavsett på vilket lagringsmedium de finns eller från vem de härrör,
- f) *säkerhetsskyddsklassificerade EU-uppgifter*: alla slags uppgifter eller all slags materiel som placerats på en EU-säkerhetsskyddsklassificeringsnivå enligt de bestämmelser som gäller inom EU-institutionerna och som omfattas av en av följande sekretessgrader:
 - TRÈS SECRET UE/EU TOP SECRET
 - SECRET UE/EU SECRET
 - CONFIDENTIEL UE/EU CONFIDENTIAL
 - RESTREINT UE/EU RESTRICTED,
- g) *FIDUCIA-uppgift*: uppgift som är försedd med FIDUCIA-markering,
- h) *behandling* av en FIDUCIA-uppgift: alla åtgärder som FIDUCIA-uppgifter kan bli föremål för under rättegången vid domstolen. Sådana åtgärder innefattar att FIDUCIA-uppgifter registreras, att någon tar del av dem, att sådana uppgifter skapas, kopieras, lagras, återlämnas och förstörs.

Artikel 2

Syfte och tillämpningsområde

1. I detta beslut fastställs de grundläggande principer och miniminormer för säkerhet som ska gälla för skydd av FIDUCIA-uppgifter under rättegången vid domstolen.
2. Dessa grundläggande principer och miniminormer för säkerhet ska gälla för alla FIDUCIA-uppgifter. De ska gälla för all skriftlig eller muntlig användning av sådana uppgifter samt för kopior som kan komma att göras av dem i enlighet med de säkerhetsbestämmelser som fastställs i detta beslut.

Artikel 3

Hur ingivande och återlämnande ska ske

Vid tillämpning av säkerhetsbestämmelserna i detta beslut gäller följande:

- Parten ska underrätta tribunalens kansli om dagen för ingivande av upplysningar eller handlingar enligt artikel 105.1 eller 105.2 i tribunalens rättegångsregler.
- Parten, som ska åtföljas av en företrädare för tribunalens kansli, är skyldig att ge in upplysningarna eller handlingarna enligt artikel 105.1 eller 105.2 i nämnda rättegångsregler till FIDUCIA-enheten under den tid då kansliet är öppet för allmänheten.
- Den part som har gett in upplysningarna eller handlingarna enligt artikel 105.1 eller 105.2 i tribunalens rättegångsregler är skyldig att hämta dem hos FIDUCIA-enheten i närvaro av en företrädare för tribunalens kansli när parten inte ger sitt tillstånd till att upplysningarna eller handlingarna kommuniceras med den andra parten enligt artikel 105.4 i nämnda rättegångsregler, när de dras tillbaka enligt artikel 105.7 i samma rättegångsregler eller så snart den frist som avses i artikel 56 första stycket i stadgan för Europeiska unionens domstol har löpt ut, såvida inte ett överklagande har getts in inom nämnda frist.
- Om tribunalens avgörande överklagas inom den frist som avses i artikel 56 första stycket i stadgan för Europeiska unionens domstol, ska de upplysningar eller handlingar som har getts in i det målet enligt artikel 105.1 eller 105.2 i tribunalens rättegångsregler göras tillgängliga för domstolen. Så snart tribunalens justitiesekreterare underrättas om att avgörandet har överklagats, ska han eller hon därför skicka en skrivelse till domstolens justitiesekreterare och underrätta honom eller henne om att de berörda upplysningarna eller handlingarna är tillgängliga för domstolen. Tribunalens justitiesekreterare ska samtidigt underrätta säkerhetsmyndigheten om att de berörda upplysningarna eller handlingarna ska göras tillgängliga för domstolen, dock utan att upplysningarna eller handlingarna förflyttas fysiskt. Denna underrättelse ska registreras av FIDUCIA-enheten. Den part som har gett in upplysningarna eller handlingarna är skyldig att hämta dem hos FIDUCIA-enheten, i närvaro av en företrädare för domstolens kansli, så snart delgivning har skett av det avgörande genom vilket målet om överklagande avgörs slutligt, förutom om målet återförvisas till tribunalen för fortsatt handläggning.

- Om målet återförvisas till tribunalen, ska domstolen göra de berörda upplysningarna eller handlingarna tillgängliga för tribunalen så snart delgivning har skett av det avgörande genom vilket målet om överklagande avgörs slutligt. Domstolens justitiesekreterare ska för detta ändamål skicka en skrivelse till tribunalens justitiesekreterare och underrätta honom eller henne om att de berörda upplysningarna eller handlingarna är tillgängliga för tribunalen. Domstolens justitiesekreterare ska samtidigt underrätta säkerhetsmyndigheten om att de berörda upplysningarna eller handlingarna ska göras tillgängliga för tribunalen, dock utan att upplysningarna eller handlingarna förflyttas fysiskt. Denna underrättelse ska registreras av FIDUCIA-enheten. Den part som har gett in upplysningarna eller handlingarna är skyldig att hämta dem hos FIDUCIA-enheten i närvaro av en företrädare för tribunalens kansli, så snart den frist som avses i artikel 56 första stycket i stadgan för Europeiska unionens domstol har löpt ut, såvida inte ett överklagande har getts in inom nämnda frist.

Artikel 4

FIDUCIA-markering

1. FIDUCIA-enheten ska förse samtliga upplysningar eller handlingar som har getts in i enlighet med artikel 105.1 eller 105.2 i tribunalens rättegångsregler med en FIDUCIA-markering.
2. Även uppgifter som helt eller delvis återger innehållet i upplysningar eller handlingar som har getts in i enlighet med artikel 105.1 eller 105.2 i nämnda rättegångsregler samt kopior av sådana upplysningar eller handlingar ska föras med en FIDUCIA-markering av FIDUCIA-enheten.
3. Även handlingar och register som FIDUCIA-enheten har upprättat med stöd av detta beslut och vars obehöriga röjande skulle kunna skada Europeiska unionens eller en eller flera av dess medlemsstaters väsentliga intressen eller deras internationella förbindelser ska föras med en FIDUCIA-markering av FIDUCIA-enheten.
4. FIDUCIA-markeringen ska anbringas synligt på alla sidor och lagringsmedier som innehåller FIDUCIA-uppgifter.
5. Anbringandet av FIDUCIA-markeringen och borttagandet av densamma, på de villkor som anges i bilaga III, ska inte påverka klassificeringen av uppgifter som lämnas till tribunalen.

Artikel 5

Skydd av FIDUCIA-uppgifter

1. FIDUCIA-uppgifter ska ha ett skydd som är likvärdigt det som ges säkerhetsskyddsklassificerade EU-uppgifter på nivå *SECRET UE/EU SECRET* enligt de bestämmelser som gäller inom EU-institutionerna i fråga om skydd för säkerhetsskyddsklassificerade EU-uppgifter.
2. En innehavare av FIDUCIA-uppgifter ska vara ansvarig för att skydda dessa uppgifter i enlighet med detta beslut.

Artikel 6

Hantering av säkerhetsrisker

1. De risker som hotar FIDUCIA-uppgifterna ska hanteras genom en riskanalysprocess. Syftet med denna är att identifiera kända säkerhetsrisker, fastställa säkerhetsåtgärder som ska minska riskerna till en acceptabel nivå i enlighet med de grundläggande principer och miniminormer som anges i detta beslut och att tillämpa dessa åtgärder. Säkerhetsmyndigheten ska kontinuerligt utvärdera åtgärdernas effektivitet.
2. Säkerhetsåtgärder för att skydda FIDUCIA-uppgifter under rättegången vid domstolen ska stå i proportion särskilt till uppgifternas eller materielens form och volym, till FIDUCIA-enhetens lokalers omgivning och struktur samt till det lokalt bedömda hotet från fientlig och/eller brottslig verksamhet, inklusive spionage, sabotage och terroristverksamhet.
3. Europeiska unionens domstols interna beredskapsplan ska beakta behovet att skydda FIDUCIA-uppgifter i krislägen för att förhindra att obehöriga får tillgång till dem eller att de obehörigen röjs samt att uppgifternas skick eller tillgänglighet försämras.

4. Åtgärder av förebyggande och återställande karaktär för att reducera effekterna av allvarliga driftsstörningar eller tillbud, på behandling och lagring av FIDUCIA-uppgifter, ska ingå i Europeiska unionens domstols interna beredskapsplan.

Artikel 7

Säkerhetsåtgärder rörande personer

1. Tillgång till FIDUCIA-uppgifter får endast beviljas personer som
 - har behov av att känna till dem,
 - är behöriga att ha tillgång till FIDUCIA-uppgifter, om inte annat följer av punkt 2,
 - och har upplysts om sitt ansvar.
2. Domarna och generaladvokaterna i domstolen ska i kraft av sin tjänst anses ha behörighet för tillgång till FIDUCIA-uppgifter.
3. Förfarandet för att fastställa huruvida en tjänsteman eller annan anställd vid Europeiska unionens domstol, med beaktande av vederbörandes lojalitet, tillförlitlighet och pålitlighet, kan ges behörighet för tillgång till FIDUCIA-uppgifter anges i bilaga I.
4. Alla berörda personer ska, innan de ges behörighet för tillgång till FIDUCIA-uppgifter och därefter regelbundet, upplysas om sitt ansvar att skydda FIDUCIA-uppgifter i enlighet med detta beslut och ska avge en skriftlig ansvarsförklaring.

Artikel 8

Fysisk säkerhet

1. Med "fysisk säkerhet" avses tillämpningen av fysiska och tekniska skyddsåtgärder för att hindra obehörig tillgång till FIDUCIA-uppgifter.
2. Fysiska säkerhetsåtgärder ska vara avsedda att förhindra intrång i FIDUCIA-enhetens lokaler i hemlighet eller genom tvång, att förhindra, upptäcka och avskräcka från otillåtna handlingar och att göra det möjligt att göra åtskillnad mellan personer med respektive utan behörighet för tillgång till FIDUCIA-uppgifter utifrån behovsprincipen. Sådana åtgärder ska fastställas utifrån en riskhanteringsprocess.
3. Fysiska säkerhetsåtgärder ska vidtas med avseende på de lokaler hos FIDUCIA-enheten där FIDUCIA-uppgifter behandlas och lagras. Åtgärderna ska vara avsedda att säkerställa ett skydd som är likvärdigt det som ges säkerhets-skyddsklassificerade EU-uppgifter på nivån SECRET UE/EU SECRET enligt de bestämmelser som gäller inom EU-institutionerna i fråga om skydd för säkerhetsskyddsklassificerade EU-uppgifter. Inga FIDUCIA-uppgifter får lagras och ingen får ta del av sådana uppgifter utanför de lokaler hos FIDUCIA-enheten som har inrättats i detta syfte inom en säkerhetszon.
4. Endast utrustning eller anordningar som överensstämmer med de bestämmelser som gäller inom EU-institutionerna i fråga om skydd för säkerhetsskyddsklassificerade EU-uppgifter ska användas för att skydda FIDUCIA-uppgifter.
5. Genomförandebestämmelser till denna artikel fastställs i bilaga II.

Artikel 9

Hantering av FIDUCIA-uppgifter

1. Med "hantering av FIDUCIA-uppgifter" avses tillämpning av administrativa åtgärder som syftar till att skydda FIDUCIA-uppgifter under rättegången vid domstolen, och till att kontrollera dem för att förebygga och upptäcka att sådana uppgifter avsiktligt eller oavsiktligt röjs eller går förlorade.
2. Åtgärder som vidtas i samband med hantering av FIDUCIA-uppgifter avser särskilt de omständigheterna att sådana uppgifter registreras, att någon tar del av dem, att sådana uppgifter skapas, kopieras, lagras, återlämnas och förstörs.

3. FIDUCIA-enheten ska registrera FIDUCIA-uppgifter när de kommer in. Ingen behandling av uppgifterna får ske innan registrering skett.
4. Säkerhetsmyndigheten ska regelbundet inspektera FIDUCIA-enhetens lokaler.
5. Genomförandebestämmelser till denna artikel fastställs i bilaga III.

Artikel 10

Skydd av elektroniskt behandlade FIDUCIA-uppgifter

1. Informations- och kommunikationssystem (datorer och kringutrustning) som används för behandling av FIDUCIA-uppgifter ska befinna sig i FIDUCIA-enhetens lokaler. De ska vara isolerade från samtliga datanätverk.
2. Säkerhetsåtgärder ska vidtas för att skydda IT-utrustning som används för behandling av FIDUCIA-uppgifter mot att sådana uppgifter röjs genom oavsiktliga elektromagnetiska läckor (säkerhetsåtgärder motsvarande de som gäller för säkerhetsskyddsklassificerade EU-uppgifter på nivån SECRET UE/EU SECRET enligt de bestämmelser som gäller inom EU-institutionerna i fråga om skydd för säkerhetsskyddsklassificerade EU-uppgifter).
3. Informations- och kommunikationssystemen ska ackrediteras av säkerhetsmyndigheten. Myndigheten ska se till att systemen överensstämmer med de bestämmelser som gäller inom EU-institutionerna i fråga om skydd för säkerhetsskyddsklassificerade EU-uppgifter.
4. Genomförandebestämmelser till denna artikel fastställs i bilaga IV.

Artikel 11

Säkerhet när utomstående personer vidtar åtgärder

1. Med "säkerhet när utomstående personer vidtar åtgärder" avses tillämpning av åtgärder som syftar till att säkerställa att leverantörer som måste utföra underhållsarbete på de från datanätverket isolerade informations- och kommunikationssystemen skyddar FIDUCIA-uppgifterna eller att sådana uppgifter skyddas vid åtgärder som innebär att FIDUCIA-uppgifterna skyndsamt måste bortföras och placeras på ett säkert ställe.
2. Säkerhetsmyndigheten får anförtro utförandet av uppgifter, som enligt ett kontrakt innefattar eller kräver tillgång till FIDUCIA-uppgifter, åt leverantörer som är registrerade i en medlemsstat.
3. Säkerhetsmyndigheten ska se till att de miniminormer för säkerhet som fastställs i detta beslut, och som det hänvisas till i kontraktet, följs vid kontraktstilldelning.
4. Personer som är anställda av en leverantör får ha tillgång till FIDUCIA-uppgifter endast om de har getts sådan behörighet av säkerhetsmyndigheten på grundval av ett personalsäkerhetsgodkännande som utfärdats av den nationella säkerhetsmyndigheten eller någon annan behörig säkerhetsmyndighet i enlighet med nationella lagar och andra författningar.
5. Genomförandebestämmelser till denna artikel fastställs i bilaga V.

Artikel 12

Förbud mot digital spridning, utlämning och utbyte av FIDUCIA-uppgifter

1. FIDUCIA-uppgifter får inte spridas digitalt.
2. Domstolen ska inte översända FIDUCIA-uppgifter till unionens institutioner, organ, kontor eller byråer. Den ska inte heller översända sådana uppgifter till medlemsstaterna, övriga rättegångsdeltagare eller till tredje man.

*Artikel 13***Säkerhetsöverträdelser och röjande av FIDUCIA-uppgifter**

1. Med säkerhetsöverträdelse avses en persons handling eller underlåtenhet som står i strid med säkerhetsbestämmelserna i detta beslut.
2. Med röjande av FIDUCIA-uppgifter avses att FIDUCIA-uppgifter till följd av en säkerhetsöverträdelse röjs helt eller delvis till personer som inte är, eller inte anses vara, behöriga personer.
3. Alla säkerhetsöverträdelser, även misstänkta sådana, ska omedelbart rapporteras till säkerhetsmyndigheten.
4. Om det är känt eller om det föreligger rimliga skäl att anta att FIDUCIA-uppgifter har röjts eller gått förlorade, ska säkerhetsmyndigheten, i nära samarbete med domstolens ordförande och justitiesekreterare, vidta lämpliga åtgärder i enlighet med tillämpliga bestämmelser för att
 - a) underrätta den part som har gett in de berörda upplysningarna eller handlingarna om detta,
 - b) begära att den behöriga myndigheten ska inleda en administrativ undersökning,
 - c) uppskatta den skada som kan ha uppkommit för unionens säkerhet eller en eller flera av dess medlemsstaters säkerhet eller deras internationella förbindelser,
 - d) förhindra att händelsen upprepas, och
 - e) underrätta behöriga myndigheter om de vidtagna åtgärderna.
5. Den som gjort sig skyldig till en säkerhetsöverträdelse ska bli föremål för disciplinåtgärder i enlighet med tillämpliga bestämmelser. Den som bär ansvaret för att FIDUCIA-uppgifter har röjts eller gått förlorade ska bli föremål för disciplinåtgärder och/eller kan bli föremål för rättsliga åtgärder i enlighet med tillämpliga bestämmelser.

*Artikel 14***Säkerhetsorganisationen inom domstolen**

1. FIDUCIA-enheten ska genomföra skyddet av FIDUCIA-uppgifter i enlighet med detta beslut.
2. Säkerhetsmyndigheten ska vara ansvarig för att detta beslut tillämpas på ett korrekt sätt. Säkerhetsmyndigheten ska därvid
 - a) tillämpa Europeiska unionens domstols säkerhetspolicy och regelbundet ompröva den,
 - b) utöva tillsyn över FIDUCIA-enhetens tillämpning av detta beslut,
 - c) i förekommande fall låta utreda, på de villkor som anges i artikel 13, inträffade eller misstänkta fall av röjande eller förlust av FIDUCIA-uppgifter, och
 - d) regelbundet inspektera de säkerhetsarrangemang som ska skydda FIDUCIA-uppgifterna i FIDUCIA-enhetens lokaler.

*Artikel 15***Praktiska genomförandebestämmelser**

Praktiska genomförandebestämmelser till detta beslut ska fastställas av säkerhetsmyndigheten i samråd med domstolens justitiesekreterare.

*Artikel 16***Ikraftträdande**

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

Luxemburg den 20 september 2016.

A. CALOT ESCOBAR
Justitiesekreterare

K. LENAERTS
Ordförande

BILAGA I

SÄKERHETSÅTGÄRDER RÖRANDE PERSONER

1. Denna bilaga innehåller genomförandebestämmelser till artikel 7.
2. Det ankommer på domstolens justitiesekreterare att upprätta en förteckning – för sitt vidkommande och i den mån det är strikt nödvändigt – över de tjänster som kräver tillgång till FIDUCIA-uppgifter och som därmed innebär att de tjänstemän eller andra anställda som innehar de aktuella tjänsterna vid domstolen måste ges behörighet att ha tillgång till FIDUCIA-uppgifter.
3. När FIDUCIA-enheten vill ge en tjänsteman eller annan anställd behörighet för tillgång till FIDUCIA-uppgifter, ska den översända det av vederbörande ifyllda frågeformuläret till den nationella säkerhetsmyndigheten i den medlemsstat där han eller hon är medborgare eller till annan behörig nationell myndighet – angiven i de bestämmelser som gäller inom EU-institutionerna i fråga om skydd för säkerhetsskyddsklassificerade EU-uppgifter (nedan kallad *den behöriga nationella säkerhetsmyndigheten*) – och begära att det görs en säkerhetsprövning för sekretessgraden SECRET UE/EU SECRET.
4. När den behöriga nationella säkerhetsmyndigheten har gjort säkerhetsprövningen ska den, i enlighet med gällande lagar och andra författningar i den aktuella medlemsstaten, delge FIDUCIA-enheten slutsatserna från prövningen.
5. Om resultatet av säkerhetsprövningen är att den behöriga nationella säkerhetsmyndigheten har fått försäkran om att ingenting negativt som skulle kunna ifrågasätta personens lojalitet, tillförlitlighet och pålitlighet är känt, får den behöriga tillsättningsmyndigheten bevilja personen i fråga behörighet för tillgång till FIDUCIA-uppgifter.
6. Om resultatet av säkerhetsprövningen är att den behöriga nationella säkerhetsmyndigheten inte har fått en sådan försäkran som avses i punkt 5, ska tillsättningsmyndigheten underrätta personen i fråga om detta. I sådant fall får FIDUCIA-enheten, på uppdrag av tillsättningsmyndigheten, be den behöriga nationella säkerhetsmyndigheten om kompletterande upplysningar som den kan lämna enligt sina nationella lagar och andra författningar. Om resultatet av säkerhetsprövningen bekräftas får behörighet för tillgång till FIDUCIA-uppgifter inte beviljas.
7. Behörighet för tillgång till FIDUCIA-uppgifter gäller i fem år. Behörigheten ska återkallas om personen i fråga lämnar den tjänst som kräver tillgång till FIDUCIA-uppgifter eller om tillsättningsmyndigheten anser att det finns skäl att återkalla behörigheten.
8. Behörighet för tillgång till FIDUCIA-uppgifter får förnyas i enlighet med förfarandet i punkterna 3–5.
9. FIDUCIA-enheten ska föra ett register över beslut att bevilja behörighet för tillgång till FIDUCIA-uppgifter.
10. Om FIDUCIA-enheten får kännedom om uppgifter om att en person med behörighet för tillgång till FIDUCIA-uppgifter utgör en säkerhetsrisk, ska FIDUCIA-enheten underrätta den behöriga nationella säkerhetsmyndigheten om detta, och tillsättningsmyndigheten får besluta att personen i fråga tills vidare inte ska ha tillgång till FIDUCIA-uppgifter eller återkalla behörigheten för tillgång till sådana uppgifter.
11. I brådskande fall får tillsättningsmyndigheten, efter att ha hört den behöriga nationella säkerhetsmyndigheten och om inget annat följer av resultaten av de preliminära kontrollerna för att fastställa att inga negativa uppgifter har framkommit, besluta att berörda tjänstemän eller andra anställda tillfälligt ska ges behörighet för tillgång till FIDUCIA-uppgifter. Denna tillfälliga behörighet gäller fram till dess att förfarandet i punkterna 3–5 har avslutats, dock inte längre än sex månader från det att begäran om säkerhetsprövning gavs in till den behöriga nationella säkerhetsmyndigheten.
12. Personer med behörighet för tillgång till FIDUCIA-uppgifter ska innan de ges tillgång till sådana uppgifter genomgå en utbildning, så att de ska kunna fullgöra sitt ansvar i samband med behandling av FIDUCIA-uppgifter. En persons behörighet för tillgång till FIDUCIA-uppgifter ska inte börja gälla förrän han eller hon har genomgått nämnda utbildning och har avgett en skriftlig ansvarsförklaring.

BILAGA II

FYSISK SÄKERHET

I. INLEDNING

1. Denna bilaga innehåller genomförandebestämmelser till artikel 8. Här anges miniminormer för fysiskt skydd av de lokaler hos FIDUCIA-enheten där FIDUCIA-uppgifter behandlas och lagras.
2. Fysiska säkerhetsåtgärder ska utformas för att hindra obehörig tillgång till FIDUCIA-uppgifter. Dessa åtgärder ska
 - a) säkerställa att FIDUCIA-uppgifter behandlas och lagras på lämpligt sätt,
 - b) göra det möjligt att göra åtskillnad mellan personer med respektive utan behörighet för tillgång till FIDUCIA-uppgifter utifrån behovsprincipen,
 - c) vara ägnade att förhindra, upptäcka och avskräcka från otillåtna handlingar, och
 - d) förhindra eller försena intrång i hemlighet eller genom tvång i FIDUCIA-enhetens lokaler.
3. Fysiska säkerhetsåtgärder ska väljas på grundval av en bedömning av de hot som föreligger mot FIDUCIA-uppgifterna. Åtgärderna ska ta hänsyn till FIDUCIA-enhetens lokalers omgivning och struktur. Säkerhetsmyndigheten ska fastställa vilken grad av säkerhet som ska uppnås för var och en av följande fysiska åtgärder:
 - a) En inhägnad som skyddar gränsen för säkerhetszonen.
 - b) Intrångsdetekteringssystem som är kopplat till säkerhetscentralen vid Europeiska unionens domstol.
 - c) Ett elektroniskt eller elektromekaniskt system för tillträdeskontroll som sköts av en säkerhetsvakt.
 - d) Säkerhetspersonal som är utbildad, står under tillsyn och har behörighet för tillgång till FIDUCIA-uppgifter.
 - e) Ett slutet videoövervakningssystem som sköts av säkerhetspersonalen och som är kopplat till intrångsdetekteringssystemet och tillträdeskontrollsystemet.
 - f) Säkerhetsbelysning som möjliggör en effektiv direkt bevakning eller bevakning via ett videoövervakningssystem.
 - g) Alla andra lämpliga fysiska åtgärder för att avskräcka från eller upptäcka obehörigt tillträde, eller för att förhindra att någon tar del av FIDUCIA-uppgifter eller att sådana uppgifter går förlorade eller skadas.

II. LOKALER FÖR ATT LAGRA OCH TA DEL AV FIDUCIA-UPPGIFTER

Inrättande av fysiskt skyddade lokaler för att lagra och ta del av FIDUCIA-uppgifter

4. Skyddade lokaler för att lagra och ta del av FIDUCIA-uppgifter ska inrättas. FIDUCIA-uppgifter får endast lagras i FIDUCIA-enhetens lokaler och det ska endast vara möjligt att ta del av sådana uppgifter i dessa lokaler. Lokalerna ska i alla avseenden överensstämma med de bestämmelser som gäller inom EU-institutionerna i fråga om skydd för säkerhetsskyddsklassificerade EU-uppgifter.
5. Inne i lokalerna ska FIDUCIA-uppgifter lagras i säkerhetsskåp, vilka i alla avseenden ska överensstämma med de bestämmelser som gäller inom EU-institutionerna i fråga om skydd för säkerhetsskyddsklassificerade EU-uppgifter.
6. Inga kommunikationssystem (telefoner eller andra elektroniska apparater) får föras in i FIDUCIA-enhetens lokaler.
7. FIDUCIA-enhetens sammanträdesrum ska vara skyddat mot avlyssning. Inspektioner för att kontrollera den elektroniska säkerheten ska ske regelbundet.

Tillträde till lokaler som används för att lagra och ta del av FIDUCIA-uppgifter

8. Tillträde till FIDUCIA-enhetens lokaler ska kontrolleras genom en videoövervakad säkerhetssluss med identifieringskontroll.
9. Personer med behörighet för tillgång till FIDUCIA-uppgifter och personer som ska anses ha sådan behörighet har tillträde till FIDUCIA-enhetens lokaler för att ta del av FIDUCIA-uppgifter på de villkor som anges i artikel 7.1 och 7.2 i detta beslut.
10. Säkerhetsmyndigheten får i undantagsfall utfärda ett tillträdestillstånd till obehöriga personer som måste utföra arbete i FIDUCIA-enhetens lokaler. Detta gäller under förutsättning att tillträdet till lokalerna inte innebär tillgång till FIDUCIA-uppgifter, vilka ska vara inlåsta i säkerhetsskåpen medan arbetena utförs. Nämda personer kan endast få tillträde till lokalerna om de åtföljs av en person från FIDUCIA-enheten med behörighet för tillgång till FIDUCIA-uppgifter, som hela tiden ska hålla personerna under uppsyn.
11. Alla inpasseringar i FIDUCIA-enhetens lokaler ska antecknas i ett tillträdesregister. Registret ska föras på en arbetsstation i lokalerna. Det informations- och kommunikationssystem som används för detta ändamål ska överensstämma med de säkerhetskrav som anges i artikel 10 i beslutet samt i bilaga IV.
12. De säkerhetsåtgärder som gäller vid skriftlig användning av FIDUCIA-uppgifter ska tillämpas vid muntlig användning av dessa uppgifter.

III. KONTROLL AV NYCKLAR OCH KOMBINATIONER SOM ANVÄNDS FÖR ATT SKYDDA FIDUCIA-UPPGIFTER

13. Säkerhetsmyndigheten ska fastställa förfaranden för hantering av nycklar och kombinationer till FIDUCIA-enhetens lokaler och säkerhetsskåp. Dessa förfaranden ska skydda mot obehörigt tillgång.
 14. Kombinationer ska memoreras av lägsta möjliga antal personer som behöver känna till dem. Kombinationerna till säkerhetsskåpen för lagring av FIDUCIA-uppgifter ska bytas ut
 - a) vid mottagande av ett nytt säkerhetsskåp,
 - b) vid varje byte av personal som känner till kombinationen,
 - c) vid inträffade eller misstänkta fall av röjande,
 - d) när ett lås har genomgått underhållsarbete eller reparation, och
 - e) minst var tolfte månad.
 15. Teknisk utrustning avsedd för fysiskt skydd av FIDUCIA-uppgifter ska överensstämma med de bestämmelser som gäller inom EU-institutionerna i fråga om skydd för säkerhetsskyddsklassificerade EU-uppgifter. Säkerhetsmyndigheten ska ansvara för att dessa bestämmelser följs.
 16. Den tekniska utrustningen ska inspekteras och underhållas regelbundet. Vid underhållsarbetet ska inspektionsresultaten beaktas för att säkerställa att utrustningen kontinuerligt fungerar på bästa sätt.
 17. Vid varje inspektion ska det göras en ny utvärdering av de enskilda säkerhetsåtgärdernas och det övergripande säkerhetssystemets effektivitet.
-

BILAGA III

HANTERING AV FIDUCIA-UPPGIFTER

I. INLEDNING

1. Denna bilaga innehåller genomförandebestämmelser till artikel 9. Här anges de administrativa åtgärder som syftar till att skydda FIDUCIA-uppgifter under rättegången vid domstolen och till att kontrollera dem för att förebygga och upptäcka att sådana uppgifter avsiktligt eller oavsiktligt röjs eller går förlorade.

II. REGISTER ÖVER FIDUCIA-UPPGIFTER

2. Ett register över FIDUCIA-uppgifter ska inrättas. Registret ska föras av FIDUCIA-enheten på en arbetsstation i FIDUCIA-enhetens lokaler. Det informations- och kommunikationssystem som används för detta ändamål ska överensstämja med de säkerhetskrav som anges i artikel 10 i beslutet samt i bilaga IV.

III. REGISTRERING AV FIDUCIA-UPPGIFTER

3. I detta beslut avses med registrering för säkerhetsändamål (nedan kallat *registrering*) tillämpning av förfaranden som gör det möjligt att följa FIDUCIA-uppgifternas livscykel, inbegripet förstöring av sådana uppgifter.
4. Registrering av FIDUCIA-uppgifter ska göras av FIDUCIA-enheten.
5. FIDUCIA-enheten ska automatiskt förse upplysningar eller handlingar som har getts in enligt artikel 105.1 eller 105.2 i tribunalens rättegångsregler med en FIDUCIA-markering. FIDUCIA-enheten ska registrera en FIDUCIA-uppgift i registret över FIDUCIA-uppgifter.
6. FIDUCIA-enheten ska upprätta en rapport som ska fogas till registret över FIDUCIA-uppgifter och däri ange under vilka omständigheter uppgiften har tagits emot. Uppgiften ska därefter behandlas på det sätt som anges i punkt 5.
7. Registrering i enlighet med punkterna 5 och 6 av en FIDUCIA-uppgift i registret över FIDUCIA-uppgifter ska inte påverka registreringen av inkommande handlingar i mål som görs av personer vid kansliet med behörighet för tillgång till FIDUCIA-uppgifter.

IV. HANTERING AV FIDUCIA-UPPGIFTER

Markering

8. När en säkerhetsskyddsklassificerad EU-uppgift eller annan uppgift ges in enligt artikel 105.1 eller 105.2 i tribunalens rättegångsregler med angivande av att kommunikering av uppgiften skulle skada unionens säkerhet eller en eller flera av dess medlemsstaters säkerhet eller deras internationella förbindelser, ska FIDUCIA-enheten förse uppgiften med FIDUCIA-markering.
9. FIDUCIA-markeringen ska vara tydligt och korrekt angiven på varje del av en handling, oavsett i vilken form uppgiften ges in (pappersform, ljudform, elektronisk form eller annan form).

Skapande av en FIDUCIA-uppgift

10. Endast personer med behörighet för tillgång till FIDUCIA-uppgifter eller personer som ska anses ha sådan behörighet får skapa en FIDUCIA-uppgift på det sätt som anges i artikel 4.2 och 4.3 i detta beslut.
11. Skapade FIDUCIA-uppgifter ska registreras av FIDUCIA-enheten i registret över FIDUCIA-uppgifter.
12. Vad som anges om behandling av FIDUCIA-uppgifter i detta beslut och i dess bilagor gäller även skapade FIDUCIA-uppgifter.

Borttagande av FIDUCIA-markering

13. FIDUCIA-markeringen ska tas bort från FIDUCIA-uppgifter i följande två fall:
 - a) När den part som har gett in FIDUCIA-uppgiften tillåter att den kommuniceras med den andra parten, ska FIDUCIA-markeringen tas bort från den ursprungligen ingivna uppgiften och samtliga uppgifter som skapats på grundval av den uppgiften.
 - b) När FIDUCIA-uppgiften återlämnas till den part som har gett in den.
14. Borttagandet av FIDUCIA-markeringen ska göras av FIDUCIA-enheten som också ska registrera borttagandet i registret över FIDUCIA-uppgifter.
15. Borttagande av FIDUCIA-markering ska inte medföra att säkerhetsskyddsklassificerade EU-uppgifter förlorar sin säkerhetsskyddsklassificering.

V. KOPIOR AV FIDUCIA-UPPGIFTER

16. Kopior av FIDUCIA-uppgifter får bara göras om det är absolut nödvändigt. I sådant fall ska FIDUCIA-enheten göra kopiorna samt numrera och registrera dem.
17. Samtliga säkerhetsbestämmelser i detta beslut och i dess bilagor ska tillämpas på sådana kopior.

VI. FÖRSTÖRING AV FIDUCIA-UPPGIFTER

18. När upplysningar eller handlingar som har getts in i enlighet med artikel 105.1 eller 105.2 i tribunalens rättegångsregler återlämnas till den part som har gett in dem, ska samtliga uppgifter som helt eller delvis återger innehållet i sådana upplysningar eller handlingar samt eventuella kopior av dem förstöras.
19. Förstöring av FIDUCIA-uppgifter, i den mening som avses i punkt 18, ska utföras av FIDUCIA-enheten. Den ska vid förstöringen använda metoder som överensstämmer med de bestämmelser som gäller inom EU-institutionerna i fråga om skydd för säkerhetsskyddsklassificerade EU-uppgifter för att förhindra att uppgifterna återskapas helt eller delvis.
20. Förstöring av FIDUCIA-uppgifter, i den mening som avses i punkt 18, ska utföras i närvaro av ett vittne med behörighet för tillgång till FIDUCIA-uppgifter.
21. FIDUCIA-enheten ska upprätta ett förstöringsprotokoll.
22. Förstöringsprotokollet ska fogas till registret över FIDUCIA-uppgifter. En kopia av protokollet ska tillställas den part som har gett in den aktuella handlingen.

BILAGA IV

SKYDD AV ELEKTRONISKT BEHANDLADE FIDUCIA-UPPGIFTER

1. Denna bilaga innehåller genomförandebestämmelser till artikel 10.
2. FIDUCIA-uppgifter får endast behandlas på elektroniska apparater (arbetsstationer, skrivare, kopieringsapparater) som inte är anslutna till datanätverket och som är belägna i FIDUCIA-enhetens lokaler.
3. Samtliga elektroniska apparater som används för behandling av FIDUCIA-uppgifter ska överensstämma med de bestämmelser som gäller inom EU-institutionerna i fråga om skydd för säkerhetsskyddsklassificerade EU-uppgifter. Apparaternas säkerhet ska säkerställas genom hela deras livscykel.
4. Samtliga möjliga anslutningar till internet och till andra enheter (LAN, WLAN, Bluetooth, etc.) ska vara permanent avaktiverade.
5. Arbetsstationerna ska vara utrustade med ett lämpligt antiviruskydd. Antivirusuppdateringar ska ske med hjälp av en cd-rom eller USB-sticka som ska användas enbart för detta ändamål.
6. Skrivarnas och kopieringsapparaternas minnen ska raderas före varje underhållsåtgärd.
7. Enbart kryptoprodukter som godkänts i enlighet med de bestämmelser som gäller inom EU-institutionerna i fråga om skydd för säkerhetsskyddsklassificerade EU-uppgifter ska användas för att behandla en sådan begäran om säkerhetsprövning som avses i bilaga I.

BILAGA V

SÄKERHET NÄR UTOMSTÅENDE PERSONER VIDTAR ÅTGÄRDER

1. Denna bilaga innehåller genomförandebestämmelser till artikel 11.
2. Leverantörer får endast ha tillgång till FIDUCIA-uppgifter i samband med underhållsarbeten på de från datanätverket isolerade informations- och kommunikationssystemen eller vid åtgärder som innebär att FIDUCIA-uppgifterna skyndsamt måste bortföras och placeras på ett säkert ställe.
3. Säkerhetsmyndigheten ska utarbeta riktlinjer i fråga om säkerheten när utomstående personer vidtar åtgärder. Dessa ska särskilt behandla säkerhetsgodkännanden för leverantörernas personal och innehållet i de kontrakt som avses i denna bilaga.
4. Handlingar som rör upphandlingar och kontraktet avseende underhåll av de från datanätverket isolerade informations- och kommunikationssystemen ska förses med FIDUCIA-markering, om de innehåller uppgifter som, om de obehörigen röjs, skulle kunna skada unionens säkerhet eller en eller flera av dess medlemsstaters säkerhet eller deras internationella förbindelser. Säkerhetsbilagan till kontraktet ska innehålla bestämmelser som ålägger leverantören att följa de miniminormer som fastställs i detta beslut. Underlåtenhet att följa dessa miniminormer kan utgöra tillräcklig grund för att häva kontraktet.
5. I kontrakt som innefattar åtgärder som innebär att FIDUCIA-uppgifterna skyndsamt måste bortföras och placeras på ett säkert ställe, ska det anges hur många säkerhetsvakter som måste inneha ett personalsäkerhetsgodkännande. Nämda kontrakt ska inte innehålla några uppgifter om det tillvägagångssätt som ska användas. Kontraktet ska inte förses med FIDUCIA-markering.
6. Leverantören får inte anlita underentreprenörer för verksamhet som specificeras i anbudsinfordran och i kontraktet och som innefattar eller kräver tillgång till FIDUCIA-uppgifter.