KOMMISSIONENS AFGØRELSE (EU, Euratom) 2018/559

af 6. april 2018

om gennemførelsesbestemmelser til artikel 6 i afgørelse (EU, Euratom) 2017/46 om kommunikations- og informationssystemernes sikkerhed i Europa-Kommissionen

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 249,

under henvisning til traktaten om oprettelse af Det Europæiske Atomenergifællesskab,

under henvisning til Kommissionens afgørelse (EU, Euratom) 2017/46 af 10. januar 2017 om kommunikations- og informationssystemernes sikkerhed i Europa-Kommissionen ([1]), særlig artikel 6, og

ud fra følgende betragtninger:

(1) Med vedtagelsen af afgørelse (EU, Euratom) 2017/46 er der behov for, at Kommissionen gennemgår, ajourfører og konsoliderer gennemførelsesbestemmelserne til den ophævede Kommissions afgørelse C(2006) 3602 om sikkerheden i forbindelse med de kommunikations- og informationssystemer, der anvendes af Kommissionen.

(2) De medlemmer af Kommissionen, som er ansvarlige for sikkerhedsspørgsmål, er i fuld overensstemmelse med de interne regler og procedurer blevet bemyndiget til at fastsætte gennemførelsesbestemmelser i overensstemmelse med artikel 13 i afgørelse (EU, Euratom) 2017/46 ([2]).

(3) Gennemførelsesbestemmelserne til afgørelse C(2006) 3602 bør derfor ophæves —

VEDTAGET DENNE AFGØRELSE:

KAPITEL 1

ALMINDELIGE BESTEMMELSER

Artikel 1

Genstand og anvendelsesområde

1. Genstand og anvendelsesområde for nærværende afgørelse er fastsat i artikel 1 i afgørelse (EU, Euratom) 2017/46.

2. Bestemmelserne i nærværende afgørelse gælder for alle kommunikations- og informationssystemer (CIS'er). De ansvarsområder, som er defineret i nærværende afgørelse, finder dog ikke anvendelse på CIS'er til håndtering af EU's klassificerede informationer. De relevante ansvarsområder for disse systemer fastlægges af systemejeren og Kommissionens sikkerhedsmyndighed i overensstemmelse med Kommissionens afgørelse (EU, Euratom) 2015/444 ([3]).

3. Kapitel 2 i nærværende afgørelse giver en oversigt over, hvordan organisering og ansvarsområder i forbindelse med IT-sikkerhed skal gennemføres i praksis. Kapitel 3 i nærværende afgørelse giver en oversigt over de processer, der vedrører artikel 6 i afgørelse (EU, Euratom) 2017/46.

Artikel 2

Definitioner

Definitionerne i artikel 2 i afgørelse (EU, Euratom) 2017/46 finder anvendelse i nærværende afgørelse. I nærværende afgørelse forstås desuden ved:

1. »kryptogodkendelsesmyndighed (CAA)«: en funktion, som varetages af Kommissionens sikkerhedsmyndighed, og som henhører under generaldirektøren for Menneskelige Ressourcer og Sikkerhed

([1]) EUT L 6 af 11.1.2017, s. 40.
([2]) Kommissionens afgørelse C(2017) 7428 final af 8. november 2017, der giver bemyndigelse til at vedtage gennemførelsesbestemmelser, standarder og retningslinjer for kommunikations- og informationssystemernes sikkerhed i Europa-Kommissionen.
([3]) Kommissionens afgørelse (EU, Euratom) 2015/444 af 13. marts 2015 om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer (EUT L 72 af 17.3.2015, s. 53).

2. »ekstern netværksforbindelse«: enhver form for elektronisk kommunikationsforbindelse mellem Kommissionens interne netværk og ethvert andet netværk, herunder internettet. Denne definition omfatter ikke tredjepartsnetværk, der leveres i henhold til kontrakt som en del af Kommissionens interne netværk

3. »nøgledeponering«: en procedure, hvorefter der opbevares kopier af krypteringsnøgler hos en eller flere forskellige parter, hvilket sikrer adskillelse af funktioner med henblik på at kunne rekonstruere nøglerne, såfremt den operationelle kopi går tabt. Nøglerne kan opdeles i to eller flere dele, som hver især deponeres hos forskellige parter for at sikre, at hele nøglen ikke ejes af en enkelt part

4. »RASCI«: en forkortelse for placeringen af roller/ansvar ud fra følgende tildelingsindikatorer:

   a) »responsible« (R): person, der handler og træffer beslutninger for at opnå det ønskede resultat

   b) »accountable« (A): person, der er ansvarlig for handlinger, beslutninger og resultater

   c) »supports« (S): person, der hjælper den ansvarlige med at udføre opgaven

   d) »consulted« (C): person, der høres med henblik på rådgivning eller udtalelse

   e) »informed« (I): person, der holdes ajour med relevante oplysninger.

KAPITEL 2

ORGANISATION OG ANSVARSOMRÅDER

Artikel 3

Roller og ansvarsområder

De roller og ansvarsområder, der vedrører artikel 4-8 i nærværende afgørelse, er defineret i bilaget i overensstemmelse med RASCI-modellen.

Artikel 4

Tilpasning til Kommissionens informationssikkerhedspolitik

1. Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed gennemgår Kommissionens IT-sikkerhedspolitik og dertil knyttede standarder og retningslinjer for at sikre, at de er i overensstemmelse med Kommissionens generelle sikkerhedspolitikker, navnlig Kommissionens afgørelse (EU, Euratom) 2015/443 ([1]) og afgørelse (EU, Euratom) 2015/444.

2. Efter anmodning fra andre af Kommissionens tjenestegrene kan Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed gennemgå deres IT-sikkerhedspolitikker eller anden IT-sikkerhedsdokumentation for at sikre, at de er i overensstemmelse med Kommissionens informationssikkerhedspolitik. Lederen af den pågældende tjenestegren i Kommissionen sikrer, at der tages hånd om uoverensstemmelser.

3. Som ansvarlig for informationssikkerheden samarbejder Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed med Generaldirektoratet for Informationsteknologi for at sikre, at IT-sikkerhedsprocesserne fuldt ud tager højde for sikkerhedsklassificeringen og sikkerhedsprincipperne som fastsat i afgørelse (EU, Euratom) 2015/443, særlig artikel 3 og 9.

KAPITEL 3

IT-SIKKERHEDSPROCESSER

Artikel 5

Krypteringsteknologier

1. Anvendelsen af krypteringsteknologier til beskyttelse af EU's klassificerede informationer (EUCI) skal være forenelig med afgørelse (EU, Euratom) 2015/444.

2. Afgørelserne om anvendelse af krypteringsteknologier til beskyttelse af andre data end EU's klassificerede informationer træffes af systemejeren for hvert CIS, idet der bådes tages hensyn til de risici, der ønskes mindsket ved kryptering, og de risici, som det medfører.

3. Kryptogodkendelsesmyndigheden (CAA) skal forhåndsgodkende alle anvendelser af krypteringsteknologier, medmindre krypteringen udelukkende anvendes til at beskytte fortroligheden af andre data end EU's klassificerede informationer ved overførsel med anvendelse af standardnetværksprotokoller.

([1]) Kommissionens afgørelse (EU, Euratom) 2015/443 af 13. marts 2015 om sikkerhedsbeskyttelse i Kommissionen (EUT L 72 af 17.3.2015, s. 41).

4. Med undtagelse af det i nærværende artikels stk. 3 omhandlede tilfælde sikrer Kommissionens tjenestegrene, at der gemmes sikkerhedskopier af samtlige krypteringsnøgler ved nøgledeponering med henblik på at gendanne lagrede data, hvis krypteringsnøglen ikke er tilgængelig. Der må kun foretages gendannelse af krypterede data ved hjælp af sikkerhedskopier, når det er godkendt i overensstemmelse med den af kryptogodkendelsesmyndigheden fastlagte standard.

5. Anmodninger om godkendelse af anvendelsen af krypteringsteknologier skal dokumenteres formelt og indeholde oplysninger om det CIS og de data, der skal beskyttes, de teknologier, der skal anvendes, og de hermed forbundne operationelle sikkerhedsprocedurer. Disse anmodninger om godkendelse undertegnes af systemejeren.

6. Anmodninger om godkendelse af anvendelsen af krypteringsteknologier skal evalueres af kryptogodkendelsesmyndigheden i overensstemmelse med de offentliggjorte standarder og krav.

Artikel 6

IT-sikkerhedsinspektioner

1. Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed gennemfører IT-sikkerhedsinspektioner for at fastslå, om IT-sikkerhedsforanstaltningerne er i overensstemmelse med Kommissionens IT-sikkerhedspolitikker, og kontrollere disse kontrolforanstaltningers integritet.

2. Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed kan foretage en IT-sikkerhedsinspektion:

a) på eget initiativ

b) på anmodning fra Styrelsesrådet for Informationssikkerhed (ISSB)

c) på anmodning fra en systemejer

d) i forbindelse med en sikkerhedshændelse eller

e) i forbindelse med identificering af en høj risiko for et bestemt system.

3. Dataejerne kan anmode om en IT-sikkerhedsinspektion, inden de lagrer deres oplysninger i et CIS.

4. Resultaterne af en inspektion dokumenteres i en formel rapport til systemejeren med kopi til den lokale IT-sikkerhedsansvarlige (LISO) og skal indeholde resultater og anbefalinger til forbedring af CIS'ets overholdelse af IT-sikkerhedspolitikken. Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed indberetter vigtige spørgsmål og anbefalinger til Styrelsesrådet for Informationssikkerhed.

5. Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed overvåger gennemførelsen af anbefalingerne.

6. IT-sikkerhedsinspektioner skal, hvor det er relevant, omfatte inspektion af tjenester, lokaler og udstyr, der stilles til rådighed for systemejeren, herunder både interne og eksterne tjenesteydere.

Artikel 7

Adgang fra eksterne netværk

1. Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed fastsætter reglerne i en standard om godkendelse af adgang mellem Kommissionens CIS'er og eksterne netværk.

2. I reglerne skal der sondres mellem forskellige typer af eksterne netværksforbindelser og fastsættes passende sikkerhedsregler for hver type forbindelse, herunder hvorvidt det er nødvendigt med en forhåndsgodkendelse til forbindelsen fra den relevante myndighed som anført i denne artikels stk. 4.

3. Om nødvendigt gives tilladelsen på baggrund af en formel anmodnings- og godkendelsesproces. Godkendelsen gælder for en nærmere fastsat periode og skal indhentes, før forbindelsen aktiveres.

4. Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed har det overordnede ansvar for godkendelsen af anmodninger, men kan på eget initiativ uddelegere ansvaret for godkendelse af visse forbindelsestyper i overensstemmelse med artikel 17, stk. 3, i afgørelse (EU, Euratom) 2015/443 og på de betingelser, der er fastsat i stk. 8.

5. Den godkendende instans kan fastsætte yderligere sikkerhedskrav som en forudsætning for godkendelse for at beskytte Kommissionens CIS og netværk mod risikoen for uautoriseret adgang eller andre brud på sikkerheden.

6. Generaldirektoratet for Informationsteknologi er standardleverandør af netværkstjenester til Kommissionen. Andre tjenestegrene i Kommissionen, som ikke benytter netværkstjenester fra Generaldirektoratet for Informationsteknologi, skal først indhente samtykke fra Styrelsesrådet for Informationssikkerhed. Kommissionens tjenestegrene skal dokumentere den kommercielle begrundelse for anmodningen og påvise, at netværkskontrollerne er tilstrækkelige til at opfylde kravene til kontrol med indgående og udgående informationsstrømme.

7. CIS-systemejeren fastsætter sikkerhedskravene for ekstern adgang til det pågældende CIS og sikrer gennemførelsen af passende foranstaltninger til at beskytte dets sikkerhed, med støtte fra den lokale IT-sikkerhedsansvarlige.

8. De sikkerhedsforanstaltninger, der gennemføres for eksterne netværksforbindelser, skal være baseret på need-to-know-princippet og »least privilege«-princippet, som sikrer, at de pågældende personer kun får de oplysninger og adgangsrettigheder, som er nødvendige for at varetage deres officielle opgaver for Kommissionen.

9. Alle eksterne netværksforbindelser filtreres og overvåges for at opdage potentielle brud på sikkerheden.

10. Hvis forbindelserne er oprettet for at gøre det muligt at udlicitere et CIS, er godkendelsen betinget af en tilfredsstillende afslutning af proceduren, der er beskrevet i artikel 8.

Artikel 8

Udlicitering af CIS'er

1. I denne afgørelse anses et CIS for udliciteret, når det leveres på grundlag af en kontrakt med en tredjepartsleverandør, hvorved CIS'et har til huse i lokaler uden for Kommissionen. Dette omfatter udlicitering af individuelle eller flere CIS'er eller andre IT-tjenester, datacentre uden for Kommissionens lokaler og eksterne tjenesters håndtering af Kommissionens datasæt.

2. Ved udliciteringen af et CIS skal der tages højde for følgende for så vidt angår følsomheden eller klassificeringen af de oplysninger, der håndteres:

a) CIS'er, der håndterer EU's klassificerede informationer, akkrediteres i overensstemmelse med afgørelse (EU, Euratom) 2015/444, og Kommissionens sikkerhedsakkrediteringsmyndighed (SAA) skal høres på forhånd. Systemer, der håndterer EU's klassificerede informationer, udliciteres ikke.

b) Systemejeren af et CIS, der håndterer andre oplysninger end EU's klassificerede informationer, iværksætter passende foranstaltninger til at håndtere de sikkerhedsmæssige behov i overensstemmelse med de relevante retlige forpligtelser eller oplysningernes følsomhed, under hensyntagen til de risici, der er forbundet med udlicitering. Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed kan stille yderligere krav.

c) I forbindelse med udliciterede udviklingsprojekter skal der tages hensyn til følsomheden i den udviklede kode og eventuelle testdata, der er anvendt ved udviklingen.

3. Ud over principperne i artikel 3 i afgørelse (EU, Euratom) 2017/46 gælder følgende principper for udliciterede CIS'er:

a) Udliciteringsordninger skal udformes således, at der undgås afhængighed af specifikke leverandører.

b) Sikkerhedsforanstaltninger i forbindelse med udlicitering skal begrænse mulighederne for, at tredjepartens ansatte får adgang til eller ændrer Kommissionen oplysninger.

c) Tredjepartens ansatte, som har adgang til et udliciteret CIS, skal udfærdige fortrolighedsaftaler.

d) Udliciteringen af et CIS skal fremgå af fortegnelsen over CIS'er.

4. Systemejeren skal sammen med dataejeren:

a) vurdere og dokumentere risici i forbindelse med udlicitering

b) fastsætte relevante sikkerhedskrav

c) rådføre sig med systemejerne af alle andre forbundne CIS'er for at sikre, at deres sikkerhedskrav medtages

d) sikre, at passende sikkerhedskrav og sikkerhedsrettigheder medtages i udliciteringskontrakten

e) opfylde andre krav i den detaljerede procedure som anført i denne artikels stk. 8.

Disse handlinger skal være afsluttet, inden kontrakten underskrives, eller der indgås anden aftale om udlicitering af et eller flere CIS'er.

5. Systemejerne forvalter risiciene i forbindelse med udlicitering i CIS'ets levetid med henblik på at opfylde de fastlagte sikkerhedskrav.

6. Systemejerne sikrer, at tredjepartsleverandører er forpligtet til omgående at underrette Kommissionen om alle IT-sikkerhedshændelser, som berører et af Kommissionens udliciterede CIS'er.

7. Systemejeren er ansvarlig for at sikre, at det enkelte CIS, udliciteringskontrakten og sikkerhedsforanstaltningerne er i overensstemmelse med Kommissionens regler om informationssikkerhed og IT-sikkerhed.

8. Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed fastsætter nærmere standarder for de ansvarsområder og aktiviteter, der er fastsat i stk. 1-7, i overensstemmelse med artikel 10 nedenfor.

KAPITEL 4

DIVERSE OG AFSLUTTENDE BESTEMMELSER

Artikel 9

Gennemsigtighed

Denne afgørelse bekendtgøres for Kommissionens personale og alle personer, som den gælder for, og offentliggøres i *Den Europæiske Unions Tidende*.

Artikel 10

Standarder

1. Bestemmelserne i denne afgørelse skal om nødvendigt beskrives nærmere i de standarder og/eller retningslinjer, der skal vedtages i overensstemmelse med afgørelse (EU, Euratom) 2017/46 og med afgørelse C(2017)7428. Disse gennemførelsesbestemmelser og afgørelse (EU, Euratom) 2017/46 beskrives nærmere i IT-standarderne og -retningslinjerne for så vidt angår specifikke sikkerhedsområder i henhold til ISO 27001:2013 bilag A. Disse standarder og retningslinjer er baseret på bedste praksis for branchen og udvælges, så de passer til Kommissionens IT-miljø.

2. Standarderne udarbejdes om nødvendigt i henhold til ISO 27001:2013 bilag A på følgende områder:

1) organisering af informationssikkerhed

2) personalesikkerhed

3) forvaltning af aktiver

4) adgangskontrol

5) kryptografi

6) fysisk og miljømæssig sikkerhed

7) driftssikkerhed

8) kommunikationssikkerhed

9) indkøb, udvikling og vedligeholdelse af systemer

10) leverandørforbindelser

11) håndtering af IT-sikkerhedshændelser

12) informationssikkerhedsaspekter ved styring af driftskontinuitet

13) overholdelse.

3. Styrelsesrådet for Informationssikkerhed godkender de standarder, der er nævnt i denne artikels stk. 1 og 2, før de vedtages.

4. Gennemførelsesbestemmelserne til afgørelse C(2006) 3602 vedrørende anvendelsesområdet for nærværende afgørelse ophæves hermed.

5. De standarder og retningslinjer, som blev vedtaget i henhold til afgørelse C(2006) 3602 af 16. august 2006, er fortsat gældende, i det omfang de ikke strider mod nærværende gennemførelsesbestemmelser, indtil de ophæves eller erstattes af de standarder eller retningslinjer, som skal vedtages i henhold til artikel 13 i afgørelse (EU, Euratom) 2017/46.

Artikel 11

Ikrafttræden

Denne afgørelse træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Udfærdiget i Bruxelles, den 6. april 2018.

På Kommissionens vegne
For formanden
Günther OETTINGER
Medlem af Kommissionen

BILAG

ROLLER OG ANSVARSOMRÅDER (RASCI)

Med RASCI-modellen tildeles roller/ansvar ved hjælp af følgende forkortelser:

a) R — Responsible

b) A — Accountable

c) S — Supporting

d) C — Consulted

e) I — Informed

Proces \ Rolle	ISSB	HR (DS)	Kommissionens tjenestegrene	Systemejer	Dataejer	LISO	GD DIGIT	Leverandører
Tilpasning til Kommissionens informationssikkerhedspolitik		**R/A**	**S**				**S**	
Krypteringsteknologier		**C**	**A**	**R**	**I**	**C**		
IT-sikkerhedsinspektioner	**I**	**A/R**		**S**	**I**	**I**	**S**	
Adgang fra eksterne netværk	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Udliciteringaf CIS'er		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] Styrelsesrådet for Informationssikkerhed (ISSB) høres i forbindelse med driften af interne netværk af andre kommissionstjenestegrene end Generaldirektoratet for Informationsteknologi (DIGIT).

[2] Systemejeren af et CIS, som udliciteres, skal være ansvarlig, og systemejeren af ethvert andet CIS, som et udliciteret CIS forbindes med, skal høres.