

Sikkerhedsgodkendelse på teleområdet

Sikkerhedsgodkendelser er en del af kravene i telereguleringen. Formålet er primært at beskytte informationer om kritisk teleinfrastruktur.

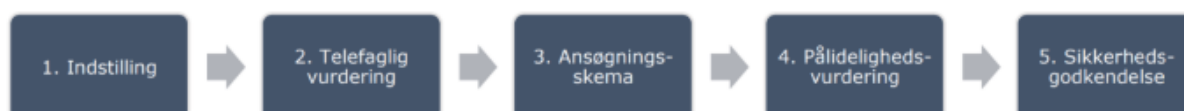
Center for Cybersikkerhed (CFCS) er ressortansvarlig for sikkerhed og beredskab på teleområdet. Det betyder, at CFCS bl.a. fører tilsyn på teleområdet og har den koordinerende rolle i forbindelse med samfundets teleforsyning i beredskabssituationer. Kravene i telereguleringen omfatter også sikkerhedsgodkendelse og kan derfor også være en del af vores tilsynsaktiviteter.

Sikkerhedsgodkendelser er en konkret vurdering af en persons pålidelighed. Formålet med sikkerhedsgodkendelse på teleområdet er primært at beskytte informationer om kritisk teleinfrastruktur. Det er derfor udbyderens pligt at vurdere, om medarbejdere eller repræsentanter for udbyderen varetager funktioner, der kræver indstilling til sikkerhedsgodkendelse.

Proces for indstilling og ansøgning

Som følge af den nylige ressortomlægning forventer CFCS, at der inden for kort tid vil ske ændringer i forbindelse med sagsbehandlingen af sikkerhedsgodkendelser. Dog er der allerede nu en ændring i forhold til elektroniske links til ansøgnings-skemaer, som FE tidligere har anvendt. Den elektroniske løsning er udfaset, hvilket betyder, at udbyderen, indtil videre, skal hente oplysningsskemaer på FE's hjemmeside i forbindelse med indstilling til sikkerhedsgodkendelse (se punkt 3).

Processen for sikkerhedsgodkendelse på teleområdet sker i fem trin og involverer CFCS, Forsvarets Efterretningstjeneste (FE) og Politiets Efterretningstjeneste (PET).



1. Teleudbyderen udfærdiger en begrundet indstilling om sikkerhedsgodkendelse af en medarbejder eller repræsentant for udbyderen. Det kan ske ved, at

teleudbyderen udfylder vedlagte skema, som sendes via Digital Post til CFCS under FE. Husk at markere tydeligt, at indstillingen sendes til telesektionen. Indstillingen kan også sendes via mail til tele@cfcs.dk.

2. CFCS afgør – efter en telefaglig vurdering – om der bør ske sikkerhedsgodkendelse af den indstillede medarbejder. De kriterier, som CFCS lægger særlig vægt på, er, om medarbejderen fx skal behandle klassificerede oplysninger, har adgang til centrale dele af særlig kritisk teleinfrastruktur, behandler oplysninger om beredskabsmæssige forhold eller varetager kontakten til CFCS på beredskabsområdet. Udbyderen modtager besked, når CFCS har afsluttet den telefaglige vurdering af udbyderens indstilling.

3. Herefter skal den indstillede medarbejder udfylde et oplysningskema, som sendes til CFCS' telesektion på e-mail tele@cfcs.dk eller via Digital Post til Forsvarets Efterretningstjeneste – Center for Cybersikkerhed, att.: Telesektionen. Skemaer findes på FE's [hjemmeside](#). Vær opmærksom på at vælge det korrekte skema alt efter, hvilken klassifikationsgrad, der indstilles til. Når skemaet er sendt, foretager PET en personundersøgelse. (Undersøgelsen sker kun, hvis både medarbejderen og dennes evt. ægtefælle/samlever giver samtykke).

4. Personundersøgelsen danner grundlaget for FE's pålidelighedsvurdering, hvor FE afgør, om den indstillede person kan sikkerhedsgodkendes. Ved afgørelsen lægges der især vægt på forhold, som kan gøre personen sårbar. Det kan fx være økonomiske forhold eller strafbare forhold, som spiller en rolle i forhold til, om vedkommende kan sikkerhedsgodkendes. Omfanget af undersøgelsen afhænger af klassifikationsgraden ([læs mere under FAQ](#)).

5. Når den indstillede medarbejder eller repræsentant for udbyderen bør og kan sikkerhedsgodkendes, får udbyderen besked om afgørelsen pr. e-mail eller Digital Post. Udbyderen orienterer herefter medarbejderen eller repræsentanten om afgørelsen.

Sagsbehandlingstid

Sagsbehandlingstiden kan tage op til 8-10 måneder. Udbyderen orienteres om væsentlige sagsskridt og om resultatet af indstillingen og ansøgningsprocessen.

CFCS anbefaler, at udbyderen udpeger en personalesikkerhedsansvarlig (PSA) til at varetage indstilling af medarbejdere eller repræsentanter for udbyderen og efterfølgende sikker opbevaring af sikkerhedsgodkendelser. Derudover kan det være med til at lette sagsbehandlingstiden.

FAQ

Svar på de mest almindelige spørgsmål om sikkerhedsgodkendelse af medarbejdere på teleområdet.

Hvornår skal man sikkerhedsgodkendes?

Kravene om sikkerhedsgodkendelse skal ses i sammenhæng med de regler om risikovurdering og risikostyring m.m., der styrer implementeringen af udbyderens almindelige forretningsmæssige sikkerheds- og sikringsforanstaltninger i forhold til udbuddet af net- og tjenester. Reglerne om sikkerhedsgodkendelser bygger oven på udbyderens risikovurdering og knytter et samfundsmæssigt beskyttelseselement til den almindelige sikkerhed.

Udbyderen skal med andre ord vurdere den enkelte medarbejder eller repræsentant for udbyderens arbejdsfunktion og -opgaver. Vedkommende skal sikkerhedsgodkendes, hvis vedkommende fx skal behandle klassificerede informationer eller har adgang til systemer, der benyttes ifm. indgreb i meddelelshemmeligheden.

Hvem skal sikkerhedsgodkendes?

Kravene om sikkerhedsgodkendelse gælder både udbyderens egne medarbejdere samt repræsentanter for udbyderen. Det kan fx være konsulenter, som er ansat af en leverandør, men som varetager opgaver for udbyderen, herunder konsulenter hos en udenlandsk leverandør, som udfører opgaver for udbyderen i udlandet.

Hvor længe holder en sikkerhedsgodkendelse?

En sikkerhedsgodkendelse holder normalt fem år. Er der tale om en udenlandsk statsborger er varigheden dog normalt begrænset til to år. Det er udbyderen selv, der skal sørge for, at sikkerhedsgodkendelsen evt. fornyes inden udløb.

Hvad er en personalsikkerhedsansvarlig?

CFCS anbefaler, at teleudbyderen udpeger en personalsikkerhedsansvarlig (PSA), der varetager kontakten til CFCS i forhold til sikkerhedsgodkendelser, og som har ansvaret for sikker opbevaring af disse sikkerhedsgodkendelser. Derudover kan det lette sagsbehandlingen hos både teleudbyderen og CFCS. CFCS anbefaler desuden, at PSA'en bliver sikkerhedsgodkendt til minimum FORTROLIGT.

Skal man godkendes igen, hvis man allerede er sikkerhedsgodkendt?

Hvis en medarbejder er sikkerhedsgodkendt af andre myndigheder, gælder sikkerhedsgodkendelsen alene for opgaver for denne myndighed og dermed ikke på teleområdet. Medarbejdere eller repræsentanter for udbyderen skal derfor også indstilles til sikkerhedsgodkendelse ved CFCS, såfremt de varetager opgaver, hvor det ud fra telereguleringen er krav herom.

Hvilken klassifikationsgrad skal man godkendes til?

Hvilken klassifikationsgrad, medarbejderen eller repræsentanten for udbyderen skal sikkerhedsgodkendes til, kommer an på det materiale eller de områder, som vedkommende har adgang til eller skal behandle. Klassifikationsgraden afhænger af informationernes indhold, og hvor meget skade det kan forvolde Danmark, hvis disse informationer videregives uden bemyndigelse. De forskellige klassificeringer (TIL TJENESTEBRUG, FORTROLIGT, HEMMELIGT og YDERST HEMMELIGT) kan læses i Justitsministeriets sikkerhedscirkulære nr. 10338 af 17. december 2014.

Hvad hvis forholdene ændrer sig?

Udbyderen skal være opmærksom på, at sikkerhedsgodkendelsen kun er gyldig, så længe medarbejderen eller repræsentanten for udbyderen er ansat i virksomheden og varetager de opgaver, som ligger til grund for indstillingen til sikkerhedsgodkendelse.

Det er udbyderens pligt at underrette CFCS, hvis ansættelsen ophører, eller der sker ændringer i de opgaver, som lægger til grund for godkendelsen.

Hvis medarbejderen f.eks. begår kriminalitet, vil FE modtage besked om dette fra politiet, og FE vil tage medarbejderens sikkerhedsgodkendelse op til fornyet overvejelse. Det kan betyde, at godkendelsen tilbagekaldes.