

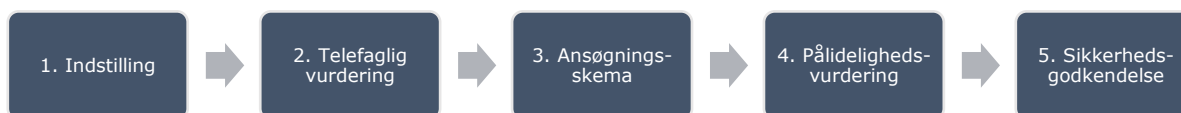
Sikkerhedsgodkendelse på teleområdet

Center for Cybersikkerhed (CFCS) er resortansvarlig for sikkerhed og beredskab på teleområdet. Det betyder, at CFCS bl.a. fører tilsyn på teleområdet og har den koordinerende rolle ift. 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

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. Den indstillede medarbejder (og dennes evt. ægtefælle/samlever) modtager et ansøgnings-skema med Digital Post, som udfyldes og sendes videre til PET, der foretager 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 sagskridt og om resultatet af indstillingen og ansøgningsprocessen.

CFCS anbefaler, at udbyderen udpeger en personalsikkerhedsansvarlig (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.

Sikkerhedsgodkendelse efter telereguleringen

[Lovbekendtgørelse nr. 153 af 1. februar 2021 om net- og informationssikkerhed](#)

- **§ 6.** En udbyder skal indstille medarbejdere og repræsentanter for udbyderen til sikkerhedsgodkendelse hos sikkerhedsmyndigheden, når de pågældende som led i deres konkrete opgaveløsning for udbyderen skal behandle klassificerede informationer eller andre informationer, der er særligt beskyttelsesværdige i relation til sikker i net og tjenester eller beredskab.
- **§ 6, stk. 2.** Erhvervsmæssige udbydere af offentlige tilgængelige elektroniske kommunikationsnet skal sikre, at medarbejdere eller repræsentanter for udbyderen, der varetager kontakten til Center for Cybersikkerhed i relation til beredskabet i henhold til regler, der er udstedt i medfør af § 5, stk. 2, i fornødent omgang sikkerhedsgodkendes efter stk. 1.

[Bekendtgørelse nr. 260 af 22. februar 2021 om sikkerhedsgodkendelse af medarbejdere på området for sikkerhed i net og tjenester](#)

- **§ 1.** Erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal sikre, at medarbejdere eller repræsentanter for udbydere, der har adgang til udstyr eller systemer, som benyttes i forbindelse med indgreb i meddelelshemmeligheden, som minimum er sikkerhedsgodkendt til klassifikationsgraden HEMMELIGT i overensstemmelse med Justitsministeriets cirkulære om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt (sikkerhedscirkulæret), jf. dog stk. 2.
- **§ 1, stk. 2.** Bestemmelsen i stk. 1 omfatter ikke medarbejdere eller repræsentanter for udbyderne, der forestår kontakten til politiet i forbindelse med indgreb i meddelelshemmeligheden og dermed er omfattet af bekendtgørelse nr. 1144 af 20. november 2006 om telenet- og teletjenesteudbyderes praktiske bistand til politiet i forbindelse med indgreb i meddelelshemmeligheden (sikkerhedsgodkendelse af personale i telebranchen), medmindre disse samtidig har adgang til udstyr eller systemer, som nævnt i stk. 1.

[Bekendtgørelse nr. 261 af 22. februar 2021 om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv.](#)

- **§ 16.** Udbyderens registre, der giver mulighed for at identificere kredsløb som værende faste kredsløb til beredskabsmæssige formål, herunder registre, der indeholder oplysninger om bestillinger, aftaler og netværks- og designinformation, skal være klassificeret i overensstemmelse med Justitsministeriets cirkulære om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt (sikkerhedscirkulæret).
- **§ 16, stk. 2.** Medarbejdere eller repræsentanter for udbyderen, der skal etablere, nedkoble, foretage ændringer i eller retablere faste kredsløb til beredskabsmæssige formål, skal være sikkerhedsgodkendt i overensstemmelse med sikkerhedscirkulæret.

FAQ

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 man ikke har adgang til Digital Post?

Hvis medarbejdere eller repræsentanter for udbyderen **ikke** har adgang til Digital Post, vil PSA'en modtage et link til FE's ansøgningsskema pr. e-mail, som skal sendes videre til den indstillede medarbejder. Det gælder fx for alle udenlandske statsborgere og danske borgere bosat i udlandet. Ansøgningsskemaet skal udfyldes og returneres af PSA'en til CFCS.

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 fx 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.

Hjælp til indstilling til CFCS

CFCS kan kontaktes på tlf. 33 32 55 80 eller mail tele@cfcs.dk, hvis der er spørgsmål til processen for sikkerhedsgodkendelse.

