**VEJ nr 9872 af 05/10/2018 (Gældende)**

# Vejledning om kriterier og krav til operatører af væsentlige tjenester i sundhedssektoren

Ministerium: Sundheds- og Ældreministeriet

Journalnummer: Sundheds- og Ældremin., Sundhedsdatastyrelsen

# Vejledning om kriterier og krav til operatører af væsentlige tjenester i sundhedssektoren

## Indledning

*Bekendtgørelse nr. 458 af 9. maj 2018 om operatører af væsentlige tjenester* udmønter dele af *lov nr. 440 af 8. maj 2018 om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren*.

Ovenstående lov og bekendtgørelse implementerer dele af det såkaldte NIS-direktiv[1)] i dansk ret inden for sundhedssektoren.

Der opstilles kriterier for, hvornår man er operatør af en væsentlig tjeneste og dermed er omfattet af loven og skal lade sig registrere. Derudover beskrives det bl.a., hvilke sikkerhedskrav man som operatør af en væsentlig tjeneste er underlagt, samt hvornår man som operatør af en væsentlig tjeneste skal underrette om en sikkerhedshændelse.

Vejledningen knytter sig til bekendtgørelse nr. 458 af 9. maj 2018 og har til formål at beskrive og uddybe de kriterier og krav, der gælder for operatører af væsentlige tjenester i sundhedssektoren.

Det skal i den forbindelse bemærkes, at visse opgaver i henhold til lov nr. 440 af 8. maj 2018 om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren, og regler udstedt i medfør af denne lov, er delegeret fra sundhedsministeren til Sundhedsdatastyrelsen, jf. *bekendtgørelse nr. 459 af 9. maj 2018 om delegation af opgaver fra sundhedsministeren til Sundhedsdatastyrelsen*. Det gælder bl.a. registrering af operatører af væsentlige tjenester samt modtagelse af underretninger om sikkerhedshændelser, som skal sendes til Sundhedsdatastyrelsen.

## 1. Identificering af operatører af væsentlige tjenester

En operatør af en væsentlig tjeneste er en offentlig eller privat enhed, som er etableret i Danmark, der:

1) leverer en tjeneste, der er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter inden for sundhedssektoren,
2) hvor leveringen af denne tjeneste afhænger af net- og informationssystemer og,
3) hvor en hændelse vil få væsentlige forstyrrende virkninger for leveringen af den pågældende tjeneste.

En operatør af en væsentlig tjeneste kan således være kommuner, regioner, privatpraktiserende læger og speciallæger, apoteker og lignende.

### 1.1. Tjenesten skal være væsentlig for opretholdelsen af sundhedsfaglig behandling

Det er vigtigt at være opmærksom på, at den pågældende tjeneste skal være væsentlig for opretholdelsen af den *sundhedsfaglige behandling*. Det betyder, at sekundær anvendelse af net- og informationssystemer til f.eks. administrative opgaver, videnskabelige og statistiske analyser og kvalitetssikring ikke skal opfattes som levering af væsentlige tjenester.

### 1.2. Leveringen af tjenesten skal afhænge af net- og informationssystemer

For at være en operatør af en væsentlig tjeneste, skal leveringen af tjenesten afhænge af net- og informationssystemer.

Det indebærer, at en leverandør af digital understøttelse af en tjeneste ikke er en operatør af en væsentlig tjeneste.

Anvender en operatør af en væsentlig tjeneste en leverandør til brug for den digitale understøttelse af sin tjeneste, vil operatøren være forpligtet til i forbindelse med sin registrering hos Sundhedsdatastyrelsen at angive leverandørens navn og adresse samt hvilken opgave, leverandøren udfører, jf. nærmere pkt. 3.

### 1.3. Konsekvenserne ved en sikkerhedshændelse

Endelig er det et krav, for at man kan identificeres som en operatør af en væsentlig tjeneste, at en hændelse vil få væsentlige forstyrrende virkninger for leveringen af den pågældende tjeneste, som medfører konsekvenser for:

a) Sundhedsberedskabet i Danmark, herunder den nationale operative stabs funktion,
b) det regionale sundhedsberedskab,
c) mere end 500.000 borgere, der er omfattet af tjenesten,
d) mere end 50.000 brugere, herunder patienter og sundhedspersoner, der er afhængige af tjenesten,
eller
e) mindst en region.

Kriterierne for, hvorvidt en sikkerhedshændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesten, er fastlagt ud fra kriterier i **Kommissionens meddelelse**[2)], som efterfølgende er blevet tilpasset strukturen i det danske sundhedsvæsen. Der er således ved fastlæggelsen af de pågældende kriterier taget højde for det eksisterende beredskab i sundhedsvæsenet på henholdsvis nationalt, regionalt og kommunalt niveau. Man vil således skulle medtænke, hvorvidt det eksisterende sundhedsberedskab bidrager til at reducere risikoen for, at en hændelse vil få væsentligt forstyrrende virkninger for leveringen af tjenesten.

Det er vigtigt ved vurderingen af, om man er operatør af en væsentlig tjeneste at være opmærksom på, at der er tale om en samlet vurdering. Det er således ikke givet, at såfremt en tjeneste medfører konsekvenser for mere end 500.000 borgere, at der så er tale om en væsentlig tjeneste. F.eks. kan et væsentligt lavere antal brugere af tjenesten få den betydning, at der ikke er tale om en væsentlig tjeneste, hvis hændelsen kan håndteres inden for rammerne af ens eksisterende beredskab.

### 1.4. Levering af tjeneste uden understøttelse af net- og informationssystemer

Kan en operatør opretholde sin tjeneste i mere end 72 timer uden understøttelse af net- og informationssystemer, er man ikke en operatør af en væsentlig tjeneste i henhold til bekendtgørelse om operatører af væsentlige tjenester, idet det forudsættes, at hændelsen kan håndteres inden for rammerne af det eksisterende sundhedsberedskab.

I vurderingen af, hvorvidt man kan opretholde sin tjeneste i mere end 72 timer uden understøttelse af net- og informationssystemer, må der foretages en identificering af de forretningsprocesser, der kan eller ikke kan opretholdes ud over de 72 timer. Eksempelvis vil en sikkerhedshændelse, f.eks. et nedbrud, der påvirker udførelsen af laboratorieanalyser have stor konsekvens for patientbehandlingen.

## 2. Sikkerhedsforanstaltninger

Operatører af væsentlige tjenester skal opretholde passende organisatoriske og tekniske foranstaltninger for at sikre robusthed, tilgængelighed, autenticitet, integritet og fortrolighed i de net- og informationssystemer, der understøtter den væsentlige tjeneste.

Dette sker på baggrund af en risikovurdering, hvor der er taget stilling til risikoen for, at et nedbrud vil få væsentlige forstyrrende virkninger på tjenesten. Det er operatøren af den væsentlige tjeneste, der fastlægger, hvordan risikovurderingen skal gennemføres, herunder hos eventuelle underleverandører, som helt eller delvis driver den væsentlige tjeneste.

Med henblik på at sikre, at der hos operatøren er tilstrækkeligt ledelsesmæssigt fokus på net- og informationssikkerhed, skal der foreligge en ledelsesgodkendt informationssikkerhedspolitik, der opdateres ved væsentlige ændringer i organisationen eller trusselsbilledet, men som minimum en gang årligt.

Der skal etableres en risikostyringsproces, der på baggrund af risikovurderingen beskriver håndtering af sikkerhedsrisici, herunder ledelsens risikovillighed.

Tilsynet med operatører af væsentlige tjenester vil tage udgangspunkt i den dokumentation, der foreligger fra operatøren på disse områder, f.eks informationssikkerhedspolitikken, SoA (Statement of Applicability) og risikoregisteret.

**3. Registrering hos Sundhedsdatastyrelsen**

Operatører af væsentlige tjenester skal lade sig registrere hos Sundhedsdatastyrelsen.

Registreringsblanketten kan findes på Sundhedsdatastyrelsens hjemmeside.

En operatør af en væsentlig tjeneste skal ved registreringen angive dennes navn og kontaktoplysninger på den eller de personer hos operatøren, som har ansvaret for registreringen hos operatøren.

Herudover skal det ved registreringen med udgangspunkt i ovenstående kriterier begrundes, hvorfor der er tale om en væsentlig tjeneste.

Endelig skal det af registreringen fremgå, hvilket eller hvilke net- og informationssystemer, operatøren er afhængig af samt oplysninger om eventuelle underleverandørers navn, adresse og opgavevaretagelse.

**4. Underretning**

Ved en hændelse, der har haft væsentlige konsekvenser for kontinuiteten leveringen af den væsentlige tjeneste, skal operatøren af denne tjeneste foretage underretning af Sundhedsdatastyrelsen og Center for Cybersikkerhed.

Underretningen skal ske via den digitale indberetningsløsning på virk.dk.

Underretningen skal som minimum indeholde oplysninger om:

1) Navn og kontaktoplysninger på operatøren,
2) Oplysninger om hændelsens årsag, karakter, varighed, forløb og konsekvenser,
3) Oplysninger om foranstaltninger, som operatøren har truffet, eller foreslår truffet, for at håndtere hændelsen,
4) Oplysninger om omfanget af hændelsen og
5) Oplysninger om eventuelle grænseoverskridende konsekvenser af hændelsen.

Det er muligt at supplere den oprindelige underretning, såfremt man ikke på anmeldelsestidspunktet har alle informationer til rådighed.

*Sundhedsdatastyrelsen, den 5. oktober 2018*

LISBETH NIELSEN

/ Steen Heilmann

1) Europa-Parlamentets og Rådets direktiv 2016/1148/EU af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen.

2) MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET Fuld udnyttelse af NIS – mod en effektiv gennemførelse af direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen. https://eur-lex.europa.eu/resource.html? uri=cellar:d829f91d-9859-11e7-b92d-01aa75ed71a1. 0022.02/DOC_2&format=PDF