NIS-DIREKTIVET STILLER NYE KRAV TIL SIKKERHED I NET- OG INFORMATIONSSYSTEMER

Visse forsyningsvirksomheder og andre operatører af væsentlige tjenester samt udbydere af digitale tjenester bør være opmærksomme på de nye regler i NIS-direktivet, der indfører generelle krav til sikkerheden i net- og informationssystemer og en underretningspligt ved sikkerhedshændelser.

Den 6. juli 2016 vedtog EU-Parlamentet direktiv 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen.

Formålet med direktivet, der ofte omtales som NIS-direktivet, er at harmonisere og skærpe reglerne om sikkerhed. Det sker i erkendelse af, at sikkerhedshændelser udgør en hyppig trussel for net- og informationssystemer, som kan få afgørende økonomiske og samfundsmæssige konsekvenser. Direktivet skal implementeres af medlemsstaterne inden 9. maj 2018.

HVEM OMFATTES AF DE NYE KRAV?

De nye regler kommer til at forpligte dels "operatører af væsentlige tjenester", dels "udbydere af digitale tjenester".

Begrebet "operatører af væsentlige tjenester" er afgrænset til operatører inden for sektorerne for drikkevandsforsyning og -distribution, energi (el, olie og gas), transport, bankvæsen, sundhed samt finansiel og digital infrastruktur. Det er derudover en betingelse, at operatøren leverer en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter, at leveringen afhænger af et net- og informationssystem, og at en sikkerhedshændelse vil få væsentlige forstyrrende virkninger for denne levering. Hver medlemsstat skal udarbejde en liste over operatører af væsentlige tjenester for hver sektor senest den 9. november 2018.

Begrebet "udbydere af digitale tjenester" er afgrænset til udbydere af digitale tjenester af typen onlinemarkedspladser, onlinesøgemaskiner eller cloud computing-tjenester.

SIKKERHEDSKRAV OG UNDERRETNINGSPLIGT

Direktivet indfører pligt for de omfattede operatører og udbydere til at træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der står i forhold til risikoen for sikkerhedshændelser på deres net- og informationssystemer.

Derudover pålægges de omhandlede operatører og udbydere en pligt til at underrette de nationale myndigheder hurtigst muligt om sikkerhedshændelser, hvis hændelserne har væsentlige konsekvenser for kontinuiteten af levering af tjenesterne.

Myndigheden skal oplyse øvrige berørte medlemsstater og kan oplyse offentligheden om hændelsen.

Med henblik på tilsynsmyndighedens vurdering af, om sikkerheden er tilstrækkelig, kan det kræves, at de omfattede operatører og udbydere udleverer oplysninger og dokumenterer gennemførelsen af sikkerhedspolitikker.

Direktivet indfører også regler, som styrker samarbejdet mellem medlemsstaterne om net- og informationssikkerhed.

FORBEDRET BESKYTTELSE AF CYBERSIKKERHED OG DATA

NIS-direktivet styrker beskyttelsen af cybersikkerheden for kritisk infrastruktur.

Sammen med persondataforordningen, der finder anvendelse fra 25. maj 2018, pålægger NIS-direktivet virksomhederne større ansvar for egne data. Virksomhederne bliver nødt til at indrette deres systemer på de nye krav - formentlig med øgede omkostninger til følge. Kravene i NIS-direktivet går i visse henseender videre end kravene i persondataforordningen, bl.a. da kravene gælder, uanset om der behandles personoplysninger eller ej. Sanktionerne for overtrædelse af reglerne i NIS-direktivet vil blive fastsat af medlemsstaterne ■

Mads Nygaard Madsen
Advokat
mnm@horten.dk

Charlotte Kunckel
Advokat
cku@horten.dk