OCH A/S
c/o Norlys
Ørestads Boulevard
DK-2300 København S
www.och.dk
CVR.nr. 18936909

OCH A/S – Cybersikkerhed – Sikkerhedsforanstaltninger

Indledning:

Den 1. juli 2025 træder EU-direktiv 2022/2555, almindeligvis betegnet NIS2, i kraft i Danmark. Direktivet er en videreudvikling af EU-direktiv 2016/1148, der samtidig ophæves.

Direktivet har til formål at styrke og ensarte cybersikkerheden, samt øge modstandskraften overfor cybertrusler, på tværs af EU.

Direktivet tilføjer nye krav, der skal efterleves af de virksomheder og myndigheder, der er omfattet af direktivet, samtidig med, at tilsyns- og håndhævelsesbeføjelser styrkes.

Sammenlignet med EU-direktiv 2016/1148 vil langt flere virksomheder og myndigheder være omfattet af det nye direktiv. Direktivet forventes også at have en afsmittende virkning, idet virksomheder, der ikke direkte er omfattet af direktivet, kan blive mødt af krav fra deres kunder, der i realiteten stiller dem som om, at de var omfattet.

Direktivet inddeler virksomheder og myndigheder, der er omfattet af direktivet, i to forskellige kategorier. Sektorer af særlig kritisk betydning (Direktivets bilag 1), samt andre kritiske sektorer (Direktivets bilag 2).

OCH A/S, herefter virksomheden eller selskabet, agerer ikke inden for et forretningsområde, der falder ind under en af de to kategorier, der er nævnt ovenfor. Virksomheden er som konsekvens heraf ikke omfattet af det nye direktiv og derved heller ikke forpligtiget til, at efterleve det.

Derimod står virksomhedens ejerkreds, der som udbydere af offentlige elektroniske kommunikationsnet og/eller offentligt tilgængelige elektroniske kommunikationstjenester, er omfattet af direktivet. Det samme gør sig gældende for virksomhedens kundekreds, der består af teleselskaber.

Som nævnt er en af forventningerne til det nye direktiv, at det vil have en afsmittende virkning på virksomheder, der ikke direkte er omfattet af direktivet, men har en kundekreds, der er.

Da virksomhedens ejer- og kundekreds er teleselskaber, der er omfattet af direktivet, er det virksomhedens forventning, at den vil blive mødet af spørgsmål til, i hvilket omfang den efterlever det nye direktiv. Dette må forventes at være en naturlig konsekvens af, at ejer- og

OCH A/S
c/o Norlys
Ørestads Boulevard
DK-2300 København S
www.och.dk
CVR.nr. 18936909

kundekreds selv stilles over for krav om, hvad de skal have styr på og kendskab til i forbindelse med hele deres værdikæde.

For at komme disse forventede krav i forkøbet har virksomheden proaktivt truffet beslutning om, at den vil sikre efterlevelse af de i direktivets artikel 21, stk. 2, nævnte punkter (a) til (j).

Ved proaktivt at tilpasse selskabets sikkerhed til at inkludere minimumssikkerheds-foranstaltningerne i direktivet får selskabet dermed signaleret til kunder, leverandører og andre interessenter, at selskabet tager passende og forholdsmæssige risikostyrings-foranstaltninger for at forhindre sikkerhedshændelser og minimere deres effekt.

Selskabet har opbakning fra topledelsen til denne tilgang til håndtering af minimums-sikkerhedsforanstaltningerne i direktivet, og at der i selskabet er et velfungerende niveau for risikostyring, it-sikkerhed og styring af konstellationen mellem selskabet og dets primære leverandører. Der er ikke identificeret uhensigtsmæssigheder relateret til direktivets krav eller den generelle cybersikkerhed i selskabet. Selskabet er velindsat i direktivet og de krav, der, forventeligt, indirekte vil blive stillet til selskabet. Selskabet har en klar tilgang til, hvordan man vil imødekomme forventninger fra kunder, som forventes at blive direkte påvirket af kravene i direktivet.

Af ovenstående grund er det ambitionen for selskabet at tilpasse sig kravene i direktivet bedst muligt under hensyntagen til selskabets størrelse og konstellation. Mere specifikt betyder det, at hovedfokus vil være på, hvordan selskabet håndterer kravene i artikel 21 (foranstaltninger på netværk og informationssystemer) og artikel 23 (rapportering om hændelser), og på artikel 20 (om risiko og styring).

Svar til sikkerhedsforanstaltninger:

Politikker for risikoanalyse og informationssikkerhed
Virksomheden har etableret politikker for risikoanalyse og informationssikkerhed. Disse politikker bliver løbende evalueret for at sikre, at de holdes opdateret, og tager højde for nye trusler og sårbarheder.

Hændelseshåndtering	
Driftsleverandør	Udviklingsleverandør

OCH A/S
c/o Norlys
Ørestads Boulevard
DK-2300 København S
www.och.dk
CVR.nr. 18936909

Virksomhedens driftsleverandør er ISO 27001:2222 certificeret. Denne certificering dækker størstedelen af de minimumsforanstaltninger, der fremgår af NIS2-direktivets artikel 21, stk. 2, litra a-j. På områder, hvor ISO 27001:2222 ikke er tilstrækkelig, har virksomhedens driftsleverandør sikret, at dens Governance, interne kontroller, samt foranstaltninger er af en sådan beskaffenhed, at de sikrer fuld overholdelse af NIS2-direktivet.	Virksomhedens udviklingsleverandør har oplyst, at den ikke er omfattet af NIS2-direktivet, hvorfor den ikke er forpligtiget til at efterleve kravene i direktivet. Virksomhedens udviklingsleverandør har, i tillæg hertil, oplyst, at den har til hensigt at implementerer NIS2-direktivet, hvilket forventes gennemført ultimo 2025.

Driftskontinuitet, såsom backup-styring og katastrofegendannelse, samt krisestyring	
Driftsleverandør	Udviklingsleverandør
Virksomhedens driftsleverandør er ISO 27001:2222 certificeret. Denne certificering dækker størstedelen af de minimumsforanstaltninger, der fremgår af NIS2-direktivets artikel 21, stk. 2, litra a-j. På områder, hvor ISO 27001:2222 ikke er tilstrækkelig, har virksomhedens driftsleverandør sikret, at dens Governance, interne kontroller, samt foranstaltninger er af en sådan beskaffenhed, at de sikrer fuld overholdelse af NIS2-direktivet.	Virksomhedens udviklingsleverandør har oplyst, at den ikke er omfattet af NIS2-direktivet, hvorfor den ikke er forpligtiget til at efterleve kravene i direktivet. Virksomhedens udviklingsleverandør har, i tillæg hertil, oplyst, at den har til hensigt at implementerer NIS2-direktivet, hvilket forventes gennemført ultimo 2025.

Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdet mellem hver enhed og dens direkte leverandører eller tjenesteudbydere	
Driftsleverandør	Udviklingsleverandør
Virksomhedens driftsleverandør er ISO 27001:2222 certificeret. Denne certificering dækker størstedelen af de minimumsforanstaltninger, der fremgår af NIS2-direktivets artikel 21, stk. 2, litra a-j. På områder, hvor ISO 27001:2222 ikke er tilstrækkelig, har virksomhedens driftsleverandør sikret, at dens Governance, interne kontroller, samt	Virksomhedens udviklingsleverandør har oplyst, at den ikke er omfattet af NIS2-direktivet, hvorfor den ikke er forpligtiget til at efterleve kravene i direktivet. Virksomhedens udviklingsleverandør har, i tillæg hertil, oplyst, at den har til hensigt at implementerer NIS2-direktivet, hvilket forventes gennemført ultimo 2025.

OCH A/S
c/o Norlys
Ørestads Boulevard
DK-2300 København S
www.och.dk
CVR.nr. 18936909

foranstaltninger er af en sådan beskaffenhed, at de sikrer fuld overholdelse af NIS2-direktivet.	

Sikkerhed ved anskaffelse, udvikling og vedligeholdelse af netværk og informationssystemer, herunder sårbarhedshåndtering og offentliggørelse	
Driftsleverandør	Udviklingsleverandør
Virksomhedens driftsleverandør er ISO 27001:2222 certificeret. Denne certificering dækker størstedelen af de minimumsforanstaltninger, der fremgår af NIS2-direktivets artikel 21, stk. 2, litra a-j. På områder, hvor ISO 27001:2222 ikke er tilstrækkelig, har virksomhedens driftsleverandør sikret, at dens Governance, interne kontroller, samt foranstaltninger er af en sådan beskaffenhed, at de sikrer fuld overholdelse af NIS2-direktivet.	Virksomhedens udviklingsleverandør har oplyst, at den ikke er omfattet af NIS2-direktivet, hvorfor den ikke er forpligtiget til, at efterleve kravene i direktivet. Virksomhedens udviklingsleverandør har, i tillæg hertil, oplyst, at den har til hensigt at implementerer NIS2-direktivet, hvilket forventes gennemført ultimo 2025.

Politikker og procedurer til at vurdere effektiviteten af risikostyringsforanstaltninger for cybersikkerhed	
Driftsleverandør	Udviklingsleverandør
Virksomhedens driftsleverandør er ISO 27001:2222 certificeret. Denne certificering dækker størstedelen af de minimumsforanstaltninger, der fremgår af NIS2-direktivets artikel 21, stk. 2, litra a-j. På områder, hvor ISO 27001:2222 ikke er tilstrækkelig, har virksomhedens driftsleverandør sikret, at dens Governance, interne kontroller, samt foranstaltninger er af en sådan beskaffenhed, at de sikrer fuld overholdelse af NIS2-direktivet.	Virksomhedens udviklingsleverandør har oplyst, at den ikke er omfattet af NIS2-direktivet, hvorfor den ikke er forpligtiget til at efterleve kravene i direktivet. Virksomhedens udviklingsleverandør har, i tillæg hertil, oplyst, at den har til hensigt at implementerer NIS2-direktivet, hvilket forventes gennemført ultimo 2025.

Grundlæggende cyberhygiejnepraksis og cybersikkerhedstræning	
Driftsleverandør	Udviklingsleverandør
Virksomhedens driftsleverandør er ISO	Virksomhedens udviklingsleverandør har

OCH A/S
c/o Norlys
Ørestads Boulevard
DK-2300 København S
www.och.dk
CVR.nr. 18936909

27001:2222 certificeret. Denne certificering dækker størstedelen af de minimumsforanstaltninger, der fremgår af NIS2-direktivets artikel 21, stk. 2, litra a-j. På områder, hvor ISO 27001:2222 ikke er tilstrækkelig, har virksomhedens driftsleverandør sikret, at dens Governance, interne kontroller, samt foranstaltninger er af en sådan beskaffenhed, at de sikrer fuld overholdelse af NIS2-direktivet.	oplyst, at den ikke er omfattet af NIS2-direktivet, hvorfor den ikke er forpligtiget til at efterleve kravene i direktivet. Virksomhedens udviklingsleverandør har, i tillæg hertil, oplyst, at den har til hensigt at implementerer NIS2-direktivet, hvilket forventes gennemført ultimo 2025.

Politikker og procedurer vedrørende brugen af kryptografi og, hvor det er relevant, kryptering	
Driftsleverandør	Udviklingsleverandør
Virksomhedens driftsleverandør er ISO 27001:2222 certificeret. Denne certificering dækker størstedelen af de minimumsforanstaltninger, der fremgår af NIS2-direktivets artikel 21, stk. 2, litra a-j. På områder, hvor ISO 27001:2222 ikke er tilstrækkelig, har virksomhedens driftsleverandør sikret, at dens Governance, interne kontroller, samt foranstaltninger er af en sådan beskaffenhed, at de sikrer fuld overholdelse af NIS2-direktivet.	Virksomhedens udviklingsleverandør har oplyst, at den ikke er omfattet af NIS2-direktivet, hvorfor den ikke er forpligtiget til at efterleve kravene i direktivet. Virksomhedens udviklingsleverandør har, i tillæg hertil, oplyst, at den har til hensigt at implementerer NIS2-direktivet, hvilket forventes gennemført ultimo 2025.

Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver	
Driftsleverandør	Udviklingsleverandør
Virksomhedens driftsleverandør er ISO 27001:2222 certificeret. Denne certificering dækker størstedelen af de minimumsforanstaltninger, der fremgår af NIS2-direktivets artikel 21, stk. 2, litra a-j. På områder, hvor ISO 27001:2222 ikke er tilstrækkelig, har virksomhedens driftsleverandør sikret, at dens Governance, interne kontroller, samt foranstaltninger er af en sådan	Virksomhedens udviklingsleverandør har oplyst, at den ikke er omfattet af NIS2-direktivet, hvorfor den ikke er forpligtiget til at efterleve kravene i direktivet. Virksomhedens udviklingsleverandør har, i tillæg hertil, oplyst, at den har til hensigt at implementerer NIS2-direktivet, hvilket forventes gennemført ultimo 2025.

OCH A/S
c/o Norlys
Ørestads Boulevard
DK-2300 København S
www.och.dk
CVR.nr. 18936909

beskaffenhed, at de sikrer fuld overholdelse af NIS2-direktivet.	

Brugen af multifaktorautentificering eller kontinuerlige autentificeringsløsninger, sikret stemme-, video- og tekstkommunikation og sikrede nødkommunikationssystemer inden for enheden, hvor det er relevant
"Man kan i dag logge på virksomhedens kundevendte portal, OCH Online, hvis man er i besiddelse af et aktivt brugernavn og den tilhørende adgangskode. Virksomheden finder, henset til dagens trusselslandskab, ikke, at dette er sikkerhedsmæssigt tilstrækkeligt. Og har derfor truffet beslutning om, at adgangen til OCH Online skal beskyttes yderligere. Virksomheden har i forbindelse med en risikoanalyse vurderet forskellige muligheder. Indførelse af krav om brug af tofaktorgodkendelse (2FA) eller IP-filtrering af adgangen til OCH Online. Tofaktorgodkendelse tilføjer et ekstra sikkerhedslag til autentificering når en bruger logger på OCH Online, mens IP-filtrering begrænser adgangen til OCH Online baseret på den IP-adresse anmodningen kommer fra. Tofaktorgodkendelse er den mest fleksible løsning, da den kan anvendes fra en hvilken som helst lokation, hvorimod IP-filtrering er bundet til en bestemt lokation. Udover at være den mest fleksible løsning er tofaktorgodkendelse samtidig den mest komplekse løsning, da brugerne skal være i besiddelse af noget tertiært, såsom en telefon eller et hardware-baseret token, hvorimod IP-filtrering håndteres på netværksniveau og er ”usynligt” for brugerne. Tofaktorgodkendelse og IP-filtrering kan, hver for sig eller i forening, anvendes til at øge sikkerheden omkring OCH Online. På baggrund af den udførte risikoanalyse er det virksomhedens vurdering, at IP-filtrering er den mest brugervenlige metode, der samtidig er sikkerhedsmæssigt tilfredsstillende, at anvende. Virksomheden har derfor besluttet at implementerer IP-filtrering i forbindelse med adgangen til OCH Online ultimo 2025. Forudsætningen herfor er, at virksomhedens kunder kan nå at blive klar hertil. Dette er for at sikre, at der er mindst mulig negativ påvirkning af virksomhedens kunder i forbindelse med implementeringen af IP-filtrering."

Konsekvensanalyse:

Driftsudfald hos selskabet og hvilke konsekvenser selskabet ser, hvis selskabets database eller Online modul er er utilgængeligt.

OCH A/S
c/o Norlys
Ørestads Boulevard
DK-2300 København S
www.och.dk
CVR.nr. 18936909

- Der vil ikke være konsekvenser i forhold til, at telefoni virker. slutbrugere vil altså fortsat kunne ringe, sende beskeder og bruge data selvom selskabets database eller Online modul er ude af drift. Selskabet har ingen direkte indvirkning på driften af de enkelte telefoni-netværk.

- Det vil ikke være muligt at flytte numre mellem teleudbydere, der ikke er på samme netværk. Det kan eventuelt have økonomiske konsekvenser for både slutbrugere og teleudbydere blandt grundet kompensationsregler, hvortil slutbrugerne har adgang til en eventuel kompensation. Flyttes numre internt vil selskabets database ikke blive opdateret og et telefoni-nummer kan derfor ligge hos en anden teleudbyder end det, selskabet tror dette ligger hos. Da selskabets kunder, herunder Rigspolitiet, har egen kopi af selskabets database vil de kunne have forkerte oplysninger.

- Selskabet vil ved et driftsudfald på selskabets database udsende informationsmail og SMS til selskabets kunder og informere om driftsudfald, efterfølgende udsende statusopdateringer og slutlig besked om at der igen er adgang til selskabets database.

- Sker der driftsudfald på Online modulet, så vil selskabet også her gøre, som beskrevet i punktet ovenfor.

Ved større driftsudfald vil selskabet ligeledes give en information til Digitaliserings-styrelsen, regulator for telefoniområdet, hvormed selskabet proaktivt har informeret Styrelsen om situationen, blandt andet i tilfælde af, at Styrelsen bliver kontaktet af en slutbruger eller teleudbyder