



**TLP: WHITE/CLEAR**

# Leverandørsikkerhed i telesektoren

TeleDCIS

16.03.2026

# TLP: WHITE/CLEAR

## Indholdsfortegnelse

Indledning.....	2
1. Formål og afgrænsning .....	2
2. Dokumentets struktur og opbygning.....	2
3. Ledelsens ansvar for leverandørsikkerhed .....	3
4. Planlægningsfasen.....	3
4.1. Underretninger til SAMSIK om aftaleforhandlinger:.....	4
4.2. Indehold vedr. underretning til SAMSIK:.....	4
4.3. Foranstaltninger til styring af risici: .....	5
4.4. Kategorisering af Leverandører .....	6
4.5. Outsourcing (eventuelt til udlandet) .....	7
5. Kravstillelse.....	7
5.1. SMART princippet.....	8
5.2. Krav til Leverandør .....	8
6. Leverandørvalg .....	9
7. Kontrakten .....	10
8. Styring.....	11
8.1. Dokumentér organisationens behov for at føre kontrol med leverandøren.....	11
8.2. Udpeg en dedikeret rolle med ansvar for organisationens leverandørsikkerhed i forhold til opfyldelsen af sikkerhedskravene i kontrakten. ....	12
8.3. Før løbende kontrol med leverandørens opfyldelse af sikkerhedskravene i kontrakten efter behov og på baggrund af en risikovurdering. ....	12
8.4. Gennemfør løbende risikovurderinger med input fra leverandøren og eventuelle underleverandører. ....	12
8.5. Håndtér evt. sikkerhedshændelser og væsentlige ændringer hos kunden, leverandøren eller i omgivelserne, der kan påvirke sikkerheden i leverancen.....	12
8.6. Underretninger som berører leverandør- eller partnerforhold.....	13
9. Afslutning.....	14
9.1. Exit-klausuler, der bør indgå (best-practice afledt af lovens krav) .....	15
9.2. Hvilke exit-klausuler skal en leverandøraftale mindst dække? (BEK 621) .....	16
10. Bilag Ledelsesstyring af informationssikkerhed .....	16
11. Bilag Compliance-tjekliste .....	17
12. Bilag Vigtige exit klausuler efter "god practice" .....	18
13. Bilag Kildehenvisninger .....	19

# TLP: WHITE/CLEAR

## Indledning

Denne vejledning beskriver leverandørstyring i telesektoren og relaterer sig til krav i regulering, der implementerer NIS2 direktivet, samt krav i øvrigt i telereguleringen af relevans for leverandørsikkerhed, herunder leverandørstyring. Vejledningen skal understøtte arbejdet med at sikre et passende niveau af cybersikkerhed i henhold til lovgivningens bestemmelser.

Der er taget afsæt i tidligere dokument: Leverandørstyring\_220424.pdf og strukturen er bibeholdt gennem hele vejledningen. I de afsnit hvor den nye lovgivning er gældende er disse afsnit opdaterede.

## 1. Formål og afgrænsning

Denne vejledning er udarbejdet med det formål at simplificere og tydeliggøre arbejdet med leverandørsikkerhed i den danske telesektor i henhold til kravene i regulering på baggrund af NIS2 direktivet og gældende dansk teleregulering i øvrigt. Denne vejledning er målrettet de "væsentlige" udbydere med en mere restriktiv lovgivning hvortil der er skærpede krav end for "vigtige" udbydere. I takt med at cybertrusler mod kritiske infrastrukturer bliver mere avancerede og målrettede, er det nødvendigt med en systematisk og risikobaseret tilgang til leverandørsikkerhed. Angreb på leverandørkæder har i flere tilfælde kompromitteret kritiske systemer, hvilket understreger behovet for øget kontrol og dokumentation i samarbejdet med eksterne parter.

Telesektoren er udpeget som samfundskritisk og er dermed forpligtet til at sikre, at både egne og leverandørers aktiviteter lever op til kravene i telereguleringen.

Vejledningen skal give telesektorens aktører et "idékatolog" til leverandørsikkerhed og kan lette den komplekse opgave, det er at få de nødvendige dokumenter udarbejdet. Vejledningen har fokus på informationssikkerhedsaspekter og omfatter ikke de juridiske aspekter ved leverandørsikkerhed, herunder kontraktindgåelse og kontraktstyring, som de enkelte teleudbyderes juridiske afdelinger selv håndterer.

## 2. Dokumentets struktur og opbygning

Vejledningen er struktureret i overensstemmelse med de seks faser i leverandørsikkerhed, som også fremgår af SAMSIK's vejledning "Cybersikkerhed i leverandørforhold" og tilpasses den kontekst, der følger af Telelovgivningen.

De seks faser er:

1. Planlægning
2. Kravstillelse
3. Leverandørvalg
4. Kontrakten
5. Styring
6. Afslutning

**Kilde:** SAMSIK's vejledning "Cybersikkerhed i leverandørforhold"

# TLP: WHITE/CLEAR

## 3. Ledelsens ansvar for leverandørsikkerhed

Organisationens øverste ledelse har både det strategiske og operationelle ansvar for, at leverandørsikkerheden lever op til kravene i lovgivningen. Leverandørsikkerhed skal forankres som en integreret del af den samlede cybersikkerhedsgovernance, og ledelsen skal løbende kunne dokumentere og påvise, at kravene følges i praksis.

Ledelsesorganet har ansvaret for styringen af cybersikkerhedsrisici i deres virksomhed, organisation eller myndighed. Ansvar skal ses i forlængelse af de opgaver, bestyrelsen har for risikostyring ifølge selskabslovens § 115, og kan sammenlignes med den opgave, bestyrelsen ellers har ift. finansielle risici samt ikke-finansielle risici (f.eks. operationel risiko, teknologisk risiko m.m.). Ledelsesorganets opgaver ift. cybersikkerhed er således ikke anderledes end andre risikostyringsområder, hvor ledelsen skal vurdere og føre kontrol med virksomheden, organisationen eller myndighedens risici. Ledelsesorganet skal godkende cybersikkerhedsforanstaltningerne. Det vil sige de tekniske, operationelle og organisatoriske sikkerhedstiltag, som enheden træffer på baggrund af forpligtelserne i medfør af lovgivningen på området. Ledelsen skal derfor forholde sig til, hvad der udgør et passende sikkerhedsniveau for enhedens net- og informationssystemer set i forhold til enhedens risikoeksponering og den samfundsmæssige betydning af de tjenester og services, som enheden leverer. Det betyder bl.a., at ledelsen på et overordnet og strategisk niveau skal træffe beslutning om, hvilke foranstaltninger organisationen skal have, og hvornår beskyttelsen er tilstrækkelig.

*Ledelsen bør som minimum:*

- Sikre, at leverandørsikkerhed indgår i organisationens strategiske cybersikkerhedsmålsætninger og styringsstruktur.
- Allokere tilstrækkelige ressourcer og etablere klare roller og ansvar for leverandørsikkerhed.
- Sikre, at leverandørsikkerhed er en del af risikostyringen og den samlede cybersikkerhedsstrategi.
- Føre tilsyn med og følge op på hændelser, afvigelser og auditresultater i relation til leverandørsikkerhed.
- Sikre, at der sker en løbende tilpasning af krav og processer i takt med ændringer i trusselsbilledet eller leverandørforhold.

Ledelsen bør desuden være involveret i væsentlige beslutninger vedrørende risikovurderinger, leverandørklassificering og godkendelse af leverandører med høj kritikalitet, og/ eller leverandører med særlige risici, f.eks. geopolitiske.

Ved manglende efterlevelse af krav i lovgivningen kan organisationen og dens ledelse pålægges administrative sanktioner, herunder bøder.

**Kilde:** Lov nr. 435 "Lov om sikkerhed og beredskab i telesektoren" (TeleNIS), Kapitel 9 (§ 31).

**Kilde:** SAMSIK's vejledning "Ledelsens rolle og opgaver"

## 4. Planlægningsfasen

Planlægningsfasen bør følge en struktureret proces, der sikrer inddragelse af alle relevante parter i organisationen, dvs. i praksis både dem som står for indkøbet/aftalen og dem som efterfølgende skal drifte aftalen/produkterne indtil de eventuelt udfases. Dette sikrer, at organisationen etablerer

# TLP: WHITE/CLEAR

de nødvendige rammer og processer til at håndtere leverandørrelationer i overensstemmelse med gældende lovgivning og vejledninger.

Dokumentér interne og eksterne forhold vedrørende den planlagte outsourcing, der kan påvirke organisationens cyber- og informationssikkerhed.

Kortlæg organisationens forretningsprocesser med fokus på den underliggende it-infrastruktur, herunder datastrømme og indbyrdes afhængigheder.

Formulér en separat politik for organisationens styring af cyber- og informationssikkerhed i kunde-leverandørforhold ved outsourcing af it.

Etablér en intern organisation egnet til leverandørsikkerhed med veldefinerede roller, de fornødne ressourcer og kompetencer, dokumenterede processer og den nødvendige it-understøttelse. I organisationens håndtering af samarbejdet med leverandøren indgår ofte en række forskellige roller og funktioner, herunder:

- Ledelsen
- Informationssikkerhedskoordinator/it-sikkerhedsansvarlig
- Kontraktansvarlig
- Jura
- It-ansvarlig
- Data- og systemejer
- Databeskyttelsesrådgiver (DPO)

Foretag en risikovurdering med fokus på særlige risici ved den planlagte outsourcing, der kan påvirke organisationens cyber- og informationssikkerhed. Risikovurderingen skal være integreret i organisationens generelle risikostyring og gennemføres med udgangspunkt i en dokumenteret proces og metode.

**Kilde:** SAMSIK's vejledning "Cybersikkerhed i leverandørforhold"

## 4.1. Underretninger til SAMSIK om aftaleforhandlinger:

Væsentlige teleudbydere skal skriftligt underrette SAMSIK forud for, at der indgås forhandlinger om aftaler om:

- 1) anskaffelser, der omfatter eller påvirker kritiske netkomponenter, systemer og værktøjer, og
- 2) varetagelse af driften af teleudbyderens kritiske netkomponenter, systemer og værktøjer.

Væsentlige teleudbydere skal skriftligt underrette SAMSIK forud for, at der indledes forhandlinger om tillæg til eksisterende aftaler, som vedrører eller på grund af tillægget vil komme til at vedrøre kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf.

**Kilde:** BEK nr. 1069 "Bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed og beredskab i telesektoren"

## 4.2. Indehold vedr. underretning til SAMSIK:

Underretningen skal som minimum indeholde:

- 1) Hvilke kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf, som aftalen påtænkes at omfatte.
- 2) Aftalens påtænkte omfang.
- 3) Eventuel placering af opgaver uden for Danmark.

# TLP: WHITE/CLEAR

- 4) Eventuelle leverandører, der påtænkes inddraget i aftaleforhandlingerne.
- 5) Overordnet tidsplan for aftaleforhandlingerne.
- 6) Aftalens påtænkte varighed.

SAMSIK kan udstede påbud om, at væsentlige teleudbydere skal fremsende det endelige udkast til en aftale til SAMSIK forud for indgåelse af den endelige aftale.

En endelig aftale kan først indgås, når den væsentlige teleudbyder har modtaget en tilbagemelding fra SAMSIK. SAMSIK skal give tilbagemeldingen efter stk. 1 snarest muligt og senest 25 arbejdsdage efter, at SAMSIK har modtaget aftaleudkastet.

Hvis aftaleudkastet ændres efter indsendelse, skal det reviderede udkast ligeledes fremsendes, medmindre ændringerne udelukkende er foretaget som følge af SAMSIK's tilbagemelding. Desuden kan SAMSIK påbyde, at endelige aftaler skal fremsendes til orientering senest 10 arbejdsdage efter indgåelse.

**Kilde:** BEK nr. 1069 "Bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed og beredskab i telesektoren"

## 4.3. Foranstaltninger til styring af risici:

Teleudbydere skal styre risici i forhold til tab af tilgængelighed, autenticitet, integritet og fortrolighed i både net- og informationssystemer. Lovgivningen sætter krav til risikostyringen, herunder til en politik for risikoanalyse, som hvad angår vigtige og væsentlige teleudbydere skal være i overensstemmelse med en international anerkendt standard som fx ISO 27005. Det skal således fremgå af denne politik, hvordan teleudbyderne arbejder med risikostyring, herunder med risikovurderinger. Risici i forhold til leverandører / forsyningskæden skal indgå i de risikovurderinger, som teleudbydere skal lave.

Lovgivningen (TeleNIS) opstiller nogle minimumselementer, der skal adresseres ved risikostyringen, herunder krav til foranstaltninger til at styre risici:

1. Politikker for risikoanalyse og informationssystemsikkerhed.
2. Håndtering af hændelser.
3. Driftskontinuitet, herunder backupstyring og reetablering efter en katastrofe og krisestyring.
4. Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere.
5. Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.
6. Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici.
7. Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.
8. Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering.
9. Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.
10. Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos enheden, hvor det er relevant.

Der er i bekendtgørelserne til TeleNIS fastlagt yderligere, konkrete krav til foranstaltninger til at styre risici, herunder fx i forhold til sikringsplaner og fysiske foranstaltninger, logning, håndtering af

# TLP: WHITE/CLEAR

ændringer i systemer og udstyr, håndtering af hændelser og sårbarheder, backup og genskabelse af data, netværkssegmentering, forsyningssikkerhed og redundans.

I praksis vil det for punkt 4. betyde:

- ◆ Leverandørrisici skal indgå i teleudbyderens løbende risikovurdering og i foranstaltningerne til at styre risici.

Yderligere punkter som med fordel inddrages i risikovurderingen:

- Væsentlige forandringer hos leverandøren, fx geografisk flytning, konkurs, ejerskifte eller skift af underleverandør.
- Ændringer i geopolitiske forhold.
- Leverandørens bidrag til den samlede trussels- og risikovurdering – fx ved at dele viden om sårbarheder og kendte trusler.
- Uoverensstemmelse mellem organisationens og leverandørens sikkerhedsniveau og risikotolerance.
- Risiko for supply chain-angreb, fx via software eller hardware, som leverandøren leverer eller drifter.
- Fysisk og logisk adgang for leverandørens personale til organisationens aktiver.
- Indsigt i forretningskritiske processer, infrastruktur og procedurer, som leverandøren kan opnå.
- Leverandørens evne og vilje til at levere nødvendig dokumentation og til at imødekomme tilsyn og audit.
- Efterlevelse af regulatoriske krav (fx GDPR og telelovgivning).
- Kritikaliteten og følsomheden af systemer og data, som omfattes af leverancen.
- Exit-risici, herunder afhængighed, datamigrering og datasletning ved samarbejdets ophør.
- Konsekvenser ved multisourcing og potentielle konflikter mellem leverandører.

**Kilde:** Lov nr. 435 "Lov om sikkerhed og beredskab i telesektoren" (TeleNIS)

**Kilde:** BEK nr. 1069 "Bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed og beredskab i telesektoren"

**Kilde:** BEK nr. 621 "Bekendtgørelse om risikostyring og sikkerhed i telesektoren"

## 4.4. Kategorisering af Leverandører

Selvom telelovgivningen ikke ordret pålægger en "kategoriseringsmodel", følger det naturligt af kravene til risikostyring, at leverandører bør **klassificeres efter deres kritikalitet og risikoprofil** for drift og informationssikkerhed.

1. **Risikobaseret** – Når loven kræver, at alle foranstaltninger skal være "passende og forholdsmæssige", må udbyderen først vurdere, *hvor stor risiko den enkelte leverandør udgør*.
2. **Proportional** – Man kan kun vælge proportionale kontroller (fx kontraktkrav, audits, kontinuitetsplaner) hvis leverandørerne er **delt op efter kritikalitet**.
3. **Best practice** – Internationale standarder (ISO 27036-1, ENISA-guidance til NIS2) anbefaler netop en **tiering** (høj-, mellem-, lav-kritisk) som praktisk metode.

# TLP: WHITE/CLEAR

Virksomheden bør definere kriterier for, hvordan de udvælger leverandører eller tjenesteudbydere. Kriterierne kan omfatte:

- leverandørernes og tjenesteudbydernes cybersikkerhedspraksis, herunder deres procedurer for sikker udvikling.
- leverandørens eller tjenesteudbyderens evne til at opfylde virksomhedens cybersikkerhedsspecifikationer.
- klassifikationsniveau for de it-tjenester, it-systemer eller it-produkter, som leverandøren eller tjenesteudbyderen leverer, herunder leverandørens opfattelse af risikoen.
- leverandørens evne til at opretholde et passende niveau af forsyningsikkerhed.
- enhedens evne og mulighed for at vælge en alternativ leverandør og begrænse leverandørafhængighed.
- leverandørens økonomi og geopolitiske risici.

Kategoriseringen bør dokumenteres og løbende revurderes – særligt ved ændringer i leverandørforhold eller trusselsbilledet.

**Kilde:** Lov nr. 435 "Lov om sikkerhed og beredskab i telesektoren" (TeleNIS)

**Kilde:** SAMSIK's vejledning "Implementering af cybersikkerhedsforanstaltninger"

**Kilde:** BEK nr. 621 "Bekendtgørelse om risikostyring og sikkerhed i telesektoren"

## 4.5. Outsourcing (eventuelt til udlandet)

Outsourcing (eventuelt til udlandet) er tilladt, men loven kræver, at du har fuldt styr på leverandørrisikoen, forhåndsvarsler kritiske kontrakter, accepterer dansk tilsyn helt ud i kæden – og i særlige tilfælde holder visse systemer fysisk i Danmark.

Foranstaltningerne skal dække "forholdene mellem den enkelte teleudbyder og udbyderens direkte leverandører eller tjenesteudbydere" – altså også udenlandske drift-, cloud- eller support-partnere. Desuden kræves det at udbyderen:

- 1) underretter SAMSIK.
- 2) sender det endelige kontraktudkast.
- 3) afventer op til 25 arbejdsdage, før en aftale om væsentlige dele af net/drift må underskrives – uanset om leverandøren ligger i Danmark eller i et andet land.

SAMSIK kan, hvis det er "af væsentlig samfundsmæssig betydning", påbyde at udstyr til fx lovlig aflytning skal opsættes og drives fra Danmark. Dermed kan visse kernefunktioner ikke outsources til udlandet.

SAMSIK kan foretage kontrolbesøg, audits og stikprøver hos leverandører og underleverandører i relation til outsourcet aktivitet for både væsentlige og vigtige udbydere.

**Kilde:** Lov nr. 435 "Lov om sikkerhed og beredskab i telesektoren" (TeleNIS)

**Kilde:** Lov nr. 1156 "Lov om leverandørsikkerhed i den kritiske teleinfrastruktur"

**Kilde:** BEK nr. 1069 "Bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed og beredskab i telesektoren"

## 5. Kravstillelse

# TLP: WHITE/CLEAR

## 5.1. SMART princippet

Ved udarbejdelse af sikkerhedskrav til leverandøren anbefales det at anvende SMART-princippet: **Specifikke, Målbare, Anvisende, Relevante og Tidsbestemte krav.**

SMART-kriterierne sikrer, at kravene er operationelle, evaluerbare og målrettede, hvilket understøtter både udvælgelse og styring af leverandøren.

**Specifikke:** Krav skal formuleres konkret og entydigt, så det er tydeligt for leverandøren, hvordan de skal opfyldes. Undgå generelle formuleringer som "Leverandøren skal foretage backup af systemet". I stedet bør kravene specificere fx omfang, frekvens og opbevaringsmetode (online/offline).

**Målbare:** Krav skal kunne dokumenteres og evalueres objektivt. Undgå formuleringer med plads til fortolkning som "tilstrækkelig logning". Stil i stedet krav, som kan verificeres binært (opfyldt/ikke opfyldt), f.eks. antal logevents, logretention eller krav til automatiseret rapportering.

**Anvisende:** Krav bør være klare og handlingsanvisende. Start med "Leverandøren skal..." og undgå overlappende eller komplekse krav med mange delpunkter. Opdel i stedet kravene logisk og struktureret, så de fremstår som selvstændige forpligtelser.

**Relevante:** Krav skal baseres på den konkrete risikovurdering og være tilpasset leverancens karakter og kritikalitet. Undgå at genbruge ældre krav uden revision. Brug fx kravkataloger eller standarder som ISO/IEC 27001, NIST 800-53, CIS Controls og SAMSIK's vejledninger – men tilpas dem til konteksten.

**Tidsbestemte:** Krav bør angive faste tidspunkter, frekvenser eller deadlines. Undgå vage begreber som "løbende" eller "regelmæssigt" og brug i stedet konkrete målelige tidsangivelser såsom "ugentligt", "inden for 24 timer" eller "senest 5 arbejdsdage efter hændelse".

SMART-princippet styrker ikke blot kravstillelsen, men danner også grundlag for klar kontraktuel regulering, leverandøropfølgning og compliance-vurdering, jf. kravene i lovgivningen og SAMSIK's vejledninger (2025).

**Kilde:** SAMSIK's vejledning "Cybersikkerhed i leverandørforhold"

## 5.2. Krav til Leverandør

### Kravkatalog

Virksomheden kan udarbejde et katalog med generelle sikkerhedskrav, der kan indsættes i alle kontrakter med leverandører uanset leverancen. Kravene bør gøres generelle, så de er relevante i alle kontrakter og kan tilpasses til den konkrete leverance, hvilket bidrager til at sikre et grundlæggende sikkerhedsniveau på tværs af organisationens leverandører. Hvis virksomheden anvender et klassifikationssystem, bør der udarbejdes et kravkatalog for hvert klassifikationsniveau. Virksomheden kan dermed overføre sikkerhedskrav fra det relevante kravkatalog til kontrakten med leverandøren, således at sikkerhedsniveauet afspejler klassifikationsniveauet forbundet med leverancen.

En leverandør skal kunne levere (derfor vigtigt at der stilles krav):

# TLP: WHITE/CLEAR

- **Løbende hændelses- og beredskabsrapportering**  
Hvis en driftsleverandør bliver ramt af en hændelse, skal teleudbyderen straks kunne identificere og rapportere det.
- **Indhent-pligt**  
Udbyderen skal sikre sig kontraktuelt, at under-leverandører og andre netpartnere leverer de data, der kræves for at opfylde bekendtgørelsens rapporteringskrav.

Kort sagt: alle centrale leverandørforhold skal kunne dokumenteres og – når situationen kræver det – rapporteres hurtigt og detaljeret til SAMSIK.

*Kilde: SAMSIK's vejledning "Cybersikkerhed i leverandørforhold"*

*Kilde: BEK nr. 1069 "Bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed og beredskab i telesektoren"*

## 6. Leverandørvalg

Loven dikterer ikke en bestemt udbuds- eller evalueringsmetode, men den forpligter teleudbyderen til at vælge og styre leverandører ud fra grundig risikovurdering, myndigheds-involvering ved kritiske kontrakter og mulighed for tilsyn – og den giver staten vetoret i særlige sikkerhedsspørgsmål.

Valget af leverandør er en kritisk beslutning med væsentlig betydning for både sikkerhed, kvalitet og overholdelse af lovgivningsmæssige krav. Virksomheden bør derfor foretage en struktureret og dokumenteret vurdering af potentielle leverandører, baseret på deres evne til at opfylde både de formelle krav og de identificerede sikkerhedsbehov. Dette omfatter også vurdering af leverandørens robusthed, samarbejdsvillighed og modenhed i forhold til cybersikkerhed. Formålet med vurderingen er at sikre, at leverandøren kan levere cyber- og informationssikkerhed på et passende niveau – både i kontraktens løbetid og ved eventuelt ophør – i overensstemmelse med lovgivningen.

Virksomheden bør inddrage følgende faktorer i vurderingen af potentielle leverandører (Listen er ikke udtømmende):

- Leverandørens dokumenterede evne til at leve op til de stillede sikkerheds- og compliancekrav.
- Leverandørens organisatoriske og tekniske sikkerhedsforanstaltninger, herunder certificeringer (fx ISO/IEC 27001).
- Geografisk placering og retsligt domicil, herunder risiko for overførsel af data til tredjelande.
- Brug af underleverandører og deres rolle i den samlede leverance.
- Leverandørens accept af krav til audit, revision og samarbejde med tilsynsmyndigheder.
- Evne og vilje til at opretholde sikkerhed i hele aftalens levetid, herunder ophørsfasen.
- Leverandørens økonomiske soliditet og ejerstruktur, herunder risici ved ændringer i ejerskab.
- Historik for compliance og eventuelle tidligere kontraktbrud eller sikkerhedshændelser.
- Risiko for afhængighed eller leverandørlåsning ved længerevarende samarbejder.
- Transition fra tidligere leverandør (hvis relevant), herunder eventuelle overgangsordninger.
- Hvilke leverandører er kritiske for virksomhedens evne til at levere samfundsvigtige ydelser?
- Har virksomheden overblik over disse direkte leverandører, og har virksomheden behov for at kende leverandørers underleverandører?

# TLP: WHITE/CLEAR

- Hvilke leverandører udgør en single point of failure i forsyningskæden?
- Er leverandører af produktionsudstyr og automation sikkerhedsmæssigt vurderet? Eksempelvis på systemer med lang levetid, hvor der sjældent bliver opdateret firmware. Herunder også, hvordan det sikres, at leverandører, der opdaterer produktionssystemer, ikke utilsigtet bringer sårbarheder ind?
- Kan virksomheden skifte kritiske leverandører i tide ved f.eks. konkurs, opkøb eller sikkerhedsbrud? Har virksomheden alternative leverandører?

**Kilde:** Lov nr. 435 "Lov om sikkerhed og beredskab i telesektoren" (TeleNIS)

**Kilde:** BEK nr. 621 "Bekendtgørelse om risikostyring og sikkerhed i telesektoren"

**Kilde:** Lov nr. 1156 "Lov om leverandørsikkerhed i den kritiske teleinfrastruktur"

## 7. Kontrakten

*I overensstemmelse med risikovurderingen kan aftaler (kontrakter) med direkte leverandører eller tjenesteudbydere eksempelvis indeholde afsnit om:*

- krav om, at leverandøren og det leverede følger relevante sikkerhedskrav, lovkrav, eksempelvis sikkerhedsgodkendelser, fortrolighedsklausuler, standarder mv.
- hvilke færdigheder og eventuelle uddannelser, der kræves af leverandørens personale
- baggrundskontrol af leverandørens personale, hvis de beskæftiger sig med enhedens kritiske aktiver (i henhold til klassificeringen af aktiver og risikovurderingen)
- leverandørens forpligtelse til at underrette enheden om alle relevante hændelser, så snart de bliver opmærksomme på hændelsen, og til at bistå enheden med at overholde sine rapporteringsforpligtelser i tilfælde af væsentlige hændelser
- at direkte leverandører og tjenesteudbydere, hvis enheden er underlagt tilsyn, samarbejder med enheden om at bistå de sektoransvarlige myndigheder i forbindelse med udførelsen af deres opgaver
- enhedens ret til revision og/eller ret til at modtage revisionsrapporter fra leverandøren
- aftale om leveringstider på serviceydelser, herunder eventuelle reparationer
- forpligtelse til at håndtere sårbarheder, der udgør en risiko for cybersikkerheden i enhedens net- og informationssystemer
- underleverandører (hvis tilladt) og foranstaltninger for underleverandører
- leverandørens forpligtelser ved aftalens ophør, eksempelvis forpligtelse til at udlevere og bortskaffe data.

Nedenstående diagram viser sammenhængen mellem det samlede kontraktgrundlag og kravkataloget. Hovedkontrakten består af kontraktgrundlaget, alle tilhørende øvrige aftaledokumenter (inkl. ændringer, tillæg og allonger) er bilag hertil. Kravkataloget er en samling af de krav og forpligtelser, der relaterer sig til sikkerhedskrav og -kontroller.

# TLP: WHITE/CLEAR



Der er typisk angivet en rangorden af aftaledokumenter i kontrakten. Den juridiske tekst er fastsat i hovedkontrakten, mens næsten alt om governance/proces fremgår af bilagsmaterialet, fx aftalehåndbøger, sikkerhedsinstruks, licensbetingelser, servicemål, samarbejdsorganisation og ændringsprocedurer.

Mange andre former for dokumenter kan dog også definere, hvad der er aftalt. Bilagene giver forklaringer og forståelse for enkeltdele, tekniske elementer mv. og har detailregulering. Ydermere kan underbilag indeholde udspecificerede detaljer og informationer, der udgør fundamentet for konkrete forpligtelser. Underbilag er dog kun nødvendige i de komplekse og meget store kontrakter.

Konsekvensanalyse vedrørende databeskyttelse (DPIA - data protection impact assessment): GDPR stiller krav til, at den dataansvarlige sikrer gennemførelse af passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at din behandling er i overensstemmelse med databeskyttelsesforordningen. Konsekvensanalysen kan hjælpe til at identificere og begrænse de påviste risici og dermed generelt være med til at skabe bedre databeskyttelse for de registreredes rettigheder. (læs mere i Datatilsynets vejledninger). Der skal gennemføres en DPIA, hvis behandling af data sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder.

*Kilde: SAMSIK's vejledning "Implementering af cybersikkerhedsforanstaltninger"*

## 8. Styring

### 8.1. Dokumentér organisationens behov for at føre kontrol med leverandøren.

Manglende eller utilstrækkelig leverandørsikkerhed kan blandt andet føre til:

- Utilstrækkelig risikohåndtering hos leverandøren.
- Flere fejl, forsinkelser og mangler i leverancen.

# TLP: WHITE/CLEAR

- Leverandørens manglende overholdelse af kontrakten.
- Kundens manglende håndhævelse af kontrakten.
- Leverandørens nedprioritering af kunden til fordel for andre kunder.
- Stigende leverandørafhængighed.

## **8.2. Udpeg en dedikeret rolle med ansvar for organisationens leverandørsikkerhed i forhold til opfyldelsen af sikkerhedskravene i kontrakten.**

Cyber- og informationssikkerhed er en integreret del af kundens leverandørsikkerhed. Kunden bør derfor udpege en dedikeret rolle i organisationen med ansvar for at kontrollere leverandørens efterlevelse af sikkerhedskravene i kontrakten

## **8.3. Før løbende kontrol med leverandørens opfyldelse af sikkerhedskravene i kontrakten efter behov og på baggrund af en risikovurdering.**

Når aftalen mellem parterne er underskrevet, og samarbejdet går i gang, bør kunden løbende kontrollere leverandørens efterlevelse af sikkerhedskravene i kontrakten efter behov. Kundens kontrol med leverandøren kan foregå på forskellige måder og omfatte flere former for dokumentation og rapportering. Leverandørens dokumentation kan blandt andet bestå af skriftlige rapporter, erklæringer, risikovurderinger og styringsdokumenter. Derudover kan kontrollen omfatte en række aktiviteter såsom:

- Statusmøder mellem kunde og leverandør (faste møder eller ad hoc).
- Skriftlig rapportering til kunden (fast afrapportering eller ved anmodning).
- Tilsyn hos leverandøren (enten varslet eller uanmeldt besøg).
- Intern audit/gennemgang eller egenkontrol foretaget af leverandøren.
- Ekstern audit/gennemgang foretaget af kunden eller en uvildig tredjepart.
- It-revision foretaget af certificerede revisorer.
- Beredskabsøvelser med kunden som deltager eller observatør.
- Sikkerhedstekniske undersøgelser (også kaldet penetrationstests).

## **8.4. Gennemfør løbende risikovurderinger med input fra leverandøren og eventuelle underleverandører.**

Kunden skal løbende gennemføre risikovurderinger for at afdække, om sikkerhedsniveauet i kunde-leverandørforholdet skal justeres som følge af ændringer i risikobilledet.

## **8.5. Håndtér evt. sikkerhedshændelser og væsentlige ændringer hos kunden, leverandøren eller i omgivelserne, der kan påvirke sikkerheden i leverancen.**

I aftaleperioden kan der ske både uforudsete og planlagte ændringer hos kunden, leverandøren eller i deres omgivelser, som påvirker cyber- og informationssikkerheden forbundet med leverancen. Det er derfor vigtigt, at begge parter bidrager til at vedligeholde sikkerhedsniveauet i kunde-leverandørforholdet. Parterne bør løbende vurdere, dokumentere og håndtere væsentlige ændringer i aftaleperioden som en del af deres styring af cyber- og informationssikkerhed. Kunden bør sikre, at leverandøren følger rettidigt op på eventuelle ændringer ved at foretage fornødne justeringer og træffe supplerende sikkerhedsforanstaltninger i henhold til aftalen

*Sådan skal en leverandør styres:*

# TLP: WHITE/CLEAR

Styrings-område	Hvad du skal være særlig opmærksom på
<b>1. Risikovurdering før indgåelse</b>	Hvis drift helt eller delvist lægges hos tredjepart, skal leverandørrisikoen indgå i teleudbyderens egen risikovurdering, og leverandøren skal holde <b>samme sikkerhedsniveau</b> som udbyderen
<b>2. Aftalegrundlag (contract management)</b>	Kontrakten skal dække <i>alle</i> relevante sikkerhedskrav og løbende opdateres, når trusler eller løsninger ændrer sig
<b>3. Løbende verifikation</b>	Udbyderen skal sikre, at leverancer (og konfiguration) <b>stemmer overens med det aftalte</b> ; det kan ske via stikprøvekontroller proportionalt med risikoen
<b>4. Dokumenteret compliance-kontrol</b>	Der skal føres og kunne fremvises <b>dokumentation for, at informationssikkerhedskravene efterleveres</b> i samarbejdet
<b>5. Adgangs- og rettighedsstyring</b>	Myndigheden kan kræve styrket logisk adgangskontrol – inkl. proces for <b>kontrol med leverandørers adgang</b> til kritiske systemer
<b>6. Kapacitets- og kompetencebevarelse</b>	Selv ved outsourcing skal udbyderen <b>fastholde interne kompetencer</b> til at validere, at leverede driftsydelser holder det aftalte niveau
<b>7. Exit- og beredskabsplaner</b>	Der skal være procedurer for <b>hjemtagning</b> af outsourcete opgaver ved misligholdelse eller konflikt i udlandet
<b>8. Ekstra tiltag ved høj leverandørrisiko</b>	SAMSIK kan påbyde foranstaltninger, jf. navnlig lov 435 og bek. 621

## 8.6. Underretninger som berører leverandør- eller partnerforhold

Sådan bruges skemaet

- Punkterne B – E dækker hele kontraktlivscyklussen: fra idéfasen til den endelige aftale med en leverandør.
- Punkterne G – I sikrer, at leverandørforhold også håndteres under driftshændelser og kriser.
- Punkt A (påbud) giver SAMSIK mulighed for påbud, når de har brug for fuld leverandør-gennemsigtighed uanset situation.

#	Hvornår udløses underretningen?	Hvad skal leverandør-/partner-oplysningerne dække?	Frist / form	Hjemmel (BEK 1069)
<b>A</b>	Når SAMSIK udsteder <i>påbud om oplysninger</i> (gælder både væsentlige og vigtige teleudbydere)	• Liste over <i>eventuelle leverandører</i> , inkl. driftsleverandører • Geografisk placering af udbyderens <b>og leverandørers hardware &amp; supportcentre</b>	Inden for den tidsfrist, SAMSIK fastsætter; data kan kræves elektronisk	§ 2, stk. 2

# TLP: WHITE/CLEAR

<b>B</b>	Før forhandlinger om nye aftaler eller tillæg, der omfatter kritiske netkomponenter eller drift	Selve underretningen om, at forhandlinger indledes	Skal sendes <b>inden forhandlingerne starter</b>	§ 3, stk. 1-2
<b>C</b>	Samme underretning som B (indholdskrav)	Skal bl.a. oplyse: • <b>Eventuelle leverandører</b> der forventes inddraget (nr. 4)	Samtidig med underretningen i B	§ 4, nr. 4
<b>D</b>	Når aftaleudkast foreligger	Fremsende <i>endeligt udkast</i> til outsourcing-/anskaffelsesaftale	SAMSIK kan påbyde fremsendelse <b>før kontrakt</b> ; har derefter 25 arbejdsdage til svar	§ 5, stk. 1-2
<b>E</b>	Når aftalen er underskrevet	Fremsende den <b>endelige aftale</b>	Senest 10 arbejdsdage efter underskrift	§ 6
<b>F</b>	<i>Væsentlige ændringer i virksomheden</i> (opkøb, fusion, frasalg), der kan ramme udliciteret drift	Underretning inkl. <b>foreløbig risikoanalyse</b> af konsekvenserne for kritiske komponenter (kan omfatte leverandør-risici)	Senest 15 arbejdsdage efter, at ændringen er kendt	§ 7, stk. 1-2
<b>G</b>	Ved <i>væsentlige hændelser</i> der påvirker net/tjenester (fx større nedbrud)	Underretningen skal udfyldes i SAMSIKs skema, som bl.a. kræver info om <i>andre berørte teleudbydere</i> (leverandører kan være blandt dem)	Straks via den digitale selvbetjeningsløsning: <a href="https://virk.dk/">https://virk.dk/</a>	§ 8, stk. 1-4
<b>H</b>	Når udbyderen skal lave hændelses-rapporten i G	Skal <i>indhente oplysninger</i> fra andre teleudbydere på sit net for at kunne rapportere korrekt	Ingen særskilt frist – »i nødvendigt omfang«	§ 11
<b>I</b>	Ved <i>aktivering af internt beredskab</i> pga. hændelse	Løbende situationsrapporter skal indeholde bl.a. <b>oplysninger om andre berørte teleudbydere</b>	Først telefonisk straks (§ 12), derefter rapporter mindst hver 2. time (§ 13)	§ 12-13

**Kilde:** SAMSIK's vejledning "Cybersikkerhed i leverandørforhold"

**Kilde:** BEK nr. 621 "Bekendtgørelse om risikostyring og sikkerhed i telesektoren"

**Kilde:** BEK nr. 1069 "Bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed og beredskab i telesektoren"

## 9. Afslutning

Når aftalen ophører, bør virksomhedens cyber- og informationssikkerhed opretholdes under afviklingen af kunde-leverandørforholdet. Dette gælder uanset om driften overdrages til en anden leverandør, eller om virksomheden vælger selv at overtage driftsopgaven (insourcing).

Ved aftaleindgåelse bør ophørsbestemmelserne som minimum indeholde følgende elementer:

- Leverandørens forpligtelser og servicemål i afviklingsperioden, herunder ved opsigelse eller ophør grundet tvist.
- Virksomhedens krav til opretholdelse af cyber- og informationssikkerhed under overdragelsen til ny leverandør eller ved insourcing.
- En komplet fortegnelse over alle virksomhedens aktiver (inkl. backups), som opbevares hos leverandøren og som skal returneres, overdrages eller destrueres.

# TLP: WHITE/CLEAR

- Dokumenterede procedurer for tilbagelevering, overdragelse eller destruktion af aktiverne.
- Fortsat tavshedspligt for begge parter efter aftalens ophør.
- Leverandørens forpligtelse til aktivt at støtte en smidig overdragelse, herunder udlevering af dokumentation, vidensoverførsel og deltagelse i overdragelsesaktiviteter.

## 9.1. Exit-klausuler, der bør indgå (best-practice afledt af lovens krav)

Tema	Hvorfor nødvendigt i forhold til lovgivning
<b>1. Kontinuitet i overgangsperioden</b> • Leverandøren fortsætter drift og fejlhåndtering, indtil alt er overdraget.	Udbyderen skal kunne levere samfundsvigtige tjenester uden afbrud (risikobaseret/proportionelt krav).
<b>2. Exit-assistance</b> • Overførsel af konfigurationer, dokumentation, know-how og personaleoplæring.	Gør det muligt at skifte leverandør uden at svække sikkerheden – og sikrer, at ny leverandør kan godkendes af myndigheden.
<b>3. Retur / sletning af data, udstyr og kryptonøgler</b> • Tidsfrister, format, bekræftelse.	Beskytter net- og informationssystemers integritet efter ophør; reducerer residual-risiko.
<b>4. Fjernelse af adgange</b> • Bruger-ID'er, certifikater, API-nøgler, fjernadgang.	Hører under "passende tekniske foranstaltninger".
<b>5. Logs &amp; revisionsspor til rådighed</b> • Opbevaringsperiode og udleveringsformat.	SAMSIK kan som udgangspunkt kræve log-data.
<b>6. Audit-/inspektionsret under exit</b> • Fuld adgang for udbyder og myndighed til systemer, lokationer, personale.	Sikrer, at SAMSIK kan føre kontrol "helt ud i kæden", jf. §§ 19 og 22.
<b>7. Tids- og aktivitetsplan (milestones)</b>	Gør det målbart, om leverandøren lever op til sine exit-forpligtelser – og giver grundlag for sanktioner.
<b>8. Fortrolighed og sikkerhedsforpligtelser, der overlever ophør</b>	Hindrer viderebrug af data og IP, bevarer compliance.
<b>9. Sanktioner ved manglende exit-opfyldelse</b> • Bod, tilbageholdt betaling, erstatningsansvar.	Underbygger risiko-baseret proportionalitet; stærke incitament i de mest kritiske leverancer.

### Praktisk fremgangsmåde:

1. Indbyg exit-kravene fra start i alle udbud/forhandlinger – de skal være en del af kontraktudkastet, som sendes til SAMSIK (25-dages stand-still).
2. Sæt transitionstesten: Kun leverandører, der kan dokumentere evne + vilje til at levere punkt 1-9, bør vælges til "væsentlige dele".
3. Hold stikprøve-klausulen skarp – SAMSIK har ret til kontrolbesøg hos leverandør / underleverandør; kontrakten skal åbne døren.

# TLP: WHITE/CLEAR

4. Plan B for national placering – hvis SAMSIK kræver, at bestemte systemer (fx LI-udstyr) bliver i DK, skal exit-klausulen gøre det muligt at flytte disse dele hurtigt.

## 9.2. Hvilke exit-klausuler skal en leverandøraftale mindst dække? (BEK 621)

Kravtype	Hvor står det i BEK 621?*	Hvad bør aftalen derfor indeholde
Hjemtagning (re-insourcing) ved misligholdelse	§ 22, nr. 4	Leverandøren skal – uden meromkostninger – bistå med at flytte drift / data hjem eller til ny leverandør. Beskriv proces, tidsplan, milepæle.
Hjemtagning ved politisk/konflikt-risiko i leverandørland	§ 22, nr. 5	Ret til akut ophør og overdragelse. Indsæt krav om nødplan og beredskab for geografisk flytning.
Afvikling af systemer (installation, flytning, afvikling)	§ 11, stk. 1	Leverandøren skal følge udbyderens afviklings-procedurer, levere scripts / dokumentation og understøtte en overgangsperiode.
Datasletning / destruktion af backup-data	§ 14, stk. 2	Krav om sikker og verificerbar sletning (fx NIST 800-88), log-bevis samt frister (fx 30 dage efter ophør).
Transfer-assistance & kompetenceoverdragelse	§ 22, nr. 7 (krav om at udbyderen skal kunne validere driften)	Leverandøren forpligtes til videnoverdragelse, dokumentation, uddannelse af udbyder/ny leverandør og levering af konfig-filer, kildekode mv.
Underleverandørers medvirken	§ 22, nr. 6	Aftalen skal sikre, at også underleverandører medvirker til exit (datatilbagelevering, sletning, adgangslukning).

Bekendtgørelsen kræver, at kontrakten giver udbyderen **fuld kontrol ved ophør** – især mulighed for at hjemtage drift, få data sikkert slettet og modtage den assistance, der gør et leverandørskifte muligt uden driftsafbrydelse. Selve varigheder, formater og SLA-niveauer fastsætter virksomheden ud fra egen risikovurdering; men aftalen skal kunne dokumentere, at kravene kan opfyldes, hvis SAMSIK påbyder det.

Der bør være et punkt i kontrakten, som sikrer udbyders rettigheder overfor leverandøren og leverandørens bistand i tilfælde af et påbud fra SAMSIK om ophævelse af leverandøraftalen.

**Kilde:** SAMSIK's vejledning "Cybersikkerhed i leverandørforhold"

**Kilde:** Lov nr. 435 "Lov om sikkerhed og beredskab i telesektoren" (TeleNIS)

**Kilde:** BEK nr. 621 "Bekendtgørelse om risikostyring og sikkerhed i telesektoren"

## 10. Bilag Ledelsesstyring af informationssikkerhed

Emne	Beskrivelse og krav	Lovhenviisning
Ledelsessystem for informationssikkerhed	Opretholder leverandøren et ledelsessystem for informationssikkerhed baseret på ISO 27001 eller tilsvarende anerkendt standard? Inkluder evt. oplysninger om certificering og scope.	BEK 621 § 6

# TLP: WHITE/CLEAR

<b>Risikostyring</b>	Har leverandøren en risikostyringsproces baseret på ISO 27005 eller tilsvarende standard? Skal kunne dokumenteres og løbende ajourføres.	BEK 621 §§ 2 og 5
<b>Awareness, træning og uddannelse</b>	Sikrer leverandøren awareness-aktiviteter og træning af relevante medarbejdere og eventuelle underleverandører?	BEK 621 § 7 og LOV 435 § 5, stk. 1, og § 6, stk. 2
<b>Personrelaterede foranstaltninger</b>	Har leverandøren en proces for vurdering af behov for fx straffeattester eller sikkerhedsgodkendelse af medarbejdere?	ISO/IEC 27002:2022 kap. 6 og 7 og LOV 435 § 16, stk. 1
<b>Fysisk sikkerhed</b>	Er der implementeret relevante fysiske sikkerhedsforanstaltninger?	BEK 621 § 9
<b>Sårbarhedshåndtering</b>	Udføres regelmæssige sikkerhedstests og sårbarhedsscanninger, og findes der en opfølgingsproces?	BEK 621 § 13
<b>Incident management, business continuity og beredskab</b>	Har leverandøren procedurer for hændeshåndtering og beredskab? Herunder test af planer og hurtig underretning.	BEK 621 § 12 BEK 622 §§ 2 og 3 og 7
<b>Rapportering om risici</b>	Er der en proces for at underrette organisationen og myndigheder om trusler eller hændelser relateret til leverancen?	BEK 1069 §§ 7 og 8
<b>Løbende statusrapportering ved beredskab</b>	Findes der en aftalt struktur og frekvens for rapportering og samarbejds møder?	BEK 1069 § 13
<b>Løbende forbedringer</b>	Udfører leverandøren løbende opdateringer baseret på risikovurderinger, hændelser eller ændret lovgivning?	ISO 27001
<b>Revision</b>	Har organisationen ret til audit og kontrol af leverandørens efterlevelse af krav og regulering?	BEK 621 § 20
<b>Support</b>	Leverer leverandøren nødvendig teknisk og sikkerhedsmæssig support, herunder angivelse af tilgængelighed og sprog?	Anbefaling (kontraktligt krav)

## 11. Bilag Compliance-tjekliste

Lov / bekendtgørelse	Krav (kort forklaring)	Dokumentation	Ansvar
<b>BEK nr. 1069 af 27/08/2025 §§ 8, 12-14</b>	Underretning til SAMSIK om væsentlig hændelse – tidlig varsling (24 t), opfølgende (72 t) og slutrapport (≤ 1 md.) samt beredskabsaktivering	Hændelses- og logark, indsendte underretningsskemaer, korrespondance med SAMSIK	Leverandør (initiel), CISO / Sikkerhedsteam (opfølgning)
<b>BEK nr. 1069 § 2</b>	Myndigheders adgang til materiale og tilsyn; SAMSIK kan påbyde udlevering af net-/system-oplysninger	Kontrakt- og systemoversigter, tilsynslog	Ledelse / Juridisk afdeling
<b>BEK nr. 1069 §§ 3-7</b>	Risikovurdering før anskaffelse / outsourcing af kritiske komponenter – forudgående skriftlig godkendelse	Risikovurdering, SAMSIK-forhåndsgodkendelse	Informationssikkerhed / CISO
<b>BEK nr. 621 af 02/06/2025 kapitel 2-3, og LOV nr. 435 § 5</b>	Iværksættelse og løbende evaluering af passende tekniske, fysiske og organisatoriske cybersikkerheds-foranstaltninger (ISO 27001-baseret ISMS, logning, patching, hændeshåndtering)	Årlig leverandør- og teknisk rapport, SoA, evt. tredjeparts-audit	Leverandør / Indkøb / Informationssikkerheds-ansvarlig

# TLP: WHITE/CLEAR

<b>BEK nr. 621 § 3, stk. 3</b>	Ledelsens årlige vurdering og opdatering af informations-systemsikkerhedspolitikken (minimum én gang om året)	Samlet årlig statusrapport, opdateret politik	CISO / Ledelse
<b>BEK nr. 621 §§ 18-20</b>	Krav til leverandører og underleverandører i forsyningskæden; ansvar for kontrol, aftalekrav og stikprøver	Underleverandør-register, kontraktkrav, kontrolevidens	Indkøb / Kontraktansvarlig / CISO
<b>BEK nr. 1069 §§ 3, 6</b>	Underretning & godkendelse ved brug/ændring af kritiske netkomponenter	Komponentliste, indberetning, SAMSIK-godkendelsesbreve	Leverandør / Teknisk ansvarlig / Indkøb
<b>BEK nr. 621 §§ 18-20</b>	Risikostyring af leverandører og forsyningskæden (supply-chain-security)	Risikovurdering, kontrol- & opfølgingsrapporter	Informationssikkerheds-ansvarlig / Indkøb
<b>BEK nr. 1069 §§ 8, 12-14</b>	Frister & proces for hændelsesunderretning (24 t / 72 t / 1 md.)	Kvittering for indsendelse, hændelseslog	CISO / Beredskabsteam
<b>LOV nr. 434 af 06/05/2025 § 7 + LOV nr. 435 af 06/05/2025 § 6 for telesektoren</b>	Ledelsesorganets overordnede ansvar for cybersikkerhed og leverandørstyring	Governance-referater, risikovurderinger, ledelsesbeslutninger	Direktion / CISO / DPO

## 12. Bilag Vigtige exit klausuler efter "god practice"

Nedenfor får du en **praktisk tjekliste** over de vigtigste ophørs-/exit-klausuler, der bør stå i en leverandøraftale, hvis driften af forretnings- eller netkritiske systemer outsources. Listen er bygget på "god praksis" fra ISO/IEC 27036-2 (leverandør-livscyklus), ENISA's NIS2-implementeringsvejledning og krav fra GDPR art. 28 om databehandlere.

Sådan bruger du skemaet

1. **Tilpas varigheder** (exit-periode, supportvindue, datalagring) til jeres egen *Business Impact Analysis* og regulative krav.
2. **Bind underleverandørerne** tidligt – ellers er pass-through-klausulen ikke håndhævelig.
3. **Test exit-proceduren** årligt (table-top + teknisk restore-test), så "latent lock-in" opdages i tide.

Med disse klausuler står virksomheden juridisk stærkt og opfylder samtidig de mest anerkendte krav til informationssikkerhed, databeskyttelse og forretningskontinuitet ved leverandørophør.

#	Hvad klausulen bør omfatte	Hvorfor / reference
<b>1. Exit-plan &amp; tidslinje</b>	Leverandøren forpligtes til at udarbejde og følge en detaljeret <i>terminationsplan</i> med milepæle, ansvar, og minimumsvarsel for overgang (fx 3-6 måneder).	ISO 27036 angiver, at aftalen har både transition- og termination-processer (Mitrtech)

# TLP: WHITE/CLEAR

<b>2. Fortsat drift under overgang</b>	SLA'er videreføres i exit-perioden, så kritiske services ikke afbrydes; leverandøren leverer "best endeavours" support indtil overdragelsen er fuldt gennemført.	Terminationsmålet er at beskytte produkt-/serviceforsyningen under ophør (Mitrtech)
<b>3. Data-portabilitet &amp; retur</b>	Alle data (produktions-, konfig-, log- og metadata) skal leveres i aftalt, åbent format samt dokumenteret struktur, så modtager kan indlæse dem uden specialværktøj.	ENISA nævner "retrieval ... of the information" ved leverandørinsolvens eller ophør
<b>4. Datasletning &amp; attest</b>	Efter succesfuld transfer skal leverandøren slette alle kopier og levere sletteattest; controlleren kan kræve bevis.	GDPR art. 28(3)(g): "sletter eller returnerer alle persondata ... medmindre lov kræver opbevaring" (enzuzo.com)
<b>5. Transfer-assistance (personer &amp; viden)</b>	Navngivne specialister stilles til rådighed (fx 40 timer/uge i 4 uger) til knowledge-transfer, hånd-i-hånd-drift og evt. oplæring af ny leverandør.	ENISA angiver "assistance ... til den myndighedskompetente enhed" samt samarbejde ved audits
<b>6. Adgang til dokumentation &amp; kildekode</b>	Alt net-, system- og sikkerheds-dokumentation, IaC-scripts, konfigurationsfiler, licenser m.m. skal afleveres og overgå i brugs- (eller ejendoms-)ret.	ISO 27036 angiver, at information security controls og ansvar dokumenteres over hele exit-processen (Mitrtech)
<b>7. Returnering eller destruktion af aktiver</b>	Hardware, kryptonøgler, certifikater, adgangskort o.l. returneres eller destrueres sikkert – inkl. bevis (chain-of-custody).	ENISA angiver procedurer for "retrieval and disposal of the information" ved insolvens/ophør
<b>8. Pass-through til underleverandører</b>	Leverandøren garanterer, at samme exit-vilkår er indarbejdet i alle underleverandør-aftaler (flow-down).	ENISA peger på supply-chain-kontinuitet i NIS2 art. 21(2)(d) (cegal.com)
<b>9. Co-operation med tilsyn &amp; audit efter ophør</b>	Leverandøren skal fortsat stille sig til rådighed for myndigheds- og kundeaudit i en fastlagt periode (fx 12 måneder).	ENISA lister "obligation ... to fully cooperate with competent authorities" i kontraktens exit-klausuler
<b>10. Finansiell afregning &amp; sikkerhedsstillelse</b>	Klare regler for slutafregning, refusion af forudbetalte ydelser og evt. garantiholdback til dækning af manglende efterlevelse i exit-fasen.	Best-practice fra TPRM-rammer (ISO 27036-2, Clause 7.5) om "avoiding ... legal and regulatory impacts" (Mitrtech)
<b>11. Step-in-/continuity-ret</b>	Kunden kan midlertidigt overtage drift (eller lade ny leverandør gøre det) ved misligholdelse, konkurs eller force majeure.	Kravet om sikring af operational continuity i LOV 435, § 5, stk. 1, nr. 3
<b>12. Varster &amp; hæve-adgang</b>	Ordinært opsigelsesvarsel (fx 30-90 dage) + øjeblikkelig hæveadgang ved væsentligt sikkerhedsbrud, lovovertrædelser eller tab af myndighedsgodkendelse.	ENISA Guiden angiver Termination rights og notice periods

## 13. Bilag Kildehenvisninger

### Kildedokumentet fra 2024



Leverandørstyring  
\_220424.docx

- TeleDCIS's "Leverandørstyring" af 22.04.2024

### Vejledninger

- SAMSIK's vejledning "Cybersikkerhed i leverandørforhold" af 06.05.2025 - <https://www.cfcs.dk/link/8797b0bd1ba842ac8a524933fc554149.aspx>

# TLP: WHITE/CLEAR

- SAMSIK's vejledning "Anvendelsesområdet" af 2025 - <https://samsik.dk/wp-content/uploads/2025/06/SAMSIK-vejledning-om-anvendelsesområdet-2025.pdf>
- SAMSIK's vejledning "Hændelsesunderretning" af juni 2025 - <https://samsik.dk/wp-content/uploads/2025/06/SAMSIK-vejledning-om-handelsesunderretning-2025.pdf>
- SAMSIK's vejledning "Implementering af cybersikkerhedsforanstaltninger" af juni 2025 - <https://samsik.dk/wp-content/uploads/2025/06/SAMSIK-vejledning-til-implementering-af-cybersikkerhedsforanstaltninger-juni-2025.pdf>
- SAMSIK's vejledning "Ledelsens rolle og opgaver" af maj 2025 - <https://samsik.dk/wp-content/uploads/2025/06/SAMSIK-vejledning-om-ledelsens-rolle-og-opgaver-maj-2025.pdf>

## Love og bekendtgørelser

- Lov nr. 433 af 06/05/2025 (CER-Loven) "Lov om kritiske enheders modstandsdygtighed (CER-loven)" - <https://www.retsinformation.dk/eli/lta/2025/433>
- Lov nr. 434 af 06/05/2025 (NIS2-Loven) "Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven)" - <https://www.retsinformation.dk/eli/lta/2025/434>
- Lov nr. 435 af 06/05/2025 "Lov om sikkerhed og beredskab i telesektoren" (TeleNIS) - <https://www.retsinformation.dk/eli/lta/2025/435>
- Lov nr 1156 af 08/06/2021 (Telesikkerhedsloven) "Lov om leverandørsikkerhed i den kritiske teleinfrastruktur" - <https://www.retsinformation.dk/eli/lta/2021/1156>
- BEK nr. 620 "Bekendtgørelse om udpegning af kompetente myndigheder og digital kommunikation omfattet af NIS 2-loven" - <https://www.retsinformation.dk/eli/lta/2025/620>
- BEK nr 621 af 02/06/2025 "Bekendtgørelse om risikostyring og sikkerhed i telesektoren" - <https://www.retsinformation.dk/eli/lta/2025/621>
- BEK nr 622 af 02/06/2025 "Bekendtgørelse om beredskab og krisestyring i telesektoren" - <https://www.retsinformation.dk/eli/lta/2025/622>
- BEK nr. 1069 af 27/08/2025 "Bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed og beredskab i telesektoren" - <https://www.retsinformation.dk/eli/lta/2025/1069>

## Standarder

- ISO/IEC 27001:2022 – Information security management systems ([iso.org/standard/27001](https://www.iso.org/standard/27001))
- ISO/IEC 27002:2022 – Code of practice for information security controls ([iso.org/standard/27002](https://www.iso.org/standard/27002))
- ISO/IEC 27005:2022 – Information security risk management ([iso.org/standard/27005](https://www.iso.org/standard/27005))
- ISO/IEC 27036 – Information security for supplier relationships ([iso.org/standard/27036](https://www.iso.org/standard/27036))

# TLP: WHITE/CLEAR

## Trusselsvurderinger

- Styrelsen for Samfundssikkerhed "Cybertruslen mod telesektoren" af marts 2025 - <https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/-cybertruslen-mod-telesektoren-2025-.pdf>