Ministeriet for Samfundssikkerhed og Beredskab

Dato: 11-04-2025
Sagsnr. 2025 - 75
Akt-id.: 4480

UDKAST

til

Bekendtgørelse om risikostyring og sikkerhed i telesektoren

I medfør af § 5, stk. 3, 1. pkt., § 18, stk. 2 og 31, stk. 3 i lov nr. … af … om sikkerhed og beredskab i telesektoren fastsættes:

Kapitel 1
Definitioner

§ 1. I denne bekendtgørelse forstås ved:

1) Beredskabssituationer og andre ekstraordinære situationer: Situationer, hvor der allerede er, eller hvor der kan opstå større ulykker, katastrofer eller hændelser, herunder krise eller krig, og hvor der er risiko for påvirkning af udbuddet af net og tjenester.

2) Elektroniske kommunikationsnet: Transmissionssystem, uanset om det bygger på en permanent infrastruktur eller en centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til

radio- og tv-spredning, og kabel-tv-net, uanset hvilken type information der overføres.

3) Elektronisk kommunikationstjeneste: En tjeneste, som normalt ydes mod betaling via elektroniske kommunikationsnet, og som med undtagelse af tjenester, der består i tilrådighedsstillelse af eller udøvelse af redaktionel kontrol over indhold fremført via elektroniske kommunikationsnet og -tjenester, omfatter følgende typer tjenester:

a) internetadgangstjenester,

b) interpersonelle kommunikationstjenester og

c) tjenester, der udelukkende eller overvejende består i overføring af signaler, som f.eks. transmissionstjenester, der anvendes til levering af maskine-til-maskine-tjenester og til radio- og tv-spredning.

4) Hændelse: En begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare.

5) Håndtering af hændelser: Enhver handling og procedure, der tager sigte på at forebygge, opdage, analysere og inddæmme eller at reagere på og reetablere sig efter en hændelse.

6) Interpersonel kommunikationstjeneste: En tjeneste, som normalt ydes mod betaling, og som muliggør direkte interpersonel og interaktiv informationsudveksling via elektroniske kommunikationsnet mellem et afgrænset antal personer, hvor de personer, der indleder eller deltager i kommunikationen, bestemmer hvem modtageren eller modtagerne skal være, undtaget tjenester, der blot muliggør interpersonel og interaktiv kommunikation som en mindre støttefunktion, der er tæt knyttet til en anden tjeneste.

7) Kritiske netkomponenter, systemer og værktøjer: Operations support-systemer, network management-systemer og business support-systemer, der kan benyttes til at aflæse, ændre indhold af eller dirigere data, som relaterer sig til slutbrugere, samt hardware, firmware og software, der anvendes i eller i forbindelse med core-net i mobilnet, fastnet, internet samt radio- og tv-distributionsnet, eller i centrale routere og servere i backbonenettene eller i kontrolenheder, som anvendes til styring i mobilnettenes radionet.

8) Net- og informationssystem:

a) Et elektronisk kommunikationsnet, jf. nr. 2.

b) Enhver anordning eller gruppe af forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data.

c) Digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a og b med henblik på deres drift, brug, beskyttelse og vedligeholdelse.

9) Nærvedhændelse: En begivenhed, der kunne have bragt tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare, men som det lykkedes at forhindre, eller som ikke indtraf.

10) Offentligt elektronisk kommunikationsnet: Et elektronisk kommunikationsnet, som udelukkende eller overvejende bruges til udbud af elektroniske kommunikationstjenester, der er tilgængelige for offentligheden, og som danner grundlag for overførsel af information mellem nettermineringspunkter.

11) Offentligt tilgængelige elektroniske kommunikationstjenester: En elektronisk kommunikationstjeneste, jf. nr. 3, der stilles til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere eller teleudbydere.

12) Radiobaseret lokalnet: Et trådløst adgangssystem med lav effekt og lille rækkevidde, der har en lav risiko for at skabe interferens med andre sådanne systemer etableret i nærheden af andre brugere, og som på et ikkeeksklusivt grundlag anvender harmoniserede radiofrekvenser.

13) Sikkerhed i net- og informationssystemer: Net- og informationssystemers, jf. nr. 7, evne til, på et givet sikkerhedsniveau, at modstå enhver begivenhed, der kan være til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer.

14) Slutbruger: En bruger af net og tjenester, som ikke på kommercielt grundlag stiller de pågældende net og tjenester til rådighed for andre.

15) Teleudbyder: Den, der med et kommercielt formål stiller produkter af offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester til rådighed for andre.

16) Vigtige teleudbyder: en teleudbyder, der udgør en vigtig teleudbyder efter lov om sikkerhed og beredskab i telesektoren.

17) Væsentlig teleudbydere: en teleudbyder, der udgør en væsentlig teleudbyder efter lov om sikkerhed og beredskab i telesektoren.

Kapitel 2
Risikoanalyse, informationssystemsikkerhedspolitik mv.

Krav for teleudbydere

§ 2. Teleudbydere skal foretage og dokumentere en risikovurdering, der skal tage stilling til risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i deres net og informationssystemer.

Stk. 2. Drives teleudbyderens net- og informationssystemer helt eller delvis af en tredjepart, skal eventuelle risici forbundet hermed medtages i risikovurderingen efter stk. 1.

Stk. 3. På baggrund af risikovurderingen efter stk. 1 og 2 skal teleudbydere træffe passende foranstaltninger til sikring af tilgængelighed, autenticitet, integritet og fortrolighed i deres net og informationssystemer. I tilfælde omfattet af stk. 2 skal teleudbyderen sikre, at den pågældende tredjepart opretholder en tilsvarende sikkerhed i forhold til driftsleverancer til teleudbyderen.

Stk. 4. Risikovurderingen efter stk. 1 og 2, samt foranstaltninger efter stk. 3 skal løbende revurderes og tilpasses, herunder ved væsentlige ændringer i teleudbyderens virksomhed og i trusselsbilledet.

Krav for væsentlige og vigtige teleudbydere

§ 3. Væsentlige og vigtige teleudbyderes politik for informationssystemsikkerhed efter § 5, stk. 1, nr. 1 i lov om sikkerhed og beredskab i telesektoren, skal være i overensstemmelse med en international anerkendt standard, eksempelvis DS/ISO/IEC 27001 eller tilsvarende og skal beskrive de tekniske, operationelle og organisatoriske rammer for arbejdet med risikostyring af sikkerheden i net og informationssystemer.

Stk. 2. Væsentlige og vigtige teleudbydere skal sikre, at deres politik for informationssystemsikkerhed er kommunikeret til alle relevante medarbejdere.

Stk. 3. Væsentlige og vigtige teleudbydere skal løbende opdatere deres politik for informationssystemsikkerhed efter stk. 1, herunder ved væsentlige ændringer af teleudbydernes virksomhed og i trusselsbilledet. Der skal dog mindst én gang om året foretages en vurdering af behovet for opdatering af politikken. Politikken for informationssystemsikkerhed skal på den baggrund opdateres i fornødent omfang.

Stk. 4. Politikken for informationssystemsikkerhed efter stk. 1 skal beskrive teleudbydernes håndtering af beredskabssituationer og andre ekstraordinære situationer.

§ 4. Væsentlige og vigtige teleudbydere skal på baggrund af politikken for informationssystemsikkerhed efter § 3, på person- eller funktionsniveau, fastlægge roller og ansvar, for teleudbydernes arbejde med sikkerhed og risikostyring. Roller og ansvar skal være dokumenteret.

Stk. 2. Roller og ansvar for teleudbyderens arbejde med sikkerhed og risikostyring efter stk. 1 skal være kommunikeret til alle relevante medarbejdere hos teleudbyderne, samt til relevante samarbejdspartnere og leverandører.

§ 5. Væsentlige og vigtige teleudbyders politik for risikoanalyse efter § 5, stk. 1, nr. 1 i lov om sikkerhed og beredskab i telesektoren skal være i overensstemmelse med en international anerkendt standard, eksempelvis DS/ISO/IEC 27005 eller tilsvarende.

Stk. 2. Politikken for risikoanalyse skal dokumenteres samt opdateres, herunder ved væsentlige ændringer i teleudbydernes virksomhed eksempelvis opkøb, fusioner, frasalg og større omorganiseringer.

Stk. 4. Væsentlige teleudbyderes politik for risikoanalyse skal tage højde for, at teleudbyderne i videst muligt omfang skal opretholde udbuddet af net og tjenester i beredskabssituationer og i andre ekstraordinære situationer med henblik på at sikre samfundets teleforsyning.

§ 6. Væsentlige teleudbydere skal styre informationssikkerheden i net og informationssystemer gennem et ledelsessystem, efter en international anerkendt standard, eksempelvis DS/ISO/IEC 27001 eller tilsvarende.

Kapitel 3
Foranstaltninger til styring af sikkerhedsrisici i net og informationssystemer

§ 7. Væsentlige og vigtige teleudbydere skal orientere relevante medarbejdere og samarbejdspartnere om det aktuelle trusselsbillede, herunder de trusler, der kan påvirke teleudbyderens net- og informationssystemer.

§ 8. Væsentlige og vigtige teleudbydere skal til brug for sin politik for risikoanalyse efter § 5 etablere og vedligeholde register over teleudbyderens kritiske netkomponenter, systemer og værktøjer.

§ 9. Væsentlige og vigtige teleudbydere skal som en del af politikken for risikoanalysen efter § 5 etablere og vedligeholde sikringsplaner for teleudbydernes kritiske netkomponenter, systemer og værktøjer.

Stk. 2. Ved udarbejdelse af sikringsplaner efter stk. 1, skal væsentlige og vigtige teleudbydere som minimum tage stilling til logisk og fysisk adgangskontrol, fysisk perimetersikring, videoovervågning, brandsikring, klimasikring og relevante varslingssystemer for ovenstående.

Stk. 3. Væsentlige og vigtige teleudbydere skal desuden som en del af politikken for risikoanalyse efter § 5 etablere relevant responsberedskab vedrørende de i stk. 2 nævnte områder.

Logning

§ 10. Væsentlige og vigtige teleudbydere skal etablere procedurer for og implementere logning og monitorering med henblik på at sikre sporbarhed ved eventuelle hændelser.

Stk. 2. Logfiler skal sikres mod manipulation.

Stk. 3. Alene et begrænset antal særligt betroede medarbejdere må kunne ændre på, hvilke informationer der logges. Sådanne ændringer skal som minimum godkendes af en anden, af teleudbyderen autoriseret person, før de kan træde i kraft. Dette skal dokumenteres.

Stk. 4. Væsentlige og vigtige teleudbydere skal sikre, at al aktivitet i forbindelse med logisk adgang til kritiske netkomponenter, systemer og værktøjer udført af medarbejdere med administratorrettigheder logges med henblik på at sikre uafviselighed.

Stk. 5. Væsentlige og vigtige teleudbydere skal regelmæssigt gennemgå logfilerne med henblik på identifikation af mulige hændelser.

Stk. 6. Væsentlige teleudbydere skal anvende centraliserede og automatiserede løsninger til brug for logopsamling, loganalyse, monitorering og identifikation af hændelser.

Stk. 7. Styrelsen for Samfundssikkerhed kan dispensere fra kravene i stk. 2-6. Dispensationen kan betinges af, at væsentlige og vigtige teleudbydere implementerer nærmere fastsatte kompenserende foranstaltninger, som fastlægges af Styrelsen for Samfundssikkerhed.

Ændringer mv. i væsentlige og vigtige teleudbyderes systemer og udstyr

§ 11. Væsentlige og vigtige teleudbydere skal i fornødent omfang etablere procedurer for installation, flytning og afvikling af, og øvrige ændringer i deres net- og informationssystemer.

Stk. 2. Ved ændringer i kritiske netkomponenter, systemer og værktøjer skal væsentlige og vigtige teleudbydere foretage risikovurdering med henblik på at definere, hvilke tests der skal udføres forud for ændringen. De identificerede tests skal være gennemført, dokumenteret og evalueret inden ændringen gennemføres.

Stk. 3. Før der foretages ændringer efter stk. 2 skal der være etableret procedurer for genskabelse til en tidligere version af systemet eller udstyret, såfremt der opstår fejl i forbindelse med ændringen.

Foranstaltninger til håndtering af hændelser, identificering af sårbarheder m.v.

§ 12. Væsentlige og vigtige teleudbydere skal etablere og vedligeholde procedurer for håndtering af hændelser. Som led i etableringen og vedligeholdelsen af procedurer efter 1. pkt., skal væsentlige og vigtige teleudbydere sikre, at roller og ansvar for håndtering af hændelser er kendt og øvet af relevant personel. Procedurerne skal som minimum beskrive håndtering og kategorisering af hændelser, sikring af nødvendige informationer til brug for efterfølgende hændelsesanalyse samt intern og ekstern rapportering, herunder underretningsforpligtigelser.

§ 13. Væsentlige og vigtige teleudbydere skal til enhver tid holde sig orienteret om nye sårbarheder, der vil kunne have konsekvenser for teleudbydernes net og informationssystemer.

Stk. 2. Væsentlige og vigtige teleudbydere skal etablere og vedligeholde relevante procedurer for regelmæssig opdatering og patchning af net- og informationssystemer.

Stk. 3. Væsentlige og vigtige teleudbydere skal regelmæssigt gennemføre relevante tekniske tests for afdækning af potentielle sårbarheder, eksempelvis i form af sårbarhedsscanninger, med henblik på at sikre, at de iværksatte foranstaltninger i net og informationssystemer til enhver tid er passende og effektive.

§ 14. Væsentlige og vigtige teleudbydere skal etablere relevante procedurer for backup og genskabelse af data, og sikre at disse procedurer regelmæssigt afprøves. Procedurerne skal opdateres i relevant omgang, herunder blandt andet ved væsentlige ændringer i backupsystemernes opbygning.

Stk. 2. Procedurerne efter stk. 1 skal som minimum dokumentere backupdatas opbevaring, transport og destruktion.

§ 15. Væsentlige og vigtige teleudbydere skal sikre en hensigtsmæssig adskillelse mellem udbydernes net, herunder produktions-, administrations-, styrings- og testnet.

Stk. 2. Opdeling af væsentlige og vigtige teleudbyderes net i flere logiske net skal ske i overensstemmelse med internationalt anerkendte standarder.

§ 16. Væsentlige og vigtige teleudbydere skal, baseret på politikken for risikoanalyse efter § 5 sikre, at der i forhold til kritiske netkomponenter, systemer og værktøjer er etableret den nødvendige nødstrømsforsyning, redundans, understøttende forsyning eller anden sikring med tilsvarende virkning.

§ 17. Væsentlige og vigtige teleudbydere skal med udgangspunkt i teleudbyderens risikoanalyse sikre, at relevante sikkerhedsaspekter inddrages så tidligt som muligt ved anskaffelse, udvikling, ændring, vedligeholdelse og afvikling af netkomponenter, systemer og værktøjer, der anvendes i net- og informationssystemer.

Samarbejde

§ 18. Etableres der et samarbejde mellem to eller flere teleudbydere, hvoraf mindst én af teleudbyderne er en væsentlig teleudbyder, finder de krav, som en væsentlig teleudbyder skal efterleve efter denne bekendtgørelse, anvendelse på de dele af den væsentlige teleudbyders net-og informationssystemer, der er omfattet af aftalen.

Stk. 2. Den aftalepart, der driver de net-og informationssystemer, som samarbejdet efter stk. 1 vedrører, er ansvarlig for, at kravene hertil i lov om sikkerhed og beredskab i telesektoren, og regler udstedt i medfør heraf efterleves.

Stk. 3. Aftaleparterne skal, på baggrund af deres risikostyring efter kapitel 2, sikre at aftalegrundlaget omfatter alle relevante sikkerhedskrav til net-og informationssystemer omfattet af samarbejdet. Aftalegrundlaget skal i fornødent omfang opdateres, når der sker ændringer som påvirker, eller kan påvirke, sikkerheden i de net- og informationssystemer, der er omfattet af aftalen, negativt.

§ 19. Etableres der et samarbejde mellem en væsentlig eller vigtig teleudbyder og en leverandør, er den pågældende teleudbyder fortsat ansvarlig for, at kravene hertil i lov om sikkerhed og beredskab i telesektoren og regler udstedt i medfør heraf efterleves for de dele af samarbejdet, der vedrører eller har direkte indvirkning på teleudbyderens net- og informationssystemer.

Stk. 2. Teleudbyderen skal, på baggrund af deres risikostyring efter kapitel 2, sikre at aftalegrundlaget omfatter alle relevante sikkerhedskrav til net-og informationssystemer omfattet af samarbejdet. Aftalegrundlaget skal i fornødent omfang opdateres, når der sker ændringer som påvirker, eller kan påvirke, sikkerheden i net- og informationssystemer negativt.

Stk. 3. Teleudbyderen skal på baggrund af risikovurdering efter § 2 sikre, at der er overensstemmelse mellem aftalepartens leverancer, herunder konfigurationen af leverancerne, og det mellem parterne aftalte.

Stk. 4. Pligten efter stk. 3 kan opfyldes gennem en stikprøvekontrol, såfremt det står i forhold til teleudbyderens risikovurdering efter § 2.

§ 20. Ved etablering at et samarbejde efter §§ 18 og 19 skal de deltagende væsentlige og vigtige teleudbydere sikre, at der sker en dokumenteret kontrol af efterlevelsen af de informationssikkerhedskrav, der fremgår af aftalegrundlaget.

Kapitel 4
Påbud om konkrete foranstaltninger

§ 21. Styrelsen for Samfundssikkerhed kan, såfremt det er af væsentlig samfundsmæssig betydning eller hvis en betydelig trussel er identificeret, og det er nødvendigt for at afhjælpe en hændelse eller hindre en sådan i at forekomme, påbyde væsentlige og vigtige teleudbydere at træffe én eller flere af følgende foranstaltninger:

1) Gennemføre en risikovurdering, der tager stilling til risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i udbyderens net og informationssystemer, jf. § 2, stk. 1.

2) Etablering eller styrkelse af logisk adgangskontrol til nærmere angivne og særligt kritiske netkomponenter, systemer og værktøjer, herunder krav til proces for adgangsstyring og kontrol med leverandørers adgang, jf. §§ 9 og 10.

3) Etablering eller styrkelse af foranstaltninger til fysisk sikring af nærmere angivne og særligt kritiske netkomponenter, systemer og værktøjer, herunder fysisk adgangskontrol, jf. § 9.

4) Sikring af sporbarhed eller logning af fysisk eller logisk adgang til nærmere angivne og særligt kritiske netkomponenter, systemer og værktøjer, herunder krav om monitorering eller gennemgang af logfiler, jf. §§ 9 og 10.

5) Opdatering af kritiske netkomponenter, systemer og værktøjer til en nyere software eller firmwareversion, jf. § 13, stk. 2.

6) Udskiftning af kritiske netkomponenter, systemer og værktøjer, der på grund af udstyrsleverandørens udmelding af stop for nye sikkerhedsopdateringer og generelle opdateringer må anses for at være forældet., jf. § 17.

7) Iværksættelse af kryptering efter internationale anerkendte standarder eller best practice på kritiske netkomponenter, systemer og værktøjer, jf. § 5, stk. 1 nr. 8) i lov om sikkerhed og beredskab i telesektoren.

8) Sikring af, at leverancer af hardware, firmware eller software, der kan udgøre en sårbarhed i den pågældende teleudbyders net og informationssystemer, undersøges for sårbarheder, jf. § 13, stk. 3.

9) Sikring af nødstrøm og redundansfor kritiske netkomponenter, systemer og værktøjer samt backup af konfigurationsdata.

10) At udstyr, der benyttes til at foretage indgreb i meddelelseshemmeligheden, skal opsættes i og drives fra Danmark.

11) At udstyr, der benyttes til at foretage indgreb i meddelelseshemmeligheden, ikke må leveres af en leverandør, som er identisk med teleudbyderens primære leverandører af kritiske netkomponenter, systemer og værktøjer.

12) Sikring af, at indlejret funktionalitet, der vil kunne benyttes til at foretage indgreb i meddelelseshemmeligheden, fjernes fra en leverance af netkomponenter, systemer og værktøjer.

13) Indstationering af personale, der er sikkerhedsgodkendt af Styrelsen for Samfundssikkerhed, hos udenlandske leverandører, som en teleudbyder har outsourcet hele eller dele af udbyderens net og tjenester eller varetagelsen af driften heraf til. Styrelsen for Samfundssikkerhed kan i den forbindelse stilles krav om, at det indstationerede personale, såfremt dette er i overensstemmelse med national lovgivning, skal have adgang til alle relevante systemer og informationer hos leverandøren med henblik på at overvåge leverandørens varetagelse af driften og udføre sikkerhedskontrol for udbyderen.

§ 22. Styrelsen for Samfundssikkerhed kan, såfremt det er af væsentlig samfundsmæssig betydning, efter en konkret vurdering påbyde væsentlige teleudbydere at foretage en eller flere af følgende foranstaltninger:

1) Gennemførelse af uafhængig sikkerhedsevaluering i forbindelse med leverancer af kritiske netkomponenter, systemer og værktøjer fra en specifik leverandør, såfremt den pågældende leverandør eller den pågældende leverance ud fra en generel sikkerhedsmæssig betragtning eller det aktuelle trusselsbillede vurderes at udgøre en særlig sikkerhedsrisiko. Styrelsen for Samfundssikkerhed kan i den forbindelse stille krav om, at sikkerhedsevalueringen gennemføres af et anerkendt evalueringsorgan, efter en anerkendt international standard og inden for nærmere fastsatte rammer.

2) Gennemførelse af intern eller ekstern teknisk sikkerhedsanalyse ved begrundet mistanke om en konkret sikkerhedshændelse.

3) Sikring af, at der ikke kan etableres direkte elektroniske supportforbindelser mellem en leverandør og en teleudbyder, såfremt den pågældende leverandør ud fra en generel sikkerhedsmæssig betragtning eller det aktuelle trusselsbillede vurderes at udgøre en særlig trussel.

4) Sikring af, at der på teleudbyderens foranstaltning i tilfælde af misligholdelse af en kontrakt om outsourcing kan ske hjemtagning af opgaver, der er outsourcede til en udenlandsk leverandør. Der kan herunder stilles krav om, at teleudbyderen skal have procedurer for hjemtagning af outsourcede områder.

5) Sikring af, at der på teleudbyderens foranstaltning, i tilfælde af risiko for en konflikt i de områder eller lande, hvortil der er sket outsourcing kan ske hjemtagning af outsourcede opgaver. Der kan herunder stilles krav om, at teleudbyderen skal have procedurer for hjemtagning af outsourcede områder.

6) Sikring af, at alle foranstaltninger i medfør af denne bekendtgørelse, der udføres af eksterne leverandører i forbindelse med outsourcing skal godkendes af teleudbyderen.

7) Fastholdelse af de nødvendige kompetencer hos teleudbyderen, hvis drift af net- og informationssystemer outsources, til at kunne foretage en kvalitativ validering af, at den leverede driftsydelse svarer

til det aftalte. Der kan herunder stilles krav om, at teleudbyderen skal fastholde de nødvendige kompetencer til at gennemføre risikovurdering efter § 2.

8) Sikring af, at konfiguration af nærmere bestemte kritiske netkomponenter, systemer og værktøjer på baggrund af nærmere angivne konkrete trusler og sårbarheder sker i henhold til nærmere fastsatte internationale standarder eller anbefalinger fra Styrelsen for Samfundssikkerhed.

Kapitel 5
Straffebestemmelser og ikrafttrædelse

§ 23. Med bøde straffes, medmindre strengere straf er forskyldt efter den øvrige lovgivning, den, der

1) overtræder §§ 2-12, § 13, stk. 2 og 3, §§ 14-20, eller

2) undlader at efterkomme et påbud efter §§ 21 eller 22.

Stk. 2. Der kan pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

§ 24 Bekendtgørelsen træder i kraft den 1. juli 2025.

Ministeriet for Samfundssikkerhed og Beredskab, den …

Torsten Schack Pedersen

/

Kristoffer Aagren