FOLKETINGSTIDENDE A

FOLKETINGET

Lovforslag nr. **L 119** Folketinget 2015-16

Fremsat den 11. februar 2016 af finansministeren (Claus Hjort Frederiksen)

Forslag

til

Lov om supplerende bestemmelser til forordning om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked

Anvendelsesområde

§ 1. Denne lov finder anvendelse på tillidstjenesteudbydere, som udbyder tillidstjenester og er etableret på det danske marked, som er omfattet af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (eIDAS-forordningen).

Kontrol og straf m.v.

§ 2. Digitaliseringsstyrelsen påser overholdelsen af eIDAS-forordningen og regler fastsat i medfør af eIDAS-forordningen. Digitaliseringsstyrelsen påser endvidere overholdelsen af denne lov og regler fastsat i medfør af loven.

§ 3. Finansministeren kan fastsætte nærmere regler om sikkerhedskrav til tillidstjenesteudbydere.

§ 4. Digitaliseringsstyrelsen er ansvarlig for tilsynsopgaver i Danmark i medfør af eIDAS-forordningens artikel 17.

Stk. 2. Finansministeren kan fastsætte nærmere regler om Digitaliseringsstyrelsens tilsyn efter stk. 1, herunder bestemmelser om indholdet af overensstemmelsesvurderingsrapporter udstedt i henhold til eIDAS-forordningens artikel 21, stk. 1.

§ 5. Myndigheder og personer, der udøver opgaver efter eIDAS-forordningens artikel 17 og 20, samt enhver, der i øvrigt yder bistand hertil, er under ansvar efter straffelovens §§ 152-152 f forpligtet til at iagttage ubetinget tavshed over for uvedkommende med hensyn til oplysninger om tillidstjenesteudbydernes systemers tekniske og sikkerhedsmæssige indretning samt processer for opretholdelse, vedligeholdelse og drift af sikkerheden omkring systemerne.

§ 6. Medmindre strengere straf er forskyldt efter anden lovgivning, straffes med bøde den, der

1) ikke overholder sikkerhedskrav til tillidstjenesteudbydere, jf. eIDAS-forordningens artikel 19, stk. 1
2) ikke overholder underretningspligt for tillidstjenesteudbydere, jf. eIDAS-forordningens artikel 19, stk. 2 eller
3) afgiver urigtige eller vildledende oplysninger til Digitaliseringsstyrelsen.

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

Ændringer i anden lovgivning

§ 7. I lov om fragtaftaler ved international vejtransport, jf. lovbekendtgørelse nr. 1122 af 18. september 2015, foretages følgende ændring:

1. I *§ 6, stk. 5,* ændres »lov om elektroniske signaturer« til: »forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF«.

Ikrafttrædelse m.v.

§ 8. Loven træder i kraft den 1. juli 2016.

Stk. 2. Samtidig hermed ophæves lov nr. 417 af 31. maj 2000 om elektroniske signaturer.

AE002274

Finansmin.,
Digitaliseringsstyrelsen

Bemærkninger til lovforslaget

Almindelige bemærkninger

2. Indledning

Området omkring elektroniske signaturer har hidtil været reguleret af direktiv 1999/93/EF om elektroniske signaturer. Direktivet blev implementeret i dansk ret ved lov nr. 417 af 31. maj 2000 om elektroniske signaturer. I medfør af loven er der udstedt to bekendtgørelser, henholdsvis bekendtgørelse nr. 923 af 5. oktober 2000 om sikkerhedskrav m.v. til nøglecentre og bekendtgørelse nr. 922 af 5. oktober 2000 om nøglecentres og systemrevisionens indberetning af oplysninger til Telestyrelsen.

Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (eIDAS-forordningen), skal erstatte det eksisterende direktiv om elektroniske signaturer, 1999/93/EF, men har et bredere anvendelsesområde, idet forordningen i tillæg til regulering af elektroniske signaturer også regulerer en bredere gruppe af elektroniske tillidstjenester samt elektroniske identiteter og dokumenter.

Baggrunden for forordningen er således, at lovgivning om elektroniske signaturer samt gensidig anerkendelse af elektronisk identifikation og autentifikation er nøgletiltag i Den digitale dagsorden for Europa, og at den eksisterende EU-lovgivning udelukkende dækker elektroniske signaturer. Endelig var der identificeret en opsplitning af markedet, idet der var forskellige regler gældende for tillidstjenesteudbydere afhængig af, hvilken medlemsstat de leverede en ydelse i. eIDAS-forordningen forventes at harmonisere området og derved skabe større tryghed, når der interageres på tværs af grænser.

Dette lovforslag fremsættes som supplement til bestemmelserne i eIDAS-forordningen med henblik på at styrke tilliden til elektroniske transaktioner på det danske marked ved at supplere det fælles grundlag for sikker elektronisk interaktion mellem borgere, virksomheder og offentlige myndigheder og derved øge effektiviteten i offentlige og private onlinetjenester, elektronisk forretningsførelse og elektronisk handel i Danmark.

Lovforslaget vil medføre ophævelse af lov om elektroniske signaturer og de to bekendtgørelser, der har hjemmel i denne. Ophævelsen skyldes, at eIDAS-forordningen har umiddelbar retsvirkning i Danmark, og at lov om elektroniske signaturer samt bekendtgørelse nr. 923 af 5. oktober 2000 om sikkerhedskrav m.v. til nøglecentre og bekendtgørelse nr. 922 af 5. oktober 2000 om nøglecentres og systemrevisionens indberetning af oplysninger til Telestyrelsen, som regulerer det samme område, derfor skal ophæves.

Lovforslaget tilsigter også at udpege det nationale tilsynsorgan, regulere sanktionering af tillidstjenesteudbydere, tavshedspligt for de persongrupper, der beskæftiger sig med tilsyn med tillidstjenesteudbydernes sikkerhedsmæssige indretning og give finansministeren bemyndigelse til på nationalt plan at fastsætte formelle detaljer omkring de sikkerheds- og tilsynsmæssige rammer.

eIDAS-forordningen blev vedtaget den 23. juli 2014, og den finder som udgangspunkt anvendelse fra den 1. juli 2016.

Forordningsgrundlaget for lovforslaget er: Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (eIDAS-forordningen).

3. Baggrund for lovforslaget

Baggrunden for lovforslaget er at sikre opfyldelse af de krav eIDAS-forordningen stiller til medlemsstaterne og samtidig give mulighed for at tilpasse formelle krav til sikkerhed og tilsyn løbende i forhold til udviklingen på området.

I henhold til artikel 288 i TEUF-traktaten gælder eIDAS-forordningen umiddelbart i hver medlemsstat. Gengivelser af bestemmelser fra eIDAS-forordningen i loven er således udelukkende begrundet i praktiske hensyn og berører ikke den nævnte forordning.

Den gældende lov om elektroniske signaturer implementerer direktiv 1999/93/EF om en fællesskabsramme for elektroniske signaturer, herefter kaldet direktivet, som blev sat i kraft den 1. oktober 2000. Lovens formål er at fremme en sikker og effektiv anvendelse af elektronisk kommunikation gennem fastsættelse af krav til visse elektroniske signaturer

og til nøglecentre, der udsteder certifikater til elektroniske signaturer. Lov om elektroniske signaturer er specifikt tilpasset elektroniske signaturer og forhold, der berører disse.

Da eIDAS-forordningen erstatter og tilbagekalder direktivet, og da eIDAS-forordningen regulerer såvel elektroniske signaturer som en række yderligere tillidstjenester, er det nødvendigt med denne lov at ophæve lov om elektroniske signaturer. Dette bevirker, at visse områder vil være utilstrækkeligt regulerede. Det foreslås derfor i nærværende lovforslag, at der gives bemyndigelse til finansministeren til at fastsætte nogle formelle krav til tilsyn og sikkerhed, der tidligere var fastsat med hjemmel i lov om elektroniske signaturer. Lovforslaget indeholder desuden en bestemmelse om tavshedspligt for myndigheder og personer, der udøver opgaver efter eIDAS-forordningens artikel 17 og 20 om tilsynsorganer og tilsyn med tillidstjenesteudbydere, samt enhver, der i øvrigt yder bistand hertil.

Det følger af eIDAS-forordningens artikel 16, at de enkelte medlemsstater skal fastsætte regler om sanktioner for overtrædelser af eIDAS-forordningen. Det er et krav, at sanktionerne er effektive, står i et rimeligt forhold til overtrædelsen og har afskrækkende virkning.

Det fremgår af eIDAS-forordningens artikel 17, stk. 1, 1. pkt., at hver medlemsstat skal udpege et tilsynsorgan, der er hjemmehørende på dens område.

eIDAS-forordningen har umiddelbar retsvirkning i Danmark, og det er derfor nødvendigt at ophæve lov om elektroniske signaturer, bekendtgørelse nr. 923 af 5. oktober 2000 om sikkerhedskrav mv. til nøglecentre, bekendtgørelse nr. 922 af 5. oktober 2000 om nøglecentres og systemrevisionens indberetning af oplysninger til Telestyrelsen.

Det fremgår af eIDAS-forordningen, at den træder i kraft i etaper. Hovedparten træder i kraft den 1. juli 2016, men visse bemyndigelsesbestemmelser trådte allerede i kraft 17. september 2014. Nedenfor findes en redegørelse for indholdet af de bestemmelser, der allerede er trådt i kraft, og som er relevante for dette lovforslag.

eIDAS-forordningens artikel 17, stk. 8, bestemmer at Kommissionen ved hjælp af gennemførelsesretsakter kan fastlægge formater og procedurer for rapporteringen i medfør af eIDAS-forordningens artikel 17, stk. 6.

Kommissionen har ved fremsættelsen af lovforslaget ikke udnyttet bemyndigelsen til via gennemførelsesretsakter at fastlægge sådanne formater og procedurer for tilsynsorganers rapportering til Kommissionen om det foregående kalenderårs primære tilsynsvirksomhed sammen med en sammenfatning af de indberetninger af brud på sikkerheden, som er modtaget fra tillidstjenesteudbyderne i overensstemmelse med eIDAS-forordningens artikel 19, stk. 2.

eIDAS-forordningens artikel 19, stk. 4 bestemmer, at Kommissionen ved gennemførelsesretsakter kan specificere tillidstjenesteudbyderes sikkerhedsforanstaltninger yderligere og vedtage formater og procedurer, herunder tidsfrister, for tillidstjenesteudbyderes underretning i tilfælde af brud på sikkerheden. Et eksempel på en tillidstjenesteudbyder i dansk kontekst er Nets DanID A/S, som udsteder den offentlige digitale signatur NemID.

Kommissionen har ved fremsættelsen ikke benyttet sig af muligheden for ved gennemførelsesretsakter yderligere at specificere eller vedtage formater og procedurer, herunder tidsfrister for tillidstjenesteudbyderes rapportering af konstaterede brud på sikkerheden eller tab af integritet, som har en væsentlig indvirkning på den udbudte tillidstjeneste eller de berørte personoplysninger.

eIDAS-forordningens artikel 21, stk. 4 bestemmer, at Kommissionen ved hjælp af gennemførelsesretsakter kan fastlægge formater og procedurer vedrørende kvalificerede tillidstjenesteudbyderes anmeldelse af hensigt om at udbyde en kvalificeret tillidstjeneste til tilsynsorganet og indsendelse af overensstemmelsesvurderingsrapport udstedt af et overensstemmelsesvurderingsorgan. Et overensstemmelsesvurderingsorgan vil typisk være et konsulenthus, der gennem akkreditering har opnået ret til at vurdere en tillidstjenesteudbyders overensstemmelse med eIDAS-forordningens krav. Resultatet af overensstemmelsesvurderingsorganets overensstemmelsesvurdering vil være en overensstemmelsesvurderingrapport.

Kommissionen har ved fremsættelsen ikke benyttet sig af muligheden for ved hjælp af gennemførelsesretsakter at fastlægge formater og procedurer for kvalificerede tillidstjenesteudbyderes anmeldelse af hensigt om at udbyde en kvalificeret tillidstjeneste til tilsynsorganet og indsendelse af overensstemmelsesvurderingrapport udstedt af et overensstemmelsesvurderingsorgan.

Det forhold, at der ikke er anført nogen endelig dato for Kommissionens nærmere regulering af de anførte områder danner baggrund for lovforslagets bestemmelser herom.

4. Lovforslagets indhold

4.1 Udpegning af tilsynsorgan.

4.1.1 Gældende ret

Det følger af eIDAS-forordningens artikel 17, stk. 1, 1. pkt., at hver medlemsstat skal udpege et tilsynsorgan, der er hjemmehørende på dens område.

Det forhold, at eIDAS-forordningen er ny, bevirker, at der på nuværende tidspunkt ikke eksisterer gældende ret, som dækker helt samme område.

Lov om elektroniske signaturer regulerer dog kvalificerede elektroniske signaturer og overlapper således delvist forhold, der reguleres i eIDAS-forordningen. I lov om elektroniske signaturer reguleres tilsyn med nøglecentre i kapitel 9. Det fremgår således, at Telestyrelsen påser overholdelse af loven og bestemmelser udstedt i medfør af loven.

4.1.2 Ministeriets overvejelser og den foreslåede ordning

Telestyrelsen eksisterer ikke længere, men opgaverne henhører i dag under Digitaliseringsstyrelsen. Med denne lov udpeger Finansministeriet derfor Digitaliseringsstyrelsen som tilsynsorgan i forhold til eIDAS-forordningen.

Digitaliseringsstyrelsen har i dag til opgave
- at modtage anmeldelse fra nøglecentre
- at fastsætte en tidsfrist for opfyldelse af påbud
- at modtage rapporter fra nøglecentre og fastsætte frist for indsendelse
- at fastsætte nærmere regler vedrørende nøglecentres rapporter samt om systemrevisionens gennemførelse i nøglecentre
- at udstede påbud om anmeldelse, rapportering og nøglecentres overensstemmelse med loven eller bestemmelser udstedt i medfør af loven
- at fastsætte tidsfrister for opfyldelse af påbud
- at pålægge nøglecentre tvangsbøder med henblik på at gennemtvinge påbud
- at kræve gennemførelse af ekstraordinær systemrevision og udpege systemrevisor
- at fratage nøglecentre retten til, at anvende betegnelsen kvalificerede certifikater
- at sikre systemrevisors habilitet
- at behandle oplysninger afgivet fra systemrevisor uden nøglecentrets accept.

Det foreslås i lovforslaget, at Digitaliseringsstyrelsen påser overholdelse af eIDAS-forordningen og regler fastsat i medfør af eIDAS-forordningen samt lovforslaget og regler fastsat i medfør af dette.

Rollen som tilsynsorgan indebærer, at Digitaliseringsstyrelsen skal føre tilsyn med tillidstjenesteudbydere, der er etableret i Danmark, for ved hjælp af forudgående og efterfølgende tilsynsvirksomhed at sikre, at disse tillidstjenesteudbydere og de tillidstjenester, de udbyder, opfylder kravene i eIDAS-forordningen.

Digitaliseringsstyrelsen skal således føre et proaktivt tilsyn med kvalificerede tillidstjenesteudbydere ved at modtage anmeldelser om tilsyn og overensstemmelsesvurderingsrapporter om kvalificerede tillidstjenester. Det proaktive tilsyn indebærer, at Digitaliseringsstyrelsen af egen drift skal iværksætte tilsyn med kvalificerede tillidstjenesteudbydere, der er etableret i Danmark.

Derudover skal Digitaliseringsstyrelsen føre et reaktivt tilsyn, herunder om nødvendigt gribe ind over for ikke-kvalificerede tillidstjenesteudbydere, der er etableret i Danmark. Det skal ske ved hjælp af efterfølgende tilsynsvirksomhed, når der underrettes om, at disse ikke-kvalificerede tillidstjenesteudbydere eller de tillidstjenester, de udbyder, angiveligt ikke opfylder kravene i eIDAS-forordningen.

Digitaliseringsstyrelsen skal med andre ord føre et reaktivt tilsyn med ikke-kvalificerede tillidstjenesteudbydere, da disse ikke er forpligtede til at anmelde deres tillidstjenester eller aflevere overensstemmelsesvurderingsrapporter i medfør af eIDAS-forordningen.

Digitaliseringsstyrelsen får til opgave
- at rapportere til de øvrige medlemsstater og Kommissionen i tilfælde af sikkerhedsbrud på en anmeldt elektronisk identifikationsordning, jf. eIDAS-forordningens artikel 10, stk. 2
- at analysere overensstemmelsesvurderingsrapporter, jf. eIDAS-forordningens artikel 17, stk. 4, litra b
- at underrette andre tilsynsorganer og offentligheden om brud på sikkerheden eller tab af integritet jf. eIDAS-forordningens artikel 17, stk. 4, litra c
- at aflægge rapport til Kommissionen om sin primære virksomhed jf. eIDAS-forordningens artikel 17, stk. 4, litra d
- at foretage kontrolundersøgelser eller anmode et overensstemmelsesvurderingsorgan om at udføre en overensstemmelsesvurdering af de kvalificerede tillidstjenesteudbydere jf. eIDAS-forordningens artikel 17, stk. 4, litra e
- at samarbejde med databeskyttelsesmyndighederne navnlig ved hurtigst muligt at underrette dem om resultaterne af kontrolundersøgelser af kvalificerede tillidstjenesteudbydere, hvis der er mistanke om overtrædelse af reglerne om beskyttelse af personoplysninger jf, eIDAS-forordningens artikel 17, stk. 4, litra f
- at tildele kvalificerede tillidstjenesteudbydere og de tjenester, de udbyder, status som kvalificeret og at trække denne status tilbage jf. eIDAS-forordningens artikel 17, stk. 4, litra g
- at underrette det organ, der er ansvarligt for den nationale positivliste, om sine afgørelser om tildeling eller tilbagetrækning af status som kvalificeret jf. eIDAS-forordningens artikel 17, stk. 4, litra h
- at kontrollere, at der findes bestemmelser om planer for virksomhedsafbrydelse, og at de anvendes korrekt, i tilfælde hvor den kvalificerede tillidstjenesteudbyder afbryder sin virksomhed, herunder hvordan oplysninger forbliver tilgængelige jf. eIDAS-forordningens artikel 17, stk. 4, litra i
- at pålægge tillidstjenesteudbydere at afhjælpe mangler i opfyldelsen af de krav, der er fastsat i forordningen, jf. eIDAS-forordningens artikel 17, stk. 4, litra j
- at oprette, vedligeholde og ajourføre en tillidsinfrastruktur i overensstemmelse med reglerne i national ret, jf. eIDAS-forordningens artikel 17, stk. 5
- senest den 31. marts hvert år at forelægge Kommissionen en rapport om det foregående kalenderårs primære tilsynsvirksomhed sammen med en sammenfatning af de indberetninger af brud på sikkerheden, som er modtaget fra tillidstjenesteudbydere, jf. eIDAS-forordningens artikel 17, stk. 6
- at udveksle god praksis med andre medlemsstaters tilsynsorganer, jf. eIDAS-forordningens artikel 18
- at samarbejde med andre tilsynsorganer og yde dem bistand i overensstemmelse med eIDAS-forordningens artikel 18
- at tilsynet en gang om året skal forelægge en sammenfattende rapport for ENISA om de indberetninger af brud på sikkerheden eller tab af integritet, som er modtaget fra tillidstjenesteudbyderne, jf. eIDAS-forordningens artikel 19, stk. 3
- at oprette, ajourføre og offentliggøre positivlister, jf. eIDAS-forordningens artikel 22.

4.2 Sanktionering for overtrædelse af eIDAS-forordningen

4.2.1 Gældende ret

Det følger af eIDAS-forordningens artikel 16, at de enkelte medlemsstater skal fastsætte regler om sanktioner for overtrædelser af eIDAS-forordningen. Det er et krav, at sanktionerne er effektive, står i et rimeligt forhold til overtrædelsen og skal have afskrækkende virkning.

Det forhold, at eIDAS-forordningen er ny, bevirker, at der på nuværende tidspunkt ikke eksisterer gældende ret, som dækker sanktionering for overtrædelse af selve eIDAS-forordningen.

I lov om elektroniske signaturer reguleres sanktionering for overtrædelse af denne i § 24.

Lov om elektroniske signaturer § 24, stk. 1, nr. 1, sanktionerer således overtrædelse af offentliggørelse af certifikat uden underskriverens samtykke, opbevaring eller kopiering af de personers signaturgenereringsdata, som nøglecentret gennem udstedelsen af certifikater måtte have fået kendskab til. Derudover sanktioneres overtrædelse af lov om elektroniske signaturer § 12, hvoraf det fremgår at et nøglecenter kun må indsamle personoplysninger i forbindelse med nøglecentervirksomheden direkte fra den registrerede eller med den registreredes udtrykkelige samtykke og kun i det omfang, det er nødvendigt for udstedelsen eller opretholdelsen af et certifikat. Personoplysninger indsamlet i forbindelse med nøglecentrets virksomhed må ikke behandles eller videregives til andet formål uden den registreredes udtrykkelige samtykke hertil.

Markedsføring eller anvendelse af signaturgenereringssystemer, der betegnes som sikre, før de er blevet efterprøvet samt afgivelse af vildledende oplysninger og overtrædelse af påbud er tillige sanktioneret i lov om elektroniske signaturer.

Lov om elektroniske signaturers § 24, stk. 1, nr. 2 og 3 sanktionerer ydermere afgivelse af urigtige oplysninger til Telestyrelsen og overtrædelse af påbud eller afgørelser fra Telestyrelsen. Sanktioneringen omfatter juridiske personer, og der er fastsat en forældelsesfrist på fem år, jf. § 24, stk. 3.

4.2.2 Ministeriets overvejelser og den foreslåede ordning

Bestemmelserne om sanktionering i lov om elektroniske signaturer har ikke været anvendt i praksis, idet der ikke har været afgivet påbud eller gennemført andre sanktioner i medfør af loven. Dette er et resultat af, at der kun i begrænset omfang har eksisteret kvalificerede nøglecentre i Danmark, og der således ikke har været situationer, der har betinget sanktioner. På den baggrund findes ingen praktisk erfaring med anvendelse af sanktioneringsbestemmelser på området.

eIDAS-forordningen og dermed lovforslaget vedrører ikke alene specifikt certifikater, som det er tilfældet med lov om elektroniske signaturer. Forordningen og dermed lovforslaget vedrører derimod tillidstjenesteudbydere og deres virksomhed i bredere forstand. Det vurderes, at såfremt en tillidstjenesteudbyder overtræder de bestemmelser, der er sanktioneret i lov om elektroniske signaturer, § 24, stk. 1, nr. 1 vil dette tillige være i strid med eIDAS-forordningens artikel 19, stk. 1 som påbyder tillidstjenesteudbydere at træffe passende tekniske og organisatoriske foranstaltninger til at styre de sikkerhedsmæssige risici i forbindelse med de tillidstjenester, de udbyder.

For så vidt angår behandling af personoplysninger er dette reguleret i lov nr. 429 af 31/05/2000 om behandling af personoplysninger. I eIDAS-forordningen er der således ikke specifikke bestemmelser om persondata, men en pligt for tilsynet til at samarbejde med databeskyttelsesmyndighederne og rapportere om hændelser relateret til persondata.

Lovforslaget indeholder sanktionering af manglende overholdelse af sikkerhedskrav og underretningspligt for tillidstjenesteudbydere, jf. eIDAS-forordningens artikel 19, stk. 1 og 2. Derudover sanktioneres tillidstjenesteudbydernes afgivelse af urigtige oplysninger til tilsynsorganet.

4.3 Bemyndigelse til fastsættelse af nærmere regler om sikkerhedskrav til tillidstjenesteudbydere

4.3.1 Gældende ret

Sikkerhedskrav til nøglecentre reguleres i lov om elektroniske signaturers kapitel 4 og bekendtgørelse om sikkerhedskrav mv. til nøglecentre. Det foreslås i lovforslaget, at disse ophæves.

Reguleringen af sikkerhedskrav til tillidstjenesteudbydere, herunder nøglecentre, vil fra den 1. juli 2016 være reguleret i eIDAS-forordningens artikel 19.

eIDAS-forordningens artikel 19, stk. 1 fastslår, at kvalificerede og ikke-kvalificerede tillidstjenesteudbydere skal træffe passende tekniske og organisatoriske foranstaltninger til at styre de sikkerhedsmæssige risici i forbindelse med de tillidstjenester, de udbyder. Under hensyn til den seneste teknologiske udvikling skal disse foranstaltninger garantere et sikkerhedsniveau, der svarer til risikoens omfang. Tillidstjenesteudbyderne bør navnlig tage skridt til at forhindre og minimere virkningen af sikkerhedsrelaterede hændelser og underrette de berørte parter om de negative virkninger af sådanne hændelser. Tillidstjenesteudbyderne skal behandle personoplysninger i overensstemmelse med direktiv 95/46/EF, som omhandler beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger. Direktiv 95/46/EF vedrører således ikke oplysninger om tillidstjenesteudbydernes systemers tekniske- og sikkerhedsmæssige indretning samt processer for opretholdelse, vedligeholdelse og drift af sikkerheden omkring systemerne. Direktivet er i dansk ret implementeret ved lov nr. 429 af 31. maj 2000 om behandling af personoplysninger.

Kommissionen gives i eIDAS-forordningens artikel 19, stk. 4, mulighed for at specificere de i stk. 1 omhandlede foranstaltninger yderligere.

Kommissionen har ved lovforslagets fremsættelse ikke benyttet sig af muligheden for at specificere yderligere via gennemførelsesretsakter, hvad der menes med passende tek-

niske og organisatoriske foranstaltninger i eIDAS-forordningen.

I lov om elektroniske signaturer, bekendtgørelse nr. 923 af 5. oktober 2000 om sikkerhedskrav mv. til nøglecentre, bekendtgørelse nr. 922 af 5. oktober 2000 om nøglecentres og systemrevisionens indberetning af oplysninger til Telestyrelsen findes ikke krav til, at tillidstjenesteudbydere skal underrette tilsynsorganet om konstaterede brud på sikkerheden.

Et sådant krav følger imidlertid af eIDAS-forordningens artikel 19, stk. 2, 1. afsnit og indebærer, at de kvalificerede og ikke-kvalificerede tillidstjenesteudbydere, der konstaterer et brud på sikkerheden eller tab af integritet, som har en væsentlig indvirkning på den udbudte tillidstjeneste eller de berørte personoplysninger, hurtigst muligt og under alle omstændigheder inden for 24 timer efter at være blevet opmærksomme på forholdet skal underrette tilsynsorganet, og eventuelt andre relevante organer som f.eks. det kompetente nationale organ for informationssikkerhed eller databeskyttelsesmyndigheden.

Kommissionen har ved lovforslagets fremsættelse ikke benyttet sig af muligheden for ved gennemførelsesretsakter at vedtage formater og procedurer, herunder tidsfrister, for tillidstjenesteudbyderes rapporteringen i forbindelse med konstaterede brud på sikkerheden.

4.3.2 Ministeriets overvejelser og den foreslåede ordning

Finansministeren gives med lovforslaget bemyndigelse til at udstede en bekendtgørelse i lighed med tidligere bekendtgørelse udstedt i medfør af lov om elektroniske signaturer i det tilfælde, at Kommissionen ikke udarbejder gennemførelsesretsakt vedrørende tillidstjenesteudbydernes sikkerhedsforanstaltninger.

Det foreslås også i lovforslaget, at finansministeren gives bemyndigelse til at fastsætte nærmere regler om sikkerhedskrav til tillidstjenesteudbydere. Da det vurderes, at der er mulighed for i højere grad at gøre reguleringen af underretningen af konstaterede sikkerhedsbrud anvendelig. Bestemmelsen skal sikre, at der er mulighed for at præcisere indholdet af sikkerhedskravene, herunder kravene til rapportering af hændelser for at sikre et tilstrækkeligt sikkerhedsniveau. De sikkerhedskrav, der forventes at blive indeholdt i bemyndigelsen, er endnu ikke endeligt fastlagt. Det forventes dog, at der vil blive taget udgangspunkt i de sikkerhedskrav, der fremgår af lov om elektroniske signaturer, bekendtgørelse om sikkerhedskrav mv. til nøglecentre og relevante sikkerhedsstandarder på området, samt materiale udarbejdet af ENISA (European Union Agency for Network and Information Security). Det kan oplyses, at ENISA pt. arbejder på en fælleseuropæisk skabelon for indberetning af sikkerhedshændelser i medfør af eIDAS-forordningens artikel 19. Såfremt Kommissionen ikke udarbejder en gennemførselsretsakt i medfør af eIDAs-forordningens artikel 19, stk. 4, kan finansministeren bl.a. udnytte bemyndigelsen til at fastsætte regler om, at denne skabelon skal anvendes.

Det bemærkes, at såfremt Kommissionen vælger at udnytte bemyndigelsen til at regulere dette nærmere via en gennemførelsesretsakt, vil en sådan have forrang for eventuelle bekendtgørelser udstedt i medfør af denne lov. Er der allerede udstedt bekendtgørelser, der strider mod gennemførelsesretsakter, vil disse blive ophævet.

4.4 Bemyndigelse til fastsættelse af yderligere bestemmelser om tilsyn

4.4.1 Gældende ret

Tilsyn med nøglecentre reguleres i lov om elektroniske signaturer kapitel 9 og indholdet af nøglecentres rapportering til Telestyrelsen reguleres i bekendtgørelse nr. 922 af 5. oktober 2000 om nøglecentres og systemrevisionens indberetning af oplysninger til Telestyrelsen. Denne regulering ophæves i medfør af lovforslaget.

Reguleringen af tilsyn, herunder nøglecentres rapportering til tilsynsorganet, vil fra den 1. juli 2016 være reguleret i eIDAS-forordningens artikler 17 og 21.

Det følger af eIDAS-forordningens artikel 17, stk. 3, at tilsynsorganet skal føre tilsyn. Selve tilsynsbegrebet er dog ikke nærmere defineret i eIDAS-forordningen.

Det følger af eIDAS-forordningens artikel 21, stk. 1 og 17, stk. 4, b at tilsynsorganet henholdsvis skal modtage og analysere overensstemmelsesvurderingsrapporter fra tillidstjenesteudbyderne.

Begrebet overensstemmelsesvurderingsrapport er ikke nærmere defineret. Det følger dog af eIDAS-forordningens artikel 21, stk. 4, 1. pkt., at Kommissionen ved hjælp af gennemførelsesretsakter kan fastlægge formater og procedurer for tillidstjenesteudbydernes indsendelse og tilsynets kontrol af indsendte overensstemmelsesvurderingsrapporter.

Kommissionen har ved lovforslagets fremsættelse ikke benyttet sig af muligheden for ved hjælp af gennemførelsesretsakter at vedtage sådanne formater og procedurer.

4.4.2. Ministeriets vurdering og den foreslåede ordning

Det vurderes at være mest hensigtsmæssigt i forhold til den konkrete udførelse af tilsynet og analyse samt vurdering af overensstemmelsesvurderingsrapporter, at der fastsættes yderligere bestemmelser om tilsynsorganets tilsyn med tillidstjenesteudbydere, herunder indholdet af overensstemmelsesvurderingsrapporterne.

Det foreslås i lovforslaget, at finansministeren gives bemyndigelse til at fastsætte yderligere bestemmelser om tilsynsorganets tilsyn med tillidstjenesteudbydere, herunder indholdet af overensstemmelsesvurderingsrapporter.

De tilsynsbestemmelser, der forventes at blive indeholdt i bemyndigelsen, er endnu ikke endeligt fastlagt. Det forventes dog, at der vil blive taget udgangspunkt i de tilsynsbestemmelser, der fremgår af lov om elektroniske signaturer og bekendtgørelse nr. 922 af 5. oktober 2000 om nøglecentres og systemrevisionens indberetning af oplysninger til Telestyrelsen og endelig relevante sikkerhedsstandarder på

området, samt materiale udarbejdet af ENISA (European Union Agency for Network and Information Security).

Det bemærkes, at såfremt Kommissionen vælger at regulere dette nærmere via en gennemførelsesretsakt, vil en sådan have forrang for eventuelle bekendtgørelser udstedt i medfør af denne lov. Er der allerede udstedt bekendtgørelser, der strider mod gennemførelsesretsakter, vil disse blive ophævet.

4.5 Tavshedspligt for tilsynsførende

4.5.1 Gældende ret

Der er ingen bestemmelser om tavshedspligt for tilsynsførende i lov om elektroniske signaturer, bekendtgørelse nr. 922 af 5. oktober 2000 om nøglecentres og systemrevisionens indberetning af oplysninger til Telestyrelsen eller bekendtgørelse nr. 923 af 5. oktober 2000 om sikkerhedskrav m.v. til nøglecentre.

Det fremgår af betragtning 11 til eIDAS-forordningen, at tillidstjenesteudbydere og tilsynsorganer bør opfylde kravene i direktiv 95/46/EF om fortrolighed og behandlingssikkerhed.

Direktiv 95/46/EF omhandler beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger. Direktiv 95/46/EF vedrører således ikke oplysninger om tillidstjenesteudbydernes systemers tekniske- og sikkerhedsmæssige indretning samt processer for opretholdelse, vedligeholdelse og drift af sikkerheden omkring systemerne.

4.5.2 Ministeriets vurdering og den foreslåede ordning

Tilsynet baserer sig på indberetninger fra tillidstjenesteudbyderne, herunder oplysninger fra overensstemmelsesvurderingsorganet indeholdt i de såkaldte overensstemmelsesvurderingsrapporter. Det er afgørende, at tilsynet får indsigt i alle oplysninger, der fremkommer i forbindelse med tilsynet om f.eks. risiko- og sikkerhedsvurderinger, herunder eventuelle sårbarheder. Disse oplysninger kan indikere svagheder i både systemer, systeminstallationer samt de sikkerhedsmæssige processer, som kan betyde, at tilsynet vil kræve forbedring af systemer, ændrede sikkerhedsmæssige processer eller lignende. Det er derfor afgørende, at disse oplysninger kan indberettes i fortrolighed, da kendskab til og indsigt i systemers og processers eventuelle svagheder vil øge risikoen for angreb på og kompromittering af sikkerheden. Det offentlige har inden for de seneste år været genstand for et stigende antal sikkerhedsmæssige hændelser, og det vurderes, at denne tendens vil fortsætte. Angreb på systemer af så central karakter som fx NemID kan have vidtrækkende konsekvenser for borgere og erhvervsdrivende samt hele den offentlige sektor. Denne type angreb vil ligeledes mindske tilliden til digitale tjenester og kan dermed hindre digitalisering og begrænse mulige gevinster.

Det er således en forudsætning for, at tilsynsorganet kan føre det nødvendige tilsyn med tillidstjenesteudbydere, at alle oplysninger og sikkerhedsmæssige procedurer om systemer, sårbarheder m.v. indgår i den rapportering, der indgives til tilsynsorganet. Der vurderes samtidig ikke at være hensyn, der tilsiger, at borgere skal være bekendt med de mere specifikke tekniske indretninger og sikkerhedsmæssige procedurer, som er med til at skabe sikkerheden i systemerne, og som derfor indgår i tilsynsarbejdet.

Lovforslaget indfører derfor en særlig tavshedspligt, der medfører, at myndigheder og personer, der udøver tilsyn med tillidstjenesteudbydere, samt enhver, der i øvrigt yder bistand til tilsynet, iagttager ubetinget tavshed over for uvedkommende med hensyn til oplysninger om tillidstjenesteudbydernes systemers tekniske- og sikkerhedsmæssige indretning samt processer for opretholdelse, vedligeholdelse og drift af sikkerheden omkring systemerne.

5. Økonomiske og administrative konsekvenser for det offentlige

Lovforslaget forventes ikke at have økonomiske konsekvenser for det offentlige, ud over hvad der allerede er angivet i forbindelse med vedtagelsen af eIDAS-forordningen.

Det forventes, at de ekstra opgaver, der følger med det udvidede tilsyn, som følger af eIDAS-forordningen, vil svare til et årsværk. Opgaven håndteres inden for eksisterende økonomiske rammer.

Lovforslaget skønnes at få administrative konsekvenser for staten.

I medfør af eIDAS-forordningen skal medlemsstaterne udpege et tilsynsorgan. Med lovforslaget foreslås det, at Digitaliseringsstyrelsen udpeges som tilsynsførende myndighed. Tilsynsopgaven vurderes at have et omfang svarende til et årsværk, hvilket er oplyst i forbindelse med vedtagelse af eIDAS-forordningen. Behovet for ekstra ressourcer bunder navnlig i udvidelse af tilsynsopgaven med tilsyn med flere typer af tillidstjenester og i forhold til krav om samarbejde mellem tilsyn på tværs af grænser og i nye rapporteringsopgaver overfor henholdsvis medlemsstaternes tilsyn, Kommissionen og ENISA om fx brud på sikkerheden eller tab af integritet, som det har modtaget fra tillidstjenesteudbyderne.

Lovforslaget har ikke administrative konsekvenser for regioner og kommuner.

Lovforslaget medfører ikke, at der oprettes nye administrative myndigheder eller væsentlige udvidelser af allerede eksisterende myndigheder.

6. Økonomiske og administrative konsekvenser for erhvervslivet m.v.

Lovforslaget har ikke væsentlige erhvervsøkonomiske konsekvenser. Dette skyldes, at lovforslagets bemyndigelser sigter mod at muliggøre opretholdelse af den nuværende retstilstand i det omfang, det er muligt.

7. Administrative konsekvenser for borgerne

Lovforslaget har ikke administrative konsekvenser for borgerne.

8. Miljømæssige konsekvenser

Lovforslaget har ikke miljømæssige konsekvenser.

9. Forholdet til EU-retten

Lovforslaget indeholder forslag til bestemmelser, der opfylder og supplerer krav fastsat i eIDAS-forordningen og bemyndigelser til at regulere sikkerhedskrav til tillidstjenesteudbydere og det nærmere indhold af tilsyn med tillidstjenesteudbydere, herunder indholdet af overensstemmelsesvurderingsrapporter.

eIDAS-forordningens fulde titel er Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF som blev trykt i Den Europæiske Unions Tidende L 257, 57. årgang, 28. august 2014.

Hovedparten af eIDAS-forordningen træder i kraft den 1. juli 2016.

eIDAS-forordningen skal erstatte det eksisterende direktiv om elektroniske signaturer, 1999/93/EF, men har et bredere anvendelsesområde, idet forordningen i tillæg til regulering af elektroniske signaturer også regulerer en bredere gruppe af elektroniske tillidstjenester samt elektroniske identiteter og dokumenter. Med lovforslaget ophæves lov om elektroniske signaturer, som implementerede direktiv 1999/93/EF.

10. Hørte myndigheder og organisationer m.v.

Udkast til lovforslaget har i perioden fra den 22. oktober 2015 til den 18. november 2015 været sendt i høring hos følgende myndigheder og organisationer m.v.:

ATP, Danmarks Nationalbank, Dansk Aktionærforening, Danske Revisorer, Danske Regioner, Finansrådet, IT-Branchen, KL, Lønmodtagernes Dyrtidsfond, National Sundheds-it, Nets DanID, Signaturgruppen, Dansk Erhverv, IBM, Danske revisorer, KMD, Finansrådet, CSC, BEC – Bankernes EDB-central, DI Digital, DANSK IT.

11. Sammenfattende skema

Samlet vurdering af lovforslagets konsekvenser

	Positive konsekvenser/mindreudgifter	Negative konsekvenser/merudgifter
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Administrative konsekvenser for stat, kommuner og regioner	Ingen	Tilsyns- og rapporteringsopgaver forventes at medføre udgifter for staten svarende til et årsværk.
Økonomiske konsekvenser for erhvervslivet	Ingen	Ingen
Administrative konsekvenser for erhvervslivet	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Administrative konsekvenser for borgerne	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget indeholder bestemmelser, der opfylder og supplerer krav fastsat i eIDAS-forordningen og bemyndigelser til at regulere sikkerhedskrav til tillidstjenesteudbydere og det nærmere indhold af tilsyn med tillidstjenesteudbydere.	

Bemærkninger til lovforslagets enkelte bestemmelser

Anvendelsesområde

Til § 1

Den foreslåede bestemmelse fastlægger forslagets anvendelsesområde.

Lov om elektroniske signaturer fandt alene anvendelse på nøglecentre etableret i Danmark.

eIDAS-forordningen finder anvendelse på alle tillidstjenesteudbydere, der er hjemmehørende i Unionen. Begrebet tillidstjenesteudbyder er defineret i eIDAS-forordningens artikel 3, nr. 19, og skal forstås som det er defineret i eIDAS-forordningen. Et eksempel på en tillidstjenesteudbyder i dansk kontekst er Nets DanID A/S.

Med bestemmelsen foreslås det, at lovforslaget finder anvendelse på tillidstjenesteudbydere, som udbyder tillidstjenester, som er etableret i Danmark, og som er omfattet af eIDAS-forordningen.

Kontrol og straf m.v.

Til § 2

Udpegning af tilsynsorganet i medfør af lov om elektroniske signaturer fremgår af § 18, stk. 1. Det foreslås, at lov om elektroniske signaturer ophæves pr. 1. juli 2016. Det fremgår af eIDAS-forordningens artikel 17, stk. 1, at medlems-

staterne skal udpege et tilsynsorgan i forhold til overholdelse af eIDAS-forordningen.

I stk. 1 foreslås det, at Digitaliseringsstyrelsen udpeges til at påse overholdelsen af eIDAS-forordningen og loven.

Det foreslås, at Digitaliseringsstyrelsen fører kontrol med, at kravene i eIDAS-forordningen og lovforslaget overholdes.

Digitaliseringsstyrelsen foreslås som tilsynsorgan efter eIDAS-forordningen, fordi Digitaliseringsstyrelsen i dag fører tilsyn med nøglecentre i henhold til lov om elektroniske signaturer. Digitaliseringsstyrelsen vurderes derfor at ligge inde med de fornødne kompetencer og den nødvendige erfaring til at varetage opgaven.

Til § 3

Sikkerhedskrav til nøglecentre reguleres i lov om elektroniske signaturer kapitel 4 og bekendtgørelse nr. 223 af 5. oktober 2000 om sikkerhedskrav m.v. til nøglecentre. Disse ophæves i medfør af lovforslaget.

Det følger af eIDAS-forordningens artikel 19, stk. 2, at tillidstjenesteudbydere skal underrette tilsynsorganet om konstaterede brud på sikkerheden. Et sådant krav findes ikke i lov om elektroniske signaturer, bekendtgørelse nr. 923 af 5. oktober 2000 om sikkerhedskrav m.v. til nøglecentre eller bekendtgørelse nr. 922 af 5. oktober 2000 om nøglecentres og systemrevisionens indberetning af oplysninger til Telestyrelsen.

Reguleringen af sikkerhedskrav til tillidstjenesteudbydere, herunder nøglecentre, vil fra den 1. juli 2016 være reguleret i eIDAS-forordningens artikel 19.

Det følger af eIDAS-forordningens artikel 19, stk. 1, at kvalificerede og ikke-kvalificerede tillidstjenesteudbydere skal træffe passende tekniske og organisatoriske foranstaltninger til at styre de sikkerhedsmæssige risici i forbindelse med de tillidstjenester, de udbyder. Under hensyn til den seneste teknologiske udvikling skal disse foranstaltninger garantere et sikkerhedsniveau, der svarer til risikoens omfang.

Kommissionen gives i eIDAS-forordningens artikel 19, stk. 4, mulighed for at specificere de i eIDAS-forordningens artikel 19, stk. 1 omhandlede foranstaltninger yderligere.

Kommissionen har ved lovforslagets fremsættelse ikke benyttet sig af muligheden for at specificere yderligere via gennemførelsesretsakter, hvad der i eIDAS-forordningen menes med, at tillidstjenesteudbydere skal træffe passende tekniske og organisatoriske foranstaltninger.

Kommissionen har ved lovforslagets fremsættelse ej heller benyttet sig af muligheden for ved gennemførelsesretsakter at vedtage formater og procedurer, herunder tidsfrister, for tillidstjenesteudbydernes rapporteringer i tilfælde af konstaterede sikkerhedsbrud.

Reguleringen af passende tekniske og organisatoriske sikkerhedsforanstaltninger i eIDAS-forordningen giver plads til fortolkning, og finansministeren gives derfor i bestemmelsens stk. 1 bemyndigelse til at udstede en bekendtgørelse i lighed med tidligere bekendtgørelse udstedt i medfør af lov om elektroniske signaturer i det tilfælde, at Kommissionen ikke udarbejder gennemførelsesretsakt på dette område.

Det vurderes, at der er mulighed for i højere grad at gøre reguleringen af underretningen af konstaterede sikkerhedsbrud praktisk anvendelig.

Denne vurdering finder støtte i det forhold, at Kommissionen i eIDAS-forordningens artikel 19, stk. 4 gives mulighed for ved gennemførelsesretsakter at vedtage formater og procedurer, herunder tidsfrister.

Det foreslås derfor i lovforslagets stk. 1, at finansministeren gives bemyndigelse til at fastsætte nærmere regler om sikkerhedskrav til tillidstjenesteudbydere. Bestemmelsen skal sikre, at der er mulighed for at præcisere indholdet af sikkerhedskravene, herunder kravene til rapportering af hændelser for at sikre et tilstrækkeligt sikkerhedsniveau. De sikkerhedskrav, der forventes at blive indeholdt i bemyndigelsen, er endnu ikke endeligt fastlagt. Det forventes dog, at der vil blive taget udgangspunkt i de sikkerhedskrav, der fremgår af lov om elektroniske signaturer, bekendtgørelse nr. 923 af 5. oktober 2000 om sikkerhedskrav m.v. til nøglecentre og relevante sikkerhedsstandarder på området, samt materiale udarbejdet af ENISA (European Union Agency for Network and Information Security). Det kan oplyses, at ENISA pt. arbejder på en fælleseuropæisk skabelon for indberetning af sikkerhedshændelser i medfør af eIDAS-forordningens artikel 19. Såfremt Kommissionen ikke udarbejder gennemførselsretsakt i medfør af eIDAS-forordningens artikel 19, stk. 4, kan finansministeren bl.a. benytte bemyndigelsen til at pege på denne skabelon i forbindelse med rapportering af sikkerhedshændelser.

Til § 4

Tilsyn med nøglecentre reguleres i lov om elektroniske signaturers kapitel 9 og indholdet af nøglecentres rapportering til Telestyrelsen reguleres i bekendtgørelse nr. 922 af 5.oktober 2000 om nøglecentres og systemrevisionens indberetning af oplysninger til Telestyrelsen. Disse ophæves i medfør af lovforslaget.

Reguleringen af tilsyn, herunder nøglecentres rapportering til tilsynsorganet, vil fra den 1. juli 2016 være reguleret i eIDAS-forordningens artikel 17 og 21.

Det følger af eIDAS-forordningens artikel 17, stk. 3, at tilsynsorganet skal føre tilsyn. Selve begrebet tilsyn er dog ikke nærmere defineret i eIDAS-forordningen.

Det følger af eIDAS-forordningens artikel 21, stk. 1 og 17, stk. 4, b, at tilsynsorganet henholdsvis skal modtage og analysere overensstemmelsesvurderingsrapporter fra tillidstjenesteudbyderne.

Begrebet overensstemmelsesvurderingsrapport er ikke nærmere defineret. Det følger dog af eIDAS-forordningens artikel 21, stk. 4, 1. pkt., at Kommissionen ved hjælp af gennemførelsesretsakter kan fastlægge formater og procedurer for tillidstjenesternes indsendelse og kontrol af overensstemmelsesvurderingsrapporter.

Kommissionen har ved lovforslagets fremsættelse ikke benyttet sig af muligheden for ved hjælp af gennemførelsesretsakter at vedtage sådanne formater og procedurer.

Den foreslåede bestemmelses *stk. 1* henviser til de tilsynsopgaver, som Digitaliseringsstyrelsen foreslås at blive ansvarlig for. Disse opgaver består i:

- at analysere overensstemmelsesvurderingsrapporter, jf. eIDAS-forordningens artikel 17, stk. 4, litra b
- at underrette andre tilsynsorganer og offentligheden om brud på sikkerheden eller tab af integritet jf. eIDAS-forordningens artikel 17, stk. 4, litra c
- at aflægge rapport til Kommissionen om sin primære virksomhed jf. eIDAS-forordningens artikel 17, stk. 4, litra d
- at foretage kontrolundersøgelser eller anmode et overensstemmelsesvurderingsorgan om at udføre en overensstemmelsesvurdering af de kvalificerede tillidstjenesteudbydere jf. eIDAS-forordningens artikel 17, stk. 4, litra e
- at samarbejde med databeskyttelsesmyndighederne navnlig ved hurtigst muligt at underrette dem om resultaterne af kontrolundersøgelser af kvalificerede tillidstjenesteudbydere, hvis der er mistanke om overtrædelse af reglerne om beskyttelse af personoplysninger jf. eIDAS-forordningens artikel 17, stk. 4, litra f
- at tildele kvalificerede tillidstjenesteudbydere og de tjenester, de udbyder, status som kvalificeret og at trække denne status tilbage jf. eIDAS-forordningens artikel 17, stk. 4, litra g
- at underrette det organ, der er ansvarligt for den nationale positivliste, om sine afgørelser om tildeling eller tilbagetrækning af status som kvalificeret jf. eIDAS-forordningens artikel 17, stk. 4, litra h
- at kontrollere, at der findes bestemmelser om planer for virksomhedsafbrydelse, og at de anvendes korrekt, i tilfælde hvor den kvalificerede tillidstjenesteudbyder afbryder sin virksomhed, herunder hvordan oplysninger forbliver tilgængelige jf. eIDAS-forordningens artikel 17, stk. 4, litra i
- at pålægge tillidstjenesteudbydere at afhjælpe mangler i opfyldelsen af de krav, der er fastsat i forordningen, jf. eIDAS-forordningens artikel 17, stk. 4, litra j
- at oprette, vedligeholde og ajourføre en tillidsinfrastruktur i overensstemmelse med reglerne i national ret, jf. eIDAS-forordningens artikel 17, stk. 5
- senest den 31. marts hvert år at forelægge Kommissionen en rapport om det foregående kalenderårs primære tilsynsvirksomhed sammen med en sammenfatning af de indberetninger af brud på sikkerheden, som er modtaget fra tillidstjenesteudbydere, jf. artikel 17, stk. 6.

I s*tk. 2.* foreslås det, at finansministeren bemyndiges til at fastsætte yderligere bestemmelser om Digitaliseringsstyrelsens tilsyn med tillidstjenesteudbydere, herunder bestemmelser om indholdet af overensstemmelsesvurderingsrapporter i henhold til eIDAS-forordningens artikel 21, stk. 1.

Den foreslåede bestemmelse er indsat, fordi der ikke er fastsat nogen endelig frist for Kommissionens eventuelle yderligere regulering af tilsynet med tillidstjenesteudbyderne og overensstemmelsesvurderingsrapporten. Bestemmelsen giver således mulighed for at indføre bestemmelser til regulering af områder, der i dag er mere detaljeret reguleret i lov om elektroniske signaturer og bekendtgørelserne dertil. Det begrundes i det forhold, at lov om elektroniske signaturer og bekendtgørelserne ophæves, hvilket vil medføre at området vil henstå utilstrækkeligt reguleret.

De tilsynsbestemmelser, der forventes at blive indeholdt i bemyndigelsen, er endnu ikke endeligt fastlagt. Det forventes dog, at der vil blive taget udgangspunkt i de tilsynsbestemmelser, der fremgår af lov om elektroniske signaturer og i bekendtgørelse nr. 922 af 5. oktober 2000 om nøglecentres og systemrevisionens indberetning af oplysninger til Telestyrelsen og relevante sikkerhedsstandarder på området, samt materiale udarbejdet af ENISA (European Union Agency for Network and Information Security).

Til § 5

Der er ingen bestemmelser om tavshedspligt for tilsynsførende i lov om elektroniske signaturer, bekendtgørelse nr. 922 af 5. oktober 2000 om nøglecentres og systemrevisionens indberetning af oplysninger til Telestyrelsen eller bekendtgørelse nr. 923 af 5. oktober 2000 om sikkerhedskrav m.v. til nøglecentre.

Det fremgår af betragtning 11 til eIDAS-forordningen, at tillidstjenesteudbydere og tilsynsorganer bør opfylde kravene i direktiv 95/46/EF om fortrolighed og behandlingssikkerhed.

Direktiv 95/46/EF omhandler beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger. Direktiv 95/46/EF vedrører således ikke oplysninger om tillidstjenesteudbydernes systemers tekniske- og sikkerhedsmæssige indretning samt processer for opretholdelse, vedligeholdelse og drift af sikkerheden omkring systemerne.

Bestemmelsen regulerer tavshedspligten for personer, der udøver tilsyn med tillidstjenesteudbyderne.

Tilsynet baserer sig på indberetninger fra tillidstjenesteudbyderne, herunder oplysninger fra overensstemmelsesvurderingsorganet indeholdt i de såkaldte overensstemmelsesvurderingsrapporter. Begrebet overensstemmelsesvurderingsorgan er defineret i eIDAS-forordningen, artikel 3, nr. 18 og skal forstås som defineret i eIDAS-forordningen. Det er afgørende, at tilsynet får indsigt i alle oplysninger, der fremkommer i forbindelse med tilsynet om f.eks. risiko- og sikkerhedsvurderinger, herunder eventuelle sårbarheder. Disse oplysninger kan indikere svagheder i både systemer, systeminstallationer samt de sikkerhedsmæssige processer, som kan betyde, at tilsynet vil kræve forbedring af systemer, ændrede sikkerhedsmæssige processer eller lignende. Det er derfor afgørende, at disse oplysninger kan indberettes i fortrolighed, da kendskab til og indsigt i systemers og processers eventuelle svagheder vil øge risikoen for angreb på og kompromittering af sikkerheden. Det offentlige har inden for de seneste år været genstand for et stigende antal sikker-

hedsmæssige hændelser, og det vurderes, at denne tendens vil fortsætte. Angreb på systemer af så central karakter som fx NemID, kan have vidtrækkende konsekvenser for borgere og erhvervsdrivende samt hele den offentlige sektor. Denne type angreb vil ligeledes mindske tilliden til digitale tjenester og kan dermed hindre digitalisering og begrænse mulige gevinster.

Det er således en forudsætning for, at tilsynsorganet kan føre det nødvendige tilsyn med tillidstjenesteudbydere, at alle oplysninger og sikkerhedsmæssige procedurer om systemer, sårbarheder m.v. indgår i den rapportering, der indgives til tilsynsorganet. Der vurderes samtidig ikke at være hensyn, der tilsiger, at borgere skal være bekendt med de mere specifikke tekniske indretninger og sikkerhedsmæssige procedurer, som er med til at skabe sikkerheden i systemerne, og som derfor indgår i tilsynsarbejdet.

Lovforslaget indfører derfor en særlig tavshedspligt, der medfører, at myndigheder og personer, der udøver tilsyn med tillidstjenesteudbydere, samt enhver, der i øvrigt yder bistand til tilsynet, iagttager ubetinget tavshed over for uvedkommende med hensyn til oplysninger om tillidstjenesteudbydernes systemers tekniske- og sikkerhedsmæssige indretning samt processer for opretholdelse, vedligeholdelse og drift af sikkerheden omkring systemerne.

Til § 6

Sanktionering af nøglecentre findes i lov om elektroniske signaturer, kapitel 11, § 24. Det foreslås i lovforslaget, at lov om elektroniske signaturer ophæves.

Bestemmelserne om sanktionering i lov om elektroniske signaturer har ikke været bragt i praktisk anvendelse, idet der ikke har været afgivet påbud eller gennemført andre sanktioner i medfør af loven. Dette er et resultat af, at der kun i begrænset omfang har eksisteret kvalificerede nøglecentre i Danmark, og der således ikke har været situationer, der har betinget sanktioner. På den baggrund findes der ingen praktisk erfaring med anvendelse af sanktioneringsbestemmelser på området.

eIDAS-forordningen og dermed lovforslaget vedrører ikke alene specifikt certifikater, som det er tilfældet med lov om elektroniske signaturer. Forordningen og dermed lovforslaget vedrører derimod tillidstjenesteudbydere og deres virksomhed i bredere forstand. Det vurderes, at såfremt en tillidstjenesteudbyder overtræder de bestemmelser, der er sanktioneret i lov om elektroniske signaturer, § 24, stk. 1, nr. 1 vil dette tillige være i strid med eIDAS-forordningens artikel 19, stk. 1 som påbyder tillidstjenesteudbydere at træffe passende tekniske og organisatoriske foranstaltninger til at styre de sikkerhedsmæssige risici i forbindelse med de tillidstjenester, de udbyder.

For så vidt angår behandling af personoplysninger er dette reguleret i lov nr. 429 af 31/05/2000 om behandling af personoplysninger. I eIDAS-forordningen er der således ikke specifikke bestemmelser om persondata, men der er en pligt for tilsynet til at samarbejde med databeskyttelsesmyndighederne og rapportere om hændelser relateret til persondata.

Lovforslaget indeholder sanktionering af manglende overholdelse af sikkerhedskrav og underretningspligt for tillidstjenesteudbydere, jf. eIDAS-forordningens artikel 19, stk. 1 og 2. Derudover sanktioneres tillidstjenesteudbydernes afgivelse af urigtige oplysninger til tilsynsorganet. eIDAS-forordningens artikel 19, stk. 1 pålægger tillidstjenesteudbydere at træffe passende tekniske og organisatoriske foranstaltninger til at styre de sikkerhedsmæssige risici i forbindelse med de tillidstjenester, de udbyder. Under hensyn til den seneste teknologiske udvikling skal disse foranstaltninger garantere et sikkerhedsniveau, der svarer til risikoens omfang. Tillidstjenesteudbyderne bør navnlig tage skridt til at forhindre og minimere virkningen af sikkerhedsrelaterede hændelser og underrette de berørte parter om de negative virkninger af sådanne hændelser. Efter eIDAS-forordningens artikel 19, stk. 2 skal tillidstjenesteudbydere, der konstaterer et brud på sikkerheden eller tab af integritet, som har en væsentlig indvirkning på den udbudte tillidstjeneste eller de berørte personoplysninger, hurtigst muligt og under alle omstændigheder inden for 24 timer efter at være blevet opmærksomme på forholdet underrette tilsynsorganet, og eventuelt andre relevante organer som f.eks. det kompetente nationale organ for informationssikkerhed eller databeskyttelsesmyndigheden.

Når det er sandsynligt, at et brud på sikkerheden eller tab af integritet vil krænke den fysiske eller juridiske person, som har modtaget tillidstjenesten, skal tillidstjenesteudbyderen også hurtigst muligt underrette den fysiske eller juridiske person om bruddet på sikkerheden eller tab af integritet.

Det følger af eIDAS-forordningens artikel 16, at medlemsstaterne skal fastsætte regler om sanktioner for overtrædelse af eIDAS-forordningen. Sanktionerne skal være effektive samt stå i rimeligt forhold til overtrædelsen og have en afskrækkende virkning.

Det vurderes, at den foreslåede bestemmelse indfrier dette ved at sanktionere for overtrædelse af eIDAS-forordningens bestemmelser om sikkerhedskrav, underretningspligt for tillidstjenesteudbydere og afgivelse af urigtige oplysninger.

Ændringer i anden lovgivning

Til § 7

Lovforslaget foreslås at træde i kraft den 1. juli 2016, samtidig med eIDAS-forordningens ikrafttræden.

I medfør af *stk. 2* foreslås det, at lov om elektroniske signaturer ophæves. Som konsekvens heraf vil de bekendtgørelser, der er udstedt i medfør af lov om elektroniske signaturer, bortfalde.

Til § 8

Lovforslaget indeholder i § 8 en ændring af lov om fragtaftaler ved international vejtransport (CMR-loven), jf. lovbekendtgørelse nr. 1122 af 18. september 2015. Efter CMR-lovens § 6, stk. 5, skal digitale signaturer, som anvendes i forbindelse med elektroniske fragtbreve, være baseret på den gældende OCES-standard eller opfylde kravene i lov

om elektroniske signaturer, der foreslås ophævet med dette lovforslag.

Den foreslåede ændring indebærer, at digitale signaturer på elektroniske fragtbreve fra den 1. juli 2016 skal være baseret på den gældende OCES-standard eller opfylde kravene i eIDAS-forordningen.

Til § 9

Det foreslås i *stk. 1*, at loven træder i kraft den 1. juli 2016.

I *stk. 2* foreslås det, at lov nr. 417 af 31. maj 2000 om elektroniske signaturer ophæves samtidig med lovens i ikrafttræden.