DIGITALISERINGSSTYRELSEN

Notat

1. oktober 2015
CSS /Daniel Hartfield-Traun
Sagsnr.: 2015 - 2035

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 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, herefter benævnt eIDAS-forordningen.

Definitioner

§ 2. De anvendte begreber og udtryk har samme betydning som i eIDAS-forordningen, herunder

1) »tillidstjeneste«: en elektronisk tjeneste, der normalt udføres mod betaling, og som består af:

   a) generering, kontrol og validering af elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler, elektroniske registrerede leveringstjenester og certifikater relateret til disse tjenester, eller

   b) generering, kontrol og validering af certifikater for webstedsautentifikation, eller

   c) bevaring af elektroniske signaturer, segl eller certifikater relateret til disse tjenester

2) »overensstemmelsesvurderingsorgan«: et organ som defineret i artikel 2, nr. 13), i forordning (EF) nr. 765/2008, der er akkrediteret i overensstemmelse med nævnte forordning med kompetence til at udføre overensstemmelsesvurderinger af en kvalificeret tillidstjenesteudbyder og de kvalificerede tillidstjenester, den udbyder

3) »tillidstjenesteudbyder«: en fysisk eller juridisk person, der udbyder en eller flere tillidstjenester, som enten en kvalificeret eller ikkekvalificeret tillidstjenesteudbyder.

Generelle bestemmelser

§ 3. Digitaliseringsstyrelsen påser overholdelse af eIDAS-forordningen og regler fastsat i medfør af eIDAS-forordningen samt denne lov og regler fastsat i medfør af loven.

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

Stk. 2. Gennemførelsesretsakter udstedt med hjemmel i artikel 19, stk.1 og 2, 24, stk. 5 samt 30, stk. 2, 2. afsnit, i eIDAS-forordningen går forud for bestemmelserne i stk. 1.

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

Stk. 2. Finansministeren kan fastsætte yderligere bestemmelser om Digitaliseringsstyrelsens tilsyn med tillidstjenesteudbydere i medfør af artikel 17, herunder bestemmelser om indholdet af overensstemmelsesvurderings-rapport i henhold til artikel 21, stk. 1.

Stk. 3. Gennemførelsesretsakter udstedt med hjemmel i artikel 21, stk. 4, i eIDAS-forordningen har forrang forud for regler fastsat i medfør af stk. 2.

§ 6. Myndigheder og personer, der udøver opgaver efter artikel 17 og 20 i eIDAS-forordningen om tilsynsorganer og tilsyn med tillidstjenesteudbydere, samt enhver, der i øvrigt yder bistand hertil skal under ansvar efter §§ 152-152 f i straffeloven 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.

§ 7. Medmindre strengere straf er forskyldt efter anden lovgivning, straffes med bøde den, der
1) ikke overholder sikkerhedskrav til kvalificerede tillidstjenesteudbydere, jf. artikel 19, stk. 1, i eIDAS-forordningen,
2) ikke overholder underretningsforpligt for kvalificerede tillidstjeneste-udbydere, jf. artikel 19, stk. 2, i eIDAS-forordningen, eller
3) afgiver urigtige eller vildledende oplysninger til Digitaliseringsstyrelsen
Stk. 2. Der kan pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Ikrafttrædelse mv.

§ 8. Loven træder i kraft den 1. juli 2016.
Stk. 2. Samtidig hermed ophæves lov nr. 417 af 31. maj 2000 om elektroniske signaturer.

§ 9. Loven gælder ikke for Færøerne og Grønland.

Bemærkninger til lovforslaget

Almindelige bemærkninger

1. Indledning

Lovforslaget er et supplement til de regler, som kommer til at gælde i medfør af eIDAS-forordningen.

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 sigter navnlig på at regulere sanktionering af tillidstjenesteudbydere, tavshedspligt for de persongrupper, der beskæftiger sig med tilsyn med tillidstjenesteudbydernes sikkerhedsmæssige indretning og på nationalt plan at fastsætte formelle detaljer omkring sikkerheds- og tilsynsmæssige rammer.

2. 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.

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.

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.

Det følger af eIDAS-forordningen, 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.

Sikkerheds- og tilsynskrav er overordnet reguleret i eIDAS-forordningen, og det fremgår tillige, at Kommissionen har bemyndigelse til at foretage nærmere regulering af områderne.

Det forhold, at der ikke er anført nogen endelig dato for Kommissionens nærmere regulering af sikkerheds- og tilsynskrav danner baggrund for lovforslag. Det er fundet mest hensigtsmæssigt, at der fastsættes bemyndigelser til Finansministeren således, at kravene kan reguleres ved bekendtgørelse.

3. Lovforslagets indhold

Den gældende lov om elektroniske signaturer implementerer direktiv 1999/93/EF om en fællesskabsramme for elektroniske signaturer, herefter kaldt direktivet og 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.

Loven er specifikt tilpasset elektroniske signaturer og forhold, der berører disse.

Da eIDAS-forordningen erstatter og tilbagekalder direktivet, og da eIDAS-forordningen regulerer en række tillidstjenester ud over elektroniske signaturer, er det nødvendigt med denne lov at ophæve loven 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.

4. Økonomiske og administrative konsekvenser for det offentlige

4.1. Økonomiske 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.

Administrative konsekvenser for det offentlige

Lovforslaget skønnes at få administrative konsekvenser for staten.

I medfør af eIDAS-forordningen skal medlemsstaterne udpege et tilsynsorgan. I denne lov 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 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.

Det foreslås, at dele af tilsynsopgaven fortsat udføres af eksterne parter, som det skete under Lov om elektroniske signaturer.

Baggrunden, for at lade dele af tilsynsopgaven udføre af eksterne parter, er at man derigennem kan udnytte den erfaring og kompetence, som allerede findes på markedet. Det kræver specialviden og indsigt at overskue og vurdere den avancerede teknologi, som anvendes hos tillidstjenesteudbydere, og denne viden hentes mest hensigtsmæssigt ind fra markedet, som også vil være certificeret til opgaven.

Lovforslaget skønnes ikke at få direkte administrative konsekvenser for regioner og kommuner.

5. Økonomiske og administrative konsekvenser for erhvervslivet mv.

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

6. Administrative konsekvenser for borgerne

Lovforslaget skønnes ikke at medføre administrative konsekvenser for borgerne.

7. Miljømæssige konsekvenser

Lovforslaget skønnes ikke at have miljømæssige konsekvenser.

8. Forholdet til EU-retten

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

9. Hørte myndigheder og organisationer m.v.

ATP, Danmarks Nationalbank, Dansk Aktionærforening, Danske Revisorer, Datatilsynet, Danske Regioner, Erhvervsstyrelsen, Finansrådet, IT-Branchen, Konkurrence- og Forbrugerstyrelsen, KL, Lønmodtagernes Dyrtidsfond, Miljøstyrelsen, National Sundheds-it, Nets, Vejdirektoratet, Erhvervsstyrelsen, Patent og Varemærkestyrelsen (DKTO), Signaturgruppen, Sikkerhedsstyrelsen, Sundhedsstyrelsen, SKAT, Trafikstyrelsen, Dansk Erhverv, IBM, Danske revisorer, KMD, Finansrådet CSC, Statens-it, BEC – Bankernes EDB-central.

10. Sammenfattende skema

Samlet vurdering af lovforslagets konsekvenser

	Positive konsekvenser/Mindreudgifter	Negative konsekvenser/ Merudgifter
Økonomiske konsekvenser for stat, kommuner, regioner	Ingen.	Ingen.
Administrative konsekvenser for det offentlige	Ingen.	Tilsyns- og rapporteringsopgaver forventes at medføre udgifter for staten svarende til et årsværk.
Økonomiske konsekvenser for erhvervsliver	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 detaljerer 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.

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

Definitioner

Til § 2

Den foreslåede bestemmelse sætter rammerne for fortolkning af loven.

Af praktiske hensyn er de begreber, der er defineret i eIDAS-forordningen, og som også anvendes i lovforslaget gengivet. Dette berører ikke eIDAS-forordningen.

Generelle bestemmelser

Til § 3.

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 til både tillidstjenesteudbydere, og de tillidstjenester tillidstjenesteudbyderne udbyder, overholdes.

.

Til § 4.

Det følger af artikel 19, stk. 1 i eIDAS-forordningen, 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.

Det er ikke nærmere defineret, hvad der ligger i "passende tekniske og organisatoriske foranstaltninger" samt " et sikkerhedsniveau, der svarer til risikoens omfang".

Det foreslås i bestemmelsens stk. 1 at, der sikres hjemmel til, at fastsætte uddybende regulering af, hvordan tillidstjenesteudbydere skal opfylde kravene i artikel 19, stk. 1.

Det vil således være muligt at uddybe artikel 19, stk. 1, ved eksempelvis at henvise til standarder i den nye lovgivning. En sådan henvisning vil kunne fremgå af en bekendtgørelse, vejledning el.

Den foreslåede bestemmelses *stk. 2* tager højde for Kommissionens bemyndigelse til at vedtage gennemførelsesretsakter på området.

Til § 5

Den foreslåede bestemmelses *stk. 1* indfrier kravet i eIDAS-forordningens artikel 17, stk. 1.

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

Den foreslåede bestemmelse er indsat, fordi der ikke er fastsat nogen endelig frist for Kommissionens regulering af tilsynet med tillidstjenesteudbyderne og overensstemmelsesvurderingsrapporten. Bestemmelsen giver således mulighed for at indføre bestemmelser til regulering af områder, der er 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 henstår utilstrækkeligt reguleret.

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

Den foreslåede bestemmelse i *stk. 3* er en forrangsbestemmelse, der tager højde for, at Kommissionen har bemyndigelse til at fastlægge formater og procedurer vedrørende overensstemmelsesvurderingsrapporterne jf. eIDAS-forordningens artikel 21, stk. 4. Udstedelse af sådanne gennemførelsesretsakter kan derfor medføre, at de af finansministeren eventuelt fastsatte bestemmelser ophæves.

Til § 6

Den foreslåede bestemmelse regulerer tavshedspligten for personer der udøver tilsyn med tillidstjenesteudbyderne.

Oplysninger i der tilvejebringes i forbindelse med tilsyn om f.eks. risiko- og sikkerhedsvurderinger, som kunne indikere svagheder i systemerne herunder i systeminstallationerne samt de sikkerhedsmæssige processer, er eksempler på oplysninger, det er afgørende, at tilsynet får indsigt i, og derfor skal kunne undtages fra aktindsigt. Dette skyldes, at 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 har 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 den offentlige sektor. Angreb vil ligeledes mindske tilliden til digitale tjenester og kan dermed hindre digitalisering og dermed begrænse mulige gevinster.

Det en forudsætning for, at Digitaliseringsstyrelsen kan føre det nødvendige tilsyn med tillidstjenesteudbydere, at alle oplysninger og sikkerhedsmæssige procedurer om systemer, sårbarheder mv. indgår i den rapportering, der indgives til Digitaliseringsstyrelsen. 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.

Der findes i dansk lovgivning flere eksempler på tavshedspligtbestemmelser for tilsynsorganer, herunder i Arbejdsmiljøloven og Lov om finansiel virksomhed.

Bilag 5 (side 1100 ff.) til Offentlighedskommissionens betænkning nr. 1510/2009 indeholder en oversigt over særlige tavshedspligtbestemmelser inden for de enkelte ministeriers ressortområder.

Det følger af forordningens artikel 18, at medlemsstaternes tilsynsorganer skal samarbejde med henblik på at udveksle god praksis.

Til § 7

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

Den foreslåede bestemmelse indfrier dette.

Til § 8

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.

Til § 9

Den foreslåede bestemmelse fastslår, at loven ikke gælder for Færøerne og Grønland.