



Fremsat den 22. oktober 2025 af ministeren for digitalisering (Caroline Stage Olsen)

Forslag

til

Lov om den nationale digitale identitetstegnebog

Kapitel 1

Lovens formål og definitioner

§ 1. Loven har til formål at understøtte den nationale digitale identitetstegnebog, der består af de tekniske løsninger tegnebogsapplikation, bevisudstedelsesservice og modtagerpartregister.

§ 2. I denne lov forstås følgende:

- 1) Autentisk kilde: Et register eller et system, som en offentlig myndighed eller et offentligretligt organ har ansvaret for, der indeholder og kan levere attributter om en fysisk person eller genstand, og som anses for at være en primær kilde til disse oplysninger eller er anerkendt som autentisk i overensstemmelse med dansk ret, herunder administrativ praksis.
- 2) Bevis: En elektronisk attestering af attributter, der er udstedt af eller på vegne af en offentlig myndighed eller et offentligretligt organ med ansvar for en autentisk kilde.
- 3) Bevisudstedelsesservice: En teknisk løsning i den nationale digitale identitetstegnebog, hvor Digitaliseringsstyrelsen på vegne af en offentlig myndighed eller et offentligretligt organ med ansvar for en autentisk kilde kan udstede beviser.
- 4) Bruger: En fysisk person, der anvender tegnebogsapplikationen.
- 5) Modtagerpart: En juridisk enhed med et CVR-nummer eller en juridisk enhed registreret i et register i et andet EU-/EØS-land svarende til Det Centrale Virksomhedsregister, der kan modtage beviser fra en brugers tegnebogsapplikation.
- 6) Modtagerpartregister: En teknisk løsning i den nationale digitale identitetstegnebog, bestående af et offentligt register, hvor en modtagerpart registrerer sig.
- 7) Offentlig myndighed: En statslig, regional eller kommunal myndighed eller sammenslutninger heraf.
- 8) Offentligretligt organ: Et organ,

- a) der er oprettet specielt med henblik på at imødekomme almenhedens behov, dog ikke behov af industriel eller kommerciel karakter,
- b) der er en juridisk person, og
- c) som for mere end halvdelen vedkommende finansieres af staten, regionale eller lokale myndigheder eller af andre offentligretlige organer eller er underlagt ledelsesmæssig kontrol af disse myndigheder eller organer eller har en bestyrelse eller direktion eller et tilsynsråd, hvor mere end halvdelen af medlemmerne udpeges af staten, regionale eller kommunale myndigheder eller andre offentligretlige organer.

- 9) Tegnebogsapplikation: En teknisk løsning i den nationale digitale identitetstegnebog, stillet til rådighed af Digitaliseringsstyrelsen gennem en mobilapplikation, som gør det muligt for en bruger at lagre, forvalte, validere og dele beviser med henblik på at overføre dem til modtagerparter og andre brugere.

Kapitel 2

Tegnebogsapplikationen

§ 3. Digitaliseringsstyrelsen stiller en tegnebogsapplikation til rådighed for fysiske personer. Digitaliseringsstyrelsen sikrer forvaltning, udvikling, drift og vedligeholdelse af tegnebogsapplikationen.

Stk. 2. Opretter en bruger, der har et CPR-nummer sig i tegnebogsapplikationen, dannes bevis for brugerens identitet. Brugeren kan tilføje sit foto til sin tegnebogsapplikation, hvorefter beviset sammen med fotoet vil udgøre et legitimationsbevis. Dette legitimationsbevis tjener samme formål som legitimationskort udstedt i medfør af lov om udstedelse af legitimationskort.

Stk. 3. Opretter en bruger, der ikke har CPR-nummer sig i tegnebogsapplikationen, dannes bevis for brugerens navn og fødselsdato.

Stk. 4. Som led i udviklingen og driften af tegnebogsapplikationen sikrer Digitaliseringsstyrelsen, at en bruger kan

anvende sin tegnebogsapplikation til at interagere med en anden brugers tegnebogsapplikation med henblik på at validere og dele beviser.

§ 4. Digitaliseringsstyrelsen kan træffe afgørelse om spærring af tegnebogsapplikationen.

Stk. 2. Ministeren for digitalisering fastsætter regler om afgørelser, jf. stk. 1, samt om forvaltningen og anvendelsen af tegnebogsapplikationen, herunder om en brugers oprettelse, en brugers spærring af tegnebogsapplikationen, en brugers sletning af beviser i tegnebogsapplikationen, tekniske krav, krav til foto og inaktivering af tegnebogsapplikationen efter brugers dødsfald.

Kapitel 3

Bevisudstedelsesservice

§ 5. Digitaliseringsstyrelsen stiller en bevisudstedelsesservice til rådighed for offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde, der som led i deres myndighedsudøvelse kan levere data fra deres autentiske kilde til brug for udstedelse af beviser til tegnebogsapplikationen. Digitaliseringsstyrelsen sikrer forvaltning, udvikling, drift og vedligeholdelse af bevisudstedelsesservice.

Stk. 2. Digitaliseringsstyrelsen sikrer som led i udviklingen og driften, at bevisudstedelsesservice indeholder følgende funktionaliteter:

- 1) Oprettelse, ændring, ajourføring og nedlæggelse af typer af beviser.
- 2) Dannelse og udstedelse af beviser.
- 3) En liste over udstedte bevisers gyldighed.
- 4) Logning af beviser, der er udstedt eller forsøgt udstedt, og transmissionskald til og fra offentlige myndigheders og offentligretlige organers it-systemer indeholdende autentiske kilder.
- 5) Identifikation og autentifikation af brugere.

§ 6. En offentlig myndighed eller et offentligretligt organ, med ansvar for en autentisk kilde, skal anvende Digitaliseringsstyrelsens bevisudstedelsesservice, når de som led i deres myndighedsudøvelse vil levere data fra deres autentiske kilde til brug for udstedelse af beviser til tegnebogsapplikationen, jf. dog stk. 2.

Stk. 2. Bestemmelsen i stk. 1 gælder ikke, hvis Digitaliseringsstyrelsens bevisudstedelsesservice ikke kan imødekomme den offentlige myndigheds eller det offentligretlige organs særlige behov. Den offentlige myndighed eller det offentligretlige organ kan i sådanne tilfælde selv udstede beviser til tegnebogsapplikationen. Bevisudstedelsen skal opfylde de regler, der fastsættes i medfør af § 7, stk. 2.

Stk. 3. En offentlig myndighed eller et offentligretligt organ, som benytter Digitaliseringsstyrelsens bevisudstedelsesservice, sikrer opdatering og ajourføring af typer af beviser samt spærring af beviser.

§ 7. Ministeren for digitalisering fastsætter regler om forvaltningen og anvendelsen af Digitaliseringsstyrelsens bevisudstedelsesservice, herunder om offentlige myndigheders

og offentligretlige organers tilslutning til og anvendelse af bevisudstedelsesservice samt tekniske krav hertil.

Stk. 2. Ministeren for digitalisering fastsætter regler om en offentlig myndigheds eller offentligretligt organs forvaltning og anvendelse af egen bevisudstedelse for beviser, der udstedes til tegnebogsapplikationen, jf. § 6, stk. 2, herunder om tekniske krav til egen bevisudstedelse.

Kapitel 4

Retsvirkning af digitalisering af beviser

§ 8. Vedkommende minister kan på sit område fastsætte regler om digitalisering af beviser til tegnebogsapplikationen og om digitaliseringens retsvirkninger, jf. dog stk. 2.

Stk. 2. Bestemmelsen i stk. 1 finder ikke anvendelse, hvor der i medfør af anden lovgivning er fastsat regler om digitalisering af beviser og retsvirkningen heraf.

Kapitel 5

Modtagerpartregisteret

§ 9. Digitaliseringsstyrelsen stiller et modtagerpartregister til rådighed for modtagerpart. Digitaliseringsstyrelsen sikrer forvaltning, udvikling, drift og vedligeholdelse af modtagerpartregisteret.

Stk. 2. En modtagerpart skal være registreret i modtagerpartregisteret, når en modtagerpart anvender en teknologi til at modtage beviser, hvorved beviser overføres via internet, jf. dog stk. 3.

Stk. 3. En modtagerpart som ikke er registreret i modtagerpartregisteret, kan under anvendelse af en teknologi, hvor beviser overføres via internettet, alene anmode om at modtage bevis, der bekræfter, hvorvidt en bruger er over eller under en given aldersgrænse.

Stk. 4. Ministeren for digitalisering kan fastsætte regler om, at overførsel via internettet af andre beviser end det bevis, der er nævnt i stk. 3, ikke kræver registrering i modtagerpartregisteret.

§ 10. Ministeren for digitalisering fastsætter regler om forvaltningen af modtagerpartregisteret, herunder om en modtagerparts registrering i modtagerpartregisteret, om tekniske krav til en modtagerpart samt om tekniske krav til modtagelse af beviser.

§ 11. Digitaliseringsstyrelsen kan spærre en modtagerpart, der er registreret i modtagerpartregisteret, hvis denne anvender modtagerpartregisteret eller beviser på en svigagtig eller en anden ulovlig måde, i strid med regler fastsat i medfør af § 10 eller i øvrigt på en måde, der er åbenlyst egnet til at svække tilliden til den nationale digitale identitetstegnebog.

Stk. 2. Ministeren for digitalisering kan fastsætte regler om betingelser for en modtagerparts genregistrering efter spærring, jf. stk. 1.

Kapitel 6

Erstatningsansvar

§ 12. Digitaliseringsstyrelsen kan alene blive erstatningsansvarlig som følge af fejl begået i forbindelse med bevisudstedelse i medfør af § 5, stk. 2, nr. 2 og 5.

Kapitel 7

Tilsyn

§ 13. Digitaliseringsstyrelsen fører tilsyn med forvaltning, drift og vedligeholdelse af den nationale digitale identitetstegnebog.

Stk. 2. Digitaliseringsstyrelsen kan føre tilsyn med offentlige myndigheders og offentligretlige organers overholdelse af regler fastsat i medfør af § 7, stk. 2.

Kapitel 8

Behandling af personoplysninger

§ 14. Digitaliseringsstyrelsen er dataansvarlig for behandling af personoplysninger i forbindelse med en brugers oprettelse af sin tegnebogsapplikation.

Stk. 2. Digitaliseringsstyrelsen er dataansvarlig for behandling af personoplysninger i bevisudstedelsesservicen,

samt for behandling af personoplysninger i forbindelse med levering af et udstedt bevis, indtil beviset er leveret til en brugers tegnebogsapplikation.

Stk. 3. Digitaliseringsstyrelsen er dataansvarlig for behandling af CVR-numre eller tilsvarende registreringer i et register i et andet EU-/EØS-land og kontaktoplysninger i modtagerpartregisteret, der henviser til en personligt ejet virksomhed, jf. § 2, nr. 5.

Stk. 4. En modtagerpart er dataansvarlig for sin behandling af de personoplysninger, som er indeholdt i de beviser, der overføres fra den enkelte brugers tegnebogsapplikation.

Kapitel 9

Ikrafttrædelses- og territorialbestemmelse

§ 15. Loven træder i kraft den 1. januar 2026.

§ 16. Loven gælder ikke for Færøerne og Grønland, men kan ved kongelig anordning helt eller delvis sættes i kraft for Færøerne og Grønland med de ændringer, som henholdsvis de færøske og de grønlandske forhold tilsiger.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning
2. Den nationale digitale identitetstegnebog
 - 2.1. Gældende ret
 - 2.1.1. Legitimationskort til personer på 15 år eller derover
 - 2.1.2. Pas
 - 2.1.3. Sundhedskort
 - 2.1.4. Kørekort
 - 2.1.5. Opholdskort til udlændinge
 - 2.2. Digitaliseringsministeriets overvejelser og den foreslåede ordning
 - 2.2.1. Tegnebogsapplikationen
 - 2.2.1.1. Beviser i tegnebogsapplikationen
 - 2.2.2. Tilrådighedsstilling af bevisudstedelsesservicen
 - 2.2.3. Modtagerpartregisteret
3. Forholdet til databeskyttelsesforordningen og databeskyttelsesretten
 - 3.1. Gældende ret
 - 3.2. Digitaliseringsministeriets overvejelser og den foreslåede ordning
4. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige
 - 4.1. Syv principper for digitaliseringsklar lovgivning
5. Økonomiske og administrative konsekvenser for erhvervslivet m.v.
6. Administrative konsekvenser for borgerne
7. Klimamæssige konsekvenser
8. Miljø- og naturmæssige konsekvenser
9. Forholdet til EU-retten
10. Hørte myndigheder og organisationer m.v.
11. Sammenfattende skema

1. Indledning

Danmark har gennem de seneste mange år markeret sig som digitalt foregangsland. Det gælder bl.a. på de store digitale infrastrukturløsninger som NemKonto, Digital Post, MitID og NemLog-in.

Disse løsninger er alle nationale løsninger, der som udgangspunkt er udviklet til brug i dansk kontekst. Særligt MitID adskiller sig dog ved også at kunne anvendes i grænseoverskridende sammenhæng. Den grænseoverskridende anvendelse er en udmøntning 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). eIDAS-forordningen fra 2014 bygger på, at hver enkelt medlemsstat udvikler en eID-løsning, der efter godkendelse i EU-Kommissionen skal gensidigt anerkendes. Det har imidlertid vist sig at være en stor opgave for de enkelte medlemsstater, og ikke alle medlemsstater har etableret egne EU-anmeldte og EU-anerkendte identifikationsløsninger, der således ikke er obligatoriske at etablere.

På ovenstående baggrund igangsatte EU-Kommissionen en revision af eIDAS-forordningen med henblik på at styrke den fælleseuropæiske anvendelse af elektroniske identifikationsløsninger. Forordningen blev ændret ved Europa-Parlamentets og Rådets Forordning (EU) 2024/1183 af 11. april 2024 om ændring af forordning (EU) nr. 910/2014, for så vidt angår fastlæggelse af den europæiske ramme for digital identitet. Den ændrede forordning trådte i kraft den 20. maj 2024 (herefter eIDAS2).

Den ændrede forordning betyder på området for elektroniske identifikationsordninger, at hver medlemsstat forpligtes til at etablere mindst en europæisk digital identitetstegnebog. Den europæiske digitale identitetstegnebog skal i fremtiden både være en fælleseuropæisk identifikationsløsning, indeholde beviser og på sigt også potentielt betalingsmuligheder m.v.

Formålet med nærværende lovforslag er udelukkende at regulere den rent nationale digitale identitetstegnebog. Lovforslaget indeholder således ikke supplerende bestemmelser til eIDAS2.

I Danmark sker første trin af udviklingen af den europæiske digitale identitetstegnebog ved etablering af den nationale digitale identitetstegnebog, som reguleres ved denne lov. Det står klart, at det er en teknisk kompliceret opgave at få alle elementer i den europæiske digitale identitetstegnebog til at virke sammen. EU-Kommissionen er således ved at udarbejde retsakter, der supplerer og konkretiserer forordningsteksten. Dertil kommer krav til certificering af identitetstegnebogen og tilsynsopgaver med såvel identitetstegnebogen som med de virksomheder og myndigheder, der i forordningen bliver forpligtet til at modtage tegnebogen. Endvidere har brugere af identitetstegnebogen en lang række rettigheder, som teknisk skal indbygges i identitetstegnebogen, og understøtte at brugerens retssikkerhed tilgodeses i selve tegnebogsløsningen.

Den nationale digitale identitetstegnebog sikrer en hurtig idriftsættelse af en rent national løsning, der udgør første trin på vej til den europæiske digitale identitetstegnebog. Den trinvis indfasning skal sikre, at dele af tegnebogens grundfunktionalitet implementeres tidligere, end det ellers ville være muligt med den europæiske digitale identitetstegnebog, der opfylder alle eIDAS2 krav. Dette skal medvirke til, at tegnebogen hurtigt kan skabe værdi og mindske risici, der kan være forbundet med it-projekter. Derudover vil der i første trin af implementeringen være etableret it-systemer og komponenter, som forventes

genbrugt og videreudviklet frem mod implementering af den europæiske digitale identitetstegnebog.

Den borgerrettede del af den nationale identitetstegnebog bygges som en mobilapplikation, der kan downloades til en mobilenhed fra en platform anvist af Digitaliseringsstyrelsen. Tegnebogsapplikationen fungerer i praksis som et samlingspunkt og opslagsværk for de digitale beviser. Den enkelte bruger kan selv vælge hvilke beviser, der skal udstedes til brugerens personlige tegnebogsapplikation. Tegnebogsapplikationen vil således adskille sig fra enkeltstående mobilapplikationer, som f.eks. den digitale kørekortapplikation, ved at kunne indeholde flere forskellige beviser i samme applikation.

Regeringen og aftalepartierne bag forebyggelsesplanen har i marts 2025 indgået en aftale, der giver detailhandlen mulighed for at anvende elektronisk aldersverificering ved fysisk salg for at sikre, at alkohol, tobak og nikotinprodukter ikke sælges til mindreårige. Hermed er det både muligt at anvende elektronisk aldersverificering ved salg af alkohol, tobak og nikotinprodukter ved online salg og i fysiske butikker. Den nationale digitale identitetstegnebog vil fra idriftsættelsen af løsningen kunne anvendes til aldersverifikation. Det er ikke alene ved køb af aldersbegrænsede produkter, at aldersverifikation er påkrævet, idet kravet tillige indgår som forudsætning for at kunne tilgå forskellige onlinetjenester. Det er hensigten, at den nationale digitale identitetstegnebog også i disse sammenhænge vil være et relevant værktøj.

Regeringen har igangsat initiativer, der skal værne om børn og unge i digital sammenhæng. Et af eksemplerne er Alliancen for en tryk hverdag for børn og unge, som regeringen har lanceret sammen med en række organisationer. Alliancen vil bl.a. arbejde på effektiv og privatlivsbeskyttende aldersverifikation i EU, så brugeren skal verificere sin alder, når der oprettes en profil på sociale medier.

Et andet eksempel er den af regeringen nedsatte trivselskommission, der i februar 2025 har afgivet rapporten ”Kort om Trivselskommissionens afrapportering. Et dansk svar på en vestlig udfordring”, og som i anbefaling 5 til et afbalanceret digitalt liv anbefaler effektiv og obligatorisk aldersverifikation.

EU-Kommissionen har også igangsat arbejde med en aldersverifikationsløsning, og det er hensigten, at den nationale digitale identitetstegnebog skal være kompatibel hermed.

2. Den nationale digitale identitetstegnebog

Lovforslaget har til formål at regulere den nationale digitale identitetstegnebog. Den nationale digitale identitetstegnebog anvendes som samlet betegnelse for de nødvendige tekniske løsninger, der tilsammen sikrer en funktionel national digital identitetstegnebog.

Lovforslaget regulerer rettigheder og pligter for de aktører, der kan anvende den nationale digitale identitetstegnebog.

Lovforslaget regulerer endvidere, at Digitaliseringsstyrelsen forpligtes til at udvikle den nationale digitale identitetstegnebog for de involverede aktører. Digitaliseringsstyrelsen tilrådighedsstiller herunder en bevisudstedelsesservice, som offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde skal anvende til at få beviser udstedt til brugernes tegnebogsapplikation. Brugen af bevisudstedelsesservicen er dog ikke obligatorisk, hvis den offentlige myndighed eller det offentligretlige organ har særlige behov til bevisudstedelsen, som ikke kan opfyldes af den bevisudstedelsesservice, som Digitaliseringsstyrelsen stiller til rådighed.

Lovforslaget giver ikke virksomheder eller borgere ret til at udstede beviser til den nationale digitale identitetstegnebog.

Brugen af den nationale digitale identitetstegnebog er frivillig for de centrale aktører: brugere, offentlige myndigheder og offentligretlige organer, som leverer data fra deres autentiske kilde til brug for udstedelse af beviser til tegnebogsapplikationen samt modtagerparter.

2.2. Gældende ret

Der findes i Danmark en lang række enkeltstående mobilapplikationer. Digitaliseringsstyrelsen foretog i juli 2023 en kortlægning af offentlige mobilapplikationer. Kortlægningen viste, at der på tidspunktet for kortlægningen var 74 offentlige danske mobilapplikationer, der opfyldte nærmere fastsatte kriterier, herunder at appen var målrettet et stort antal borgere, for at tælle med i kortlægningen. Det må på den baggrund konstateres, at der er et stort potentiale for at tilføre den nationale digitale identitetstegnebog indhold og derved give brugeren mulighed for at samle de offentlige mobilapplikationer. Der findes ikke gældende ret, der regulerer en national digital identitetstegnebog eller lignende offentlig mobilapplikation, hvor en bruger kan samle sine digitale beviser udstedt af offentlige myndigheder eller offentligretlige organer.

Der findes gældende ret, som regulerer anvendelsen og retsvirkningen af en række af de forskellige fysiske og digitale individuelle legitimationsformer, som potentielt vil kunne udstedes til tegnebogsapplikationen.

2.1.1. Legitimationskort til personer på 15 år eller derover

De gældende regler om udstedelse af legitimationskort findes i lov om udstedelse af legitimationskort (lovbekendtgørelse nr. 236 af 15. marts 2017). Lov om udstedelse af legitimationskort har til formål at sikre, at alle personer på 15 år og derover, der er bopælsregistreret i Det Centrale Personregister (CPR), kan erhverve et legitimationskort. Loven om udstedelse af legitimationskort løser et praktisk problem ved at gøre det muligt for borgere, der hverken har kørekort eller pas at erhverve fysisk billedlegitimation, der størrelsesmæssigt minder om et fysisk kørekort. Lov om udstedelse af legitimationskort regulerer imidlertid alene fysiske legitimationsbeviser og ikke digitale legitimationsbeviser.

2.1.2. Pas

De gældende regler om udstedelse af pas findes i lov om pas til danske statsborgere m.v., jf. lovbekendtgørelse nr. 76 af 19. januar 2017, med senere ændringer og bekendtgørelse om pas mv. (bekendtgørelse nr. 2693 af 28. december 2021 med senere ændringer).

Formålet med passet er, at indehaveren skal kunne legitimere sig i forbindelse med rejser til og fra udlandet.

2.1.3. Sundhedskort

De gældende regler om udformningen af sundhedskortet findes i bekendtgørelse om valgfri indplacering i sikringsgrupper og udstedelse af sundhedskort mv. (bekendtgørelse nr. 529 af 21. maj 2025). Bekendtgørelsen er udstedt med hjemmel i sundhedsloven, jf. lovbekendtgørelse nr. 275 af 12. marts 2025. Efter gældende ret forsynes en person, der er registreret i Det Centrale Personregister (CPR) med bopæl eller fast opholdssted her i landet med et sundhedskort, som giver personen ret til sundhedsydelser, jf. sundhedslovens § 12 og §§ 6 og 7 i bekendtgørelse om valgfri indplacering i sikringsgrupper og udstedelse af sundhedskort mv. (bekendtgørelse nr. 529 af 21. maj 2025).

Sundhedskortet gælder som dokumentation for retten til sundhedsydelser, jf. sundhedslovens § 12, stk. 1, 2. pkt.

2.1.4. Kørekort

De gældende regler om kørekort, herunder vedrørende betingelserne for erhvervelse af kørekort, findes i kørekortbekendtgørelsen (bekendtgørelse nr. 875 af 27. juni 2024 om kørekort med senere ændringer). Bekendtgørelsen er udstedt med hjemmel i færdselsloven, jf. lovbekendtgørelse nr. 168 af 14. februar 2023, med senere ændringer.

Kørekortbekendtgørelsen indeholder bestemmelser, der gennemfører Europa-Parlamentets og Rådets direktiv 2006/126/EF af 20. december 2006 om kørekort med senere ændringer (3. kørekortdirektiv).

Direktivet fastsætter bl.a. en række mindstekrav til udstedelse af kørekort og til udformningen af kørekortet. Direktivet forudsætter bl.a., at et kørekort giver førerret til én eller flere kategorier af motordrevne køretøjer, dertil fastsættes krav om, at kørekort alene tildeles, efter at en person har bestået en teoretisk prøve og en praktisk prøve.

Kørekortet har til formål at dokumentere førerret til et motordrevet køretøj. Ved 3. kørekortdirektiv er der bl.a. indført en enhedsmodel til kørekort i medlemslandene (EU-kørekortmodellen). Formålet hermed er bl.a. at give mulighed for at forbedre beskyttelsen mod forfalskninger.

Europa-Parlamentet og Rådet er ved at udarbejde det 4. kørekortdirektiv. Det er bl.a. hensigten med det 4. kørekortdirektiv, at europæiske kørekort bliver digitaliseret og skal kunne udstedes til den europæiske identitetstegnebog.

Indehaveren af et dansk kørekort kan som supplement til sit kørekort være indehaver af et digitalt kørekort, jf. kørekortbekendtgørelsens § 6, stk. 1. Et digitalt kørekort, gælder som dokumentation for indehaverens kørekort under kørsel i Danmark og følger i øvrigt gyldigheden for indehaverens kørekort, jf. kørekortbekendtgørelsens § 6, stk. 2.

2.1.5. Opholdskort til udlændinge

Enhver tredjelandsstatsborger, der meddeles opholdstilladelse i Danmark efter udlændingelovens §§ 7-9 f, 9i-n, 9 p og 9 q (lovbekendtgørelse nr. 1009 af 2. september 2024), bortset fra udlændinge under 18 år, der har fast ophold hos forældremyndighedens indehaver, får udstedt opholdskort med biometriske kendetegn (fotografi og fingeraftryk). Udlændinge under 18 år, der har fast ophold hos forældremyndighedens indehaver, behøver ikke opholdskort, men kan få udstedt opholdskort, hvis der ansøges om det. Der vil i den forbindelse blive optaget biometri, medmindre udlændingen er under 6 år, hvorefter et opholdskort alene vil blive udstedt med fotografi. Udlændinge under 18 år, der ikke har fast ophold hos forældremyndighedens indehaver, men i stedet bor hos f.eks. plejeforældre, nære slægtninge eller har ophold på baggrund af skoleophold, skal have udstedt opholdskort, og der skal derfor optages biometri i forbindelse med, at ansøgningen indgives. De biometriske kendetegn lagres på en chip i kortet. Opholdskortet er dokumentation for, at den pågældende har en opholdstilladelse i Danmark.

En tredjelandsstatsborger skal under ophold her i landet til stadighed medføre dokumentation for sin danske opholdstilladelse, jf. § 32 i udlændingebekendtgørelsen (bekendtgørelse nr. 1532 af 5. december 2024). Udlændinge med ret til ophold efter EU-reglerne om fri bevægelighed får efter ansøgning udstedt et registreringsbevis eller et opholdskort i overensstemmelse med EU-opholdsbekendtgørelsen (bekendtgørelse nr. 1457 af 6. oktober 2020).

Det følger af CPR-lovens § 17, jf. lovbekendtgørelse nr. 1010 af 23. juni 2023, med senere ændringer, at udlændinge med opholdstilladelse eller bevis registreres i Det Centrale Personregister (CPR).

En asylansøger har ikke opholdstilladelse i Danmark og får derfor heller ikke udstedt et opholdskort, ligesom en asylansøger ikke bopælsregistreres i CPR. En asylansøger modtager et asylansøgerkort som bevis på, at den pågældende har ret til at opholde sig i Danmark, mens sagen behandles. Hvis en asylansøger meddeles opholdstilladelse efter udlændingelovens § 7 (asyl), modtager den pågældende et opholdskort.

2.2. Digitaliseringsministeriets overvejelser og den forelåede ordning

Med forslaget om en national digital identitetstegnebog er det indledningsvist hensigten at udvikle bevis for identitet, samt at muliggøre at brugeren kan tilføje sit foto til bevis for identitet, således at beviset sammen med fotoet kan fungere som billedlegitimation på samme måde som legitimati-

onskort udstedt efter lov om legitimationskort. For brugere uden CPR-nummer er det hensigten at udvikle bevis for navn og fødselsdato. Det er endvidere hensigten, at det gradvist skal være muligt for brugeren at få udstedt flere beviser til tegnebogsapplikationen, forudsat at myndigheden, der råder over de data, der kræves for at danne et givent bevis, muliggør bevisudstedelse til tegnebogsapplikationen.

Eksisterende offentlige mobilapplikationer, der indeholder enkeltstående beviser, vil fortsat kunne eksistere som selvstændige mobilapplikationer, uanset at beviserne tillige vil kunne udstedes til den nationale digitale identitetstegnebog. Forslaget hindrer heller ikke udviklingen af nye offentlige selvstændige mobilapplikationer.

Den nationale digitale identitetstegnebog er en nyskabelse i den offentlige digitalisering, og udgør første trin på vej til den europæiske digitale identitetstegnebog. Indledningsvis er det alene Digitaliseringsstyrelsen, der udsteder beviser til den nationale digitale identitetstegnebog i form af bevis for identitet, som ved tilføjelse af foto vil udgøre et legitimationsbevis, der kan tjene samme formål som legitimationskortet udstedt i medfør af lov om udstedelse af legitimationskort.

Med den løbende udvikling af identitetstegnebogen vil det blive muligt for andre offentlige myndigheder og offentlig-retlige organer, at få udstedt beviser til en brugers tegnebogsapplikation. For at gøre udstedelsen smidig for myndighederne er det hensigten, at Digitaliseringsstyrelsen stiller en bevisudstedelsesservice til rådighed for myndighederne.

En modtagerpart kan være såvel en offentlig myndighed m.v. som en privat aktør.

Et bevis fra tegnebogsapplikationen kan modtages på forskellig vis, hvoraf nogle typer modtagelse kræver registrering i modtagerpartregisteret.

2.2.1. Tegnebogsapplikationen

Tegnebogsapplikationen er et værktøj som brugeren kan benytte til at dele digitale beviser på en sikker og privatlivsbeskyttende måde.

Tegnebogsapplikationen er en applikation, som brugeren downloader og installerer på sin mobile enhed, typisk en smartphone. Brugeren skal anvende sit MitID eller andet eID, som er integreret til eID-gateway (herefter MitID eller andet eID), for at oprette sig i tegnebogsapplikationen.

Hver bruger, der opretter sig i tegnebogsapplikation, har sin egen individuelle tegnebogsapplikation. De beviser, som brugeren anmoder om at få udstedt, er kun placeret på brugers enhed, og er ikke centralt lagret. Det betyder bl.a., at tegnebogsapplikationens beviser udelukkende er underlagt brugerens råderet, og brugen af tegnebogsapplikationen er frivillig. Brugeren har således enekontrol i forhold til anvendelse af bevis for identitet og øvrige beviser, der er indeholdt i tegnebogsapplikationen. Tegnebogsapplikationen

i medfør af den foreslåede lov skal således forstås som hver brugers individuelle tegnebogsapplikation.

En bruger, der vælger at bruge tegnebogsapplikationen, kan kun downloade tegnebogsapplikationen fra en af Digitaliseringsstyrelsen anvist platform, som f.eks. kan være Google Play eller Apples App Store. Af sikkerhedshensyn må ikke-anviste platforme ikke benyttes til at downloade tegnebogsapplikationen.

2.2.1.1. Beviser i tegnebogsapplikationen

Som anført i pkt. 2.2. udvikles bevis for brugerens identitet, som sammen med foto vil udgøre et legitimationsbevis, der kan tjene samme formål som legitimationskortet udstedt i medfør af lov om udstedelse af legitimationskort. Til brugere uden CPR-nummer udvikles bevis for navn og fødselsdato. Det er endvidere hensigten, at det gradvist skal være muligt for brugerne at få udstedt flere beviser til tegnebogsapplikationen, forudsat at den offentlige myndighed eller det offentligretlige organ, der råder over de data, der kræves for at danne et givent bevis, muliggør bevisudstedelse.

Som anført i pkt. 2.1.1. har lov om udstedelse af legitimationskort til formål at sikre, at alle personer på 15 år og derover, der er bopælsregistreret i Det Centrale Personregister (CPR), kan erhverve et legitimationskort. Loven om udstedelse af legitimationskort løser et praktisk problem ved at gøre det muligt for borgere, der hverken har kørekort eller pas, at erhverve fysisk billedlegitimation, der størrelsesmæssigt minder om et fysisk kørekort. Lov om udstedelse af legitimationskort regulerer imidlertid alene fysiske legitimationskort og ikke digitale legitimationsbeviser. Der findes derfor ikke på nuværende tidspunkt et digitalt legitimationsbevis, som kan anvendes til generel digital legitimation.

Digitaliseringsministeriet finder efter en samlet vurdering, at der er et behov for, at en bruger skal kunne legitimere sig i digitale sammenhænge, hvilket ikke understøttes af et fysisk legitimationsbevis. Det er Digitaliseringsministeriets vurdering, at der er stort potentiale i, at den nationale digitale identitetstegnebog indeholder et digitalt legitimationsbevis, som kan tjene samme formål som det fysiske legitimationskort.

Det er op til de ansvarlige ressortministre at vurdere om data fra deres enkeltstående mobilapplikationer, som f.eks. kørekort-appen eller sundhedskort-appen, på sigt skal kunne udstedes som beviser til tegnebogsapplikationen. Digitaliseringsministeriet har derfor vurderet, at det er hensigtsmæssigt, at digitalisering af beviser til tegnebogsapplikationen og retsvirkningen af digitaliserede beviser fra andre ressortområder kan reguleres i bekendtgørelsesform af hensyn til at sikre fleksibilitet og rummelighed i reguleringen af disse. Det er således hensigten, at den foreslåede § 8 skal kunne gøre det administrativt hurtigere at understøtte den retlige regulering af udstedelse af beviser til tegnebogsapplikation på de forskellige ressortområder. Det er op til det enkelte ressortområde at vurdere behovet for digitalisering

af beviser til tegnebogsapplikationen, samt at vurdere om dette er i overensstemmelse med øvrig lovgivning på området. De enkelte ressortområder kan desuden foretage en selvstændig vurdering af, om beviser inden for deres område kan digitaliseres og gøres tilgængelige for anvendelse i tegnebogsapplikationen.

2.2.2. Tilrådighedsstilling af bevisudstedelsesservicen

Med introduktionen af bevisudstedelsesservicen er det Digitaliseringsministeriets hensigt at understøtte en fortsat udvikling af tidssvarende digital infrastruktur i den offentlige sektor. Formålet med bevisudstedelsesservicen er, at offentlige myndigheder og offentligretlige organer, som har ansvaret for en autentisk kilde, kan få udstedt beviser digitalt til en brugers tegnebogsapplikation, som led i deres myndighedsudøvelse, ved at levere data fra deres autentiske kilde til bevisudstedelsesservicen. Bevisudstedelsesservicen er således alene et værktøj til oprettelsen af beviser, der letter arbejdsbyrden hos den enkelte offentlige myndighed eller offentligretlige organ. Den tekniske løsning, bevisudstedelsesservicen, udgør sammen med de tekniske løsninger tegnebogsapplikationen og modtagerpartregisteret den nationale digitale identitetstegnebog.

Det vil med den foreslåede ordning være Digitaliseringsstyrelsen, der indkøber og udvikler bevisudstedelsesservicen, hvorefter Digitaliseringsstyrelsen vil være systemejer og varetage de opgaver, som følger hermed. Digitaliseringsstyrelsen har i denne sammenhæng en særlig status som instrument og teknisk tjeneste for hele den offentlige sektor, og skal imødekomme alle offentlige myndigheders og offentligretlige organers bestillinger i overensstemmelse med lovens bestemmelser.

Den udbudsretlige relation mellem Digitaliseringsstyrelsen og de offentlige myndigheder og offentligretlige organer er i denne henseende af intern karakter, kendetegnet ved Digitaliseringsstyrelsens underordning og afhængighed af de offentlige myndigheder og offentligretlige organer, når de afgiver deres bestillinger i medfør af loven.

Offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde vil med den foreslåede ordning have en pligt til at anskaffe bevisudstedelsesservicen fra Digitaliseringsstyrelsen, og vil skulle anvende bevisudstedelsesservicen, når beviset udstedes til tegnebogsapplikationen som led i myndighedsudøvelse. Dette gælder dog ikke, hvis bevisudstedelsesservicen ikke kan imødekomme en offentlig myndigheds eller et offentligretligt organs særlige behov, jf. den foreslåede bestemmelse i § 6, stk. 2.

For den offentlige sektor vil bevisudstedelsesservicen være en central løsning til understøttelse af et mere digitaliseret samfund, idet bevisudstedelsesservicen gør det nemt for en myndighed at digitalisere beviser, som f.eks. før alene var fysiske beviser. Bevisudstedelsesservicen understøtter den teknologiske udvikling af identitetstegnebogskonceptet, der introduceres med eIDAS2. Det foreslås derfor ved denne

lov, at Digitaliseringsstyrelsen pålægges som myndighedsopgave at stille bevisudstedelsesservicen til rådighed for offentlige myndigheder og offentligretlige organer på vegne af den danske stat. Tilrådighedsstillelsen af bevisudstedelsesservicen forudsætter, at Digitaliseringsstyrelsen sikrer forvaltning samt udvikling, drift og vedligeholdelse af bevisudstedelsesservicen.

Den foreslåede løsning indebærer således, at Digitaliseringsstyrelsen gives en eksklusiv rettighed, som omhandlet i § 17 i udbudsloven, til at tilrådighedsstille bevisudstedelsesservicen til offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde, som pålægges pligt til at anvende løsningen, når anvendelsen sker som led i myndighedsudøvelsen. Loven med tilhørende bekendtgørelser udgør i denne sammenhæng en ensidig administrativ retsakt, der alene opstiller betingelser for Digitaliseringsstyrelsen. Eftersom alle regler om tilrådighedsstillelse og anvendelse vil følge af loven, vil der ikke være tale om en gensidigt bebyrdende kontrakt, jf. udbudslovens § 24, nr. 24, og offentlige myndigheder og offentligretlige organer kan således anskaffe bevisudstedelsesservicen fra Digitaliseringsstyrelsen i medfør af loven, uden at skulle gennemføre et udbud, jf. også præambelbetragtning nr. 5 og 34 i Europa-Parlamentets og Rådets direktiv nr. 2014/24 af 26. februar 2014 om offentlige udbud og om ophævelse af direktiv 2004/18/EF (herefter udbudsdirektivet).

Anskaffelsespligten for offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde giver Digitaliseringsstyrelsen en eksklusiv rettighed, og har til formål at sikre den offentlige orden og sikkerhed, herunder hensynet til de samfundsøkonomiske overvejelser om fælles anskaffelse af it-løsninger i det offentlige.

Pligten til at anskaffe bevisudstedelsesservicen vil dog ikke gælde, hvis bevisudstedelsesservicen ikke kan imødekomme den offentlige myndigheds eller det offentligretlige organs særlige behov. Det er hensigten, at offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde kun anvender undtagelsen til anskaffelsespligten, når der er et sagligt og proportionalt grundlag for, at bevisudstedelsesservicen ikke kan anvendes ud fra en betragtning om særlige behov. Det vil f.eks. være tilfældet, hvis omkostningerne forbundet med tilpasning af den offentlige myndigheds eller det offentligretlige organs it-systemer klart overstiger behovet for anvendelse af bevisudstedelsesservicen til at gennemføre udstedelse af beviser. Et andet eksempel på særlige behov kan være, hvis en offentlig myndighed har unikke sikkerhedskrav, der ikke kan opfyldes af Digitaliseringsstyrelsens løsning som f.eks. særlige signeringskrav. I disse tilfælde vil den offentlige myndighed eller det offentligretlige organ i stedet have mulighed for at få udstedt digitale beviser på anden vis, og har i dette tilfælde selv ansvaret for udstedelsen af disse beviser, der oprettes på anden vis end via Digitaliseringsstyrelsens bevisudstedelsesservice.

En offentlig myndigheds eller et offentligretligt organs egen

bevisudstedelse skal opfylde de krav, der fastsættes i medfør af bemyndigelsen i den foreslåede § 7, stk. 2.

2.2.3. Modtagerpartregisteret

Modtagerpartregisteret er ikke identisk med det modtagerpartregister, der reguleres af eIDAS2, idet lovforslaget udelukkende har til formål at regulere modtagerpartregisteret i den rent nationale digitale identitetstegnebog.

Modtagerpartregisteret har til formål at sikre at modtagerpartarter, der ønsker at modtage beviser, der indeholder personoplysninger, er registreret med navn og kontaktinformationer samt CVR-nummer eller tilsvarende registrering i et andet EU-/EØS-land. Formålet med modtagerpartregisteret er således, at en bruger ved, hvilken modtagerpart, som brugeren interagerer med. Det er ikke alle modtagerpartarter, der er forpligtet til at oprette sig i modtagerpartregisteret. Dette beror på en afvejning af de byrder, der er forbundet med registrering sammenholdt med brugerens behov for at kunne identificere modtagerparten, jf. de almindelige bemærkninger i pkt. 3.2. om forholdet til databeskyttelsesforordningen og databeskyttelsesretten.

Ved registrering i modtagerpartregisteret sikres en entydig identifikation af modtagerparten. Når en registreret modtagerpart anmoder om at modtage et bevis fra en brugers tegnebogsapplikation, identificerer modtagerparten sig over for tegnebogsapplikationen. Tegnebogsapplikationen sikrer, at modtagerparten autentificerer sig korrekt.

3. Forholdet til databeskyttelsesforordningen og databeskyttelsesretten

Den nationale digitale identitetstegnebog består af tre tekniske løsninger, der samlet sikrer, at identitetstegnebogen er funktionsdygtig. De tre it-løsninger udgøres af en tegnebogsapplikation, en bevisudstedelsesservice og et modtagerpartregister. De tre løsninger er integreret til hinanden, men kan udvikles, driftes og vedligeholdelse separat.

Som anført i de almindelige bemærkninger i pkt. 1, etableres den nationale digitale identitetstegnebog som første trin på vej til den europæiske digitale identitetstegnebog. Den nationale digitale identitetstegnebog sikrer bl.a., at der opnås erfaringer med de tekniske løsninger samt introducerer identitetstegnebogskonceptet for brugere og modtagerpartarter, inden den europæiske digitale identitetstegnebog udvikles og idriftsættes i overensstemmelse med eIDAS2.

Identitetstegnebogskonceptet har brugeren i centrum, og bygges op om brugerens enekontrol i forhold til hvor, og over for hvem tegnebogsapplikationen anvendes. Enekontrollen indebærer således, at kun brugeren har det samlede overblik over, hvilke beviser der er udstedt til tegnebogsapplikationen, og hvor brugerens tegnebogsapplikation har været anvendt. Hensynet til brugerens enekontrol er varetaget ved, at de tre tekniske løsninger er adskilt med klare sikkerhedsmæssige og funktionelle grænser, som sikrer databeskyttelse og integritet.

I pkt. 3.2. beskrives de enkelte løsninger, herunder hvordan de udvikles, således at databeskyttelse gennem design sikrer, at hensynet til brugerens enekontrol varetages.

3.1. Gældende ret

Behandling af personoplysninger er omfattet af Europa-Parlamentets og Rådets forordning nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen) og lovbekendtgørelse nr. 289 af 8. marts 2024 om supplerende bestemmelser til forordningen om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

Databeskyttelsesforordningen og databeskyttelsesloven gælder for behandling af personoplysninger, der helt eller delvist foretages ved hjælp af automatisk (elektronisk) databehandling, og for anden ikke-automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

I databeskyttelsesforordningens kapitel II findes de relevante bestemmelser om, hvornår personoplysninger må behandles, herunder indsamles, udveksles og viderebehandles.

Behandling af personoplysninger er lovlig, hvis én af betingelserne i databeskyttelsesforordningens artikel 6, stk. 1, litra a-f, er opfyldt, herunder hvis behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige (litra c), eller hvis behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt (litra e). Behandling i medfør af databeskyttelsesforordningens artikel 6, stk. 1, litra c og e, skal have et såkaldt supplerende retsgrundlag. Dette følger af forordningens artikel 6, stk. 3.

Behandling af følsomme oplysninger er som udgangspunkt forbudt, jf. databeskyttelsesforordningens artikel 9, stk. 1. Dette forbud finder dog ikke anvendelse, bl.a. hvis behandling er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale ret og står i rimeligt forhold til det mål der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.

Det forudsættes med den foreslåede ordning, at Digitaliseringsstyrelsen som myndighedsopgave pålægges at tilvejebringe den nationale digitale identitetstegnebog. Som led heri har Digitaliseringsstyrelsen en opgave i teknisk at facilitere, at en bruger kan oprette sig i tegnebogsapplikationen. Det falder således inden for rammerne af myndighedsudøvelse at behandle de almindelige personoplysninger, der er nødvendige for at oprette en bruger og gøre tegnebogsapplikationen operationel.

Det forudsættes med den foreslåede ordning, at Digitaliseringsstyrelsen som myndighedsopgave pålægges at facilitere, at modtagerparter kan registrere sig i modtagerpartregisteret. Hvis en modtagerpart er en enkeltmandsvirksomhed, vil der i modtagerpartregisteret blive behandlet almindelige personoplysninger om indehaveren af enkeltmandsvirksomheden.

Ifølge databeskyttelsesforordningens artikel 6, stk. 2 og 3, er det muligt at implementere mere specifikke bestemmelser, der tilpasser anvendelsen af artikel 6, stk. 1, litra c, og artikel 6, stk. 1, litra e. De foreslåede bestemmelser i §§ 3, 5 og 14, stk. 3, udgør således supplerende retsgrundlag til databeskyttelsesforordningens artikel 6, stk. 1, litra e. Det vurderes, at de foreslåede bestemmelser er proportionale i forhold til de legitime mål og respekterer det væsentligste indhold af retten til databeskyttelse, da behandlingen er betinget af nødvendighed, jf. ovenfor.

Det forudsættes endvidere med den foreslåede ordning, at Digitaliseringsstyrelsen som myndighedsopgave også pålægges at kunne udstede beviser på vegne af andre offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde. Som led i denne myndighedsudøvelse vil det være nødvendigt, at Digitaliseringsstyrelsen kan behandle videregivne personoplysninger fra de offentlige myndigheders og offentligretlige organers autentiske kilder for at kunne danne og udstede beviser. Disse personoplysninger kan være følsomme personoplysninger, der omfattes af databeskyttelsesforordningens art. 9, stk. 1, herunder helbredsoplysninger. Det er ikke muligt at oplyste hvilke følsomme personoplysninger, der kan blive behandlet, da dette afhænger af, hvilke personoplysninger der indgår i et bevis. Det er Digitaliseringsministeriets vurdering, at behandling af de særlige kategorier af personoplysninger i sådanne tilfælde vil være nødvendig af hensyn til væsentlige samfundsinteresser, som angivet i databeskyttelsesforordningens art. 9, stk. 2, litra g.

Digitaliseringsministeriet skal afslutningsvist bemærke, at det forudsættes, at de øvrige bestemmelser i databeskyttelsesforordningen og databeskyttelsesloven, herunder de grundlæggende principper i databeskyttelsesforordningens artikel 5 også iagttages, når der behandles personoplysninger i medfør af de foreslåede bestemmelser.

3.2. Digitaliseringsministeriets overvejelser og den foreslåede ordning

Tegnebogsapplikationen er den løsning, som brugeren er i direkte kontakt med. Tegnebogsapplikationen er teknisk understøttet af en bagvedliggende infrastruktur, der sikrer, at tegnebogsapplikationen kan interagere med bevisudstedelsesservicen, modtagerpartregisteret og modtagerparter.

Ved første anvendelse efter download af tegnebogsapplikationen skal brugeren oprette sig ved anvendelse af MitID eller andet eID. På baggrund af denne autentifikation dannes et bevis i den bagvedliggende tekniske infrastruktur, der dan-

ner grundlag for en digital bekræftelse af, at den oprettede tegnebogsapplikation er en ægte og gyldig tegnebogsapplikation.

Det er ikke muligt at oprette en aktiv tegnebogsapplikation uden, at der som minimum dannes bevis for identitet eller bevis for navn og fødselsdato. Hvilket bevis, der dannes, afhænger af om brugeren har et CPR-nummer eller ikke har et CPR-nummer. Beviset er nødvendigt for, at tegnebogsapplikationen kan aktiveres. Nyt login med et MitID eller andet eID er påkrævet, idet der ikke må udveksles oplysninger om brugerens login i tegnebogsapplikationen mellem tegnebogsapplikationens bagvedliggende infrastruktur og bevisudstedelsesservicen.

På baggrund af en anmodning om udstedelse af bevis fra en bruger med CPR-nummer, sker der en forespørgsel fra bevisudstedelsesservicen til Datafordeleren, der på baggrund af modtagne oplysninger om brugeren returnerer data, der formateres i bevisudstedelsesservicen og overføres til tegnebogsapplikationen. Herefter er brugerens oprettelse i tegnebogsapplikationen fuldført. For brugere uden CPR-nummer dannes bevis for navn og fødselsdato på baggrund af data fra autentifikationssvaret fra NemLog-in.

Brugeren kan vælge at tilføje sit foto til sin tegnebogsapplikation enten under oprettelsen eller på et senere tidspunkt. Dette sker ved brugerens scanning af sit pas. Fotoet fra passet behandles herefter i tegnebogsapplikationens bagvedliggende infrastruktur og lagres på brugerens enhed.

Efter tilføjelse af foto vil bevis for brugerens identitet, der forudsætter, at brugeren har et CPR-nummer, udgøre legitimationsbevis, der kan tjene samme formål som legitimationskortet udstedt i medfør af lov om udstedelse af legitimationskort, jf. den foreslåede bestemmelse i § 3, stk. 2, og de specielle bemærkninger hertil.

Tilføjelse af foto til tegnebogsapplikationen for brugere uden CPR-nummer, vil ikke medføre, at bevis for navn og fødselsdato sammen med fotoet, kan tjene samme formål som legitimationskortet udstedt i medfør af lov om udstedelse af legitimationskort jf. den foreslåede § 3, stk. 2, modsætningsvist.

Brugeren har enekontrol over indholdet i sin tegnebogsapplikation, og kan dele beviser til en modtagerpart eller en anden bruger, eller slette beviser i sin tegnebogsapplikation, ligesom brugeren kan vælge at spærre sin tegnebogsapplikation. Det bemærkes i den forbindelse, at såfremt brugeren sletter bevis for identitet eller bevis for navn og fødselsdato, kan tegnebogsapplikationen ikke fungere, uagtet at øvrige beviser ikke slettes af brugeren.

Bevisudstedelsesservicen er en service, som Digitaliseringsstyrelsen stiller til rådighed for offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde, når de som led i deres myndighedsudøvelse vælger at levere data fra deres autentiske kilde for at få udstedt beviser til en brugers tegnebogsapplikation. En bruger har således ikke

retskrav på at få udstedt beviser til sin digitale tegnebogsapplikation, ligesom brugeren heller ikke, i medfør af den foreslåede lov, kan blive mødt med krav fra en modtagerpart om at overføre et bevis fra sin digitale tegnebogsapplikation til en modtagerpart. Den frivillige brug af den nationale digitale identitetstegnebog gør sig således gældende hos hver af de enkelte aktører.

Bevisudstedelsesservicen kan alene anvendes af offentlige myndigheder og offentligretlige organer og ikke private juridiske enheder.

Digitaliseringsstyrelsen agerer selvstændigt i rollen som tilrådighedsstiller af bevisudstedelsesservicen, idet Digitaliseringsstyrelsen afgør til hvilket formål og med hvilke hjælpemidler, der udstedes beviser, herunder hvilke krav, der skal opfyldes af en autentisk kilde, for at dennes videregivelse af oplysninger kan danne et bevis. Digitaliseringsstyrelsen er dataansvarlig for behandling af personoplysninger i bevisudstedelsesservicen, samt for behandling af personoplysninger i forbindelse med transmission og levering af et udstedt bevis, indtil beviset er leveret til brugerens tegnebogsapplikation. Bevisudstedelsesservicen gemmer ikke oplysninger om hvilke beviser der er udstedt til en given bruger, men et udstedt bevis får en mærkning, der ikke er personhenførbart, og som følger beviset. Denne mærkning kan en modtagerpart anvende til at kontrollere bevisets ægthed og gyldighed.

Bevisudstedelsesservicen foretager logning af transmissionskald til og fra en offentlig myndigheds eller et offentligretligt organs autentiske kilde, jf. de specielle bemærkninger til den foreslåede § 5, stk. 2, nr. 4. Logningen er anonymiseret og anvendes til fejlsøgning. Dette vil f.eks. være relevant, hvis en bruger henvender sig om manglende udstedelse af et bevis uagtet anmodning herom. Bevisudstedelsesservicen vil i et sådant tilfælde kunne spore, om der på en given dato har været gennemført transmissionskald til og fra en autentisk kilde. Indholdet af transmissionskald logges ikke.

Modtagerpartregisteret sikrer, at en bruger ved, hvem vedkommende interagerer med. Det er dog ikke alle modtagerpart, der kræves oprettet i modtagerpartregisteret.

I det fysiske møde mellem bruger og modtagerpart er brugeren bekendt med, hvilke fysiske omgivelser, som brugeren befinder sig i. F.eks. ved køb af aldersbegrænsede varer, hvor brugeren er bevidst om, at denne befinder sig i kiosk A eller supermarked B. Det vurderes derfor at være for byrdefuldt at kræve registrering i disse situationer, idet brugeren på anden vis let kan få viden om modtagerpartens identitet. Det er efter Digitaliseringsministeriets vurdering en rimelig afgrænsning, henset til de byrder, der er forbundet med registrering, sammenholdt med brugerens behov for kunne identificere modtagerparten.

Det bemærkes i den forbindelse, at personoplysninger, der overføres via internettet til modtagerparten uden at være omfattet af den foreslåede § 9, stk. 3, eller regler, der måtte

blive fastsat i medfør af den foreslåede bestemmelse i § 9, stk. 4, altid kræver registrering af modtagerparten i modtagerpartregisteret, uanset om overførsel af beviser sker i fysisk møde eller online uden fysisk nærvær mellem bruger og modtagerpart. Dette beror på, at brugerens oplysninger i disse tilfælde kan blive yderligere behandlet, uden at det er synligt for brugeren. Et eksempel herpå kan være en virksomhed, der efterfølgende over for en myndighed skal kunne dokumentere, at virksomheden har indhentet et givent bevis hos en kunde. Registrering i modtagerpartregisteret betyder, at brugeren inden interaktion med modtagerparten får vished for, at modtagerparten er optaget i modtagerpartregisteret, og dermed er identificerbar.

Modtagerparten bliver selvstændigt dataansvarlig for modtagne beviser og skal herunder have fornøden behandlingshjemmel. Dette gælder også selvom, at modtagerparten ikke er omfattet af krav om registrering i modtagerpartregisteret.

Ved optagelse i modtagerpartregisteret dannes en entydig identifikation af modtagerparten. Når en registreret modtagerpart anmoder om at modtage et bevis fra en brugers tegnebogsapplikation, identificerer modtagerparten sig over for tegnebogsapplikationen. Tegnebogsapplikationen sikrer, at modtagerparten autentificerer sig korrekt.

I lovforslagets foreslåede § 14 fastlægges dataansvar for de enkelte aktører i den nationale digitale identitetstegnebog. Digitaliseringsministeriet har fundet det hensigtsmæssigt at indføre den foreslåede bestemmelse af hensyn til at sikre gennemsigtighed i forhold til de aktører, der berøres af bestemmelsen.

4. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Der pålægges ikke økonomiske konsekvenser for det offentlige, herunder kommuner og regioner. Det foreslåede lovforslag medfører ingen direkte pligter for det offentlige, men medfører alene en frivillig mulighed for at få udstedt beviser til en brugers tegnebogsapplikation gennem bevisudstedelsesservicen, jf. den foreslåede lovs kapitel 3. Hvis en offentlig myndighed eller et offentligretligt organ ønsker at få udstedt et bevis til en brugers tegnebogsapplikation, følger der som udgangspunkt en pligt til at anvende bevisudstedelsesservicen, der er reguleret i den foreslåede lovs kapitel 3. Digitaliseringsstyrelsen pålægges ved lovforslaget at varetage myndighedsopgaven at forvalte, udvikle, drifte og vedligeholde bevisudstedelsesservicen. Digitaliseringsstyrelsen afholder udgifterne til forvaltning, udvikling, drift og vedligeholdelse af bevisudstedelsesservicen, herunder omkostningerne i forbindelse med omdannelse af data fra myndighedens autentiske kilde til data, som er kompatibel med kravene til et bevis i den nationale digitale identitetstegnebog.

Det vurderes, at lovforslaget ikke har implementeringskonsekvenser for det offentlige, herunder kommuner og regioner.

4.1. Syv principper for digitaliseringsklar lovgivning

Lovforslaget vurderes at leve op til de syv principper for digitaliseringsklar lovgivning, og har været i høring i Digitaliseringsstyrelsens sekretariat for Digitaliseringsklar lovgivning. Særligt lever lovforslaget op til princip 4 om sammenhæng på tværs og genbrug af data, princip 5 om tryk og sikker datahåndtering og princip 6 om anvendelse af offentlig infrastruktur. Lovforslaget er udformet i overensstemmelse med princip 4 om sammenhæng på tværs, eftersom de data og de oplysninger, som lægges til grund for beviser, der udstedes i den nationale digitale identitetstegnebog, er baseret på offentlige myndigheders egne autentiske kilder om fysiske personer. Princippet ses efterlevet ved, at der trækkes på eksisterende datakilder, herunder CPR-registeret.

Angående princip 5 om tryk og sikker datahåndtering er den nationale digitale identitetstegnebog udviklet med udgangspunkt i princippet om databeskyttelse gennem design. Den nationale digitale identitetstegnebog er derfor en løsning med særlig fokus på at beskytte privatlivets fred, og sikrer, at der ikke udveksles unødigt information samtidig med, at brugeren er i kontrol med løsningen. Løsningen behandler data, der på brugerens instruks udstedes til tegnebogsapplikationen, og data opbevares herefter alene i brugerens egen tegnebogsapplikation. Brugeren vælger selv, om og hvornår brugeren vil frigive data fra tegnebogsapplikationen. Brugeren vil således i den nationale digitale identitetstegnebog have enekontrol over egne data i tegnebogsapplikationen.

Særligt for princip 6 om anvendelse af offentlig infrastruktur kan anføres, at oprettelsen af en bruger i tegnebogsapplikationen er baseret på et MitID eller andet eID. Oprettelse af en bruger i tegnebogsapplikationen ved et MitID eller andet eID er hensigtsmæssig at anvende, da der både sikres en meget høj grad af sikkerhed og genbrug af løsninger på tværs. Ydermere kan anføres, at data til brug for dannelse af bevis for identitet eller bevis for navn og fødselsdato, som er en forudsætning for at have en operationel tegnebogsapplikation, er baseret på data hentet fra hhv. Datafordeleren og NemLog-in. Der henvises i øvrigt til de almindelige bemærkninger pkt. 3. om forholdet til databeskyttelsesforordningen og databeskyttelsesretten.

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

Det er hensigten med lovforslaget, at erhvervsdrivende kan blive modtagerparter for modtagelse af beviser i den nationale digitale identitetstegnebog, jf. den foreslåede bestemmelse i § 2, nr. 5, jf. § 9. Den nationale digitale identitetstegnebog vil kunne anvendes som aldersverifikation, og vil derfor kunne understøtte regeringens arbejde med at begrænse børn og unges forbrug og påbegyndelse af forbrug af tobak, nikotin og alkohol. Modtagelse af den nationale digitale identitetstegnebog er dog en frivillig mulighed for erhvervslivet. Det er alene efter den foreslåede bestemmelse i § 9, stk. 2, at den erhvervsdrivende skal registreres i modtagerpartregisteret. Det er denne registrering, som vil

udgøre en mindre administrativ konsekvens i form af øget tidsforbrug. De nærmere regler om registrering i modtagerpartregisteret vil blive udmøntet i en bekendtgørelse, jf. den foreslåede bestemmelse i § 10. Det forventes alene at være en mindre andel af de erhvervsdrivende, som vil have behov for at registrere sig i modtagerpartregisteret. Det vurderes på denne baggrund, at de erhvervsøkonomiske og administrative konsekvenser vil ligge markant under bagatelgrænserne på hhv. 10 mio. kr. og 4 mio. kr., og de kvantificeres derfor ikke yderligere.

6. Administrative konsekvenser for borgerne

Lovforslaget medfører ingen administrative konsekvenser for borgerne.

7. Klimamæssige konsekvenser

Lovforslaget medfører ingen klimamæssige konsekvenser.

8. Miljø- og naturmæssige konsekvenser

Lovforslaget medfører ingen miljø- og naturmæssige konsekvenser.

9. Forholdet til EU-retten

Med Europa-Parlamentet 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) som ændret ved Europa-Parlamentets og Rådets Forordning (EU) 2024/1183 af 11. april 2024 (eIDAS2) forpligtes hver medlemsstat til at etablere en europæisk digital identitetstegnebog. Den europæiske digitale identitetstegnebog skal i fremtiden både være en fælleseuropæisk identifikationsløsning, rumme beviser og på sigt også betalingsmuligheder m.v.

I Danmark sker første trin af udviklingen af den europæiske digitale identitetstegnebog ved etablering af den nationale digitale identitetstegnebog, som reguleres ved denne lov, der således ikke udgør en supplerende lov til eIDAS2. Det står klart, at det er en teknisk kompliceret opgave at få alle elementer i den europæiske digitale identitetstegnebog til

at virke sammen. EU-Kommissionen er således ved at udarbejde retsakter, der supplerer og konkretiserer forordningsteksten. Dertil kommer krav til certificering af identitetstegnebogen og tilsynsopgaver med såvel identitetstegnebogen som med de virksomheder og myndigheder, der i forordningen bliver forpligtet til at modtage tegnebogen. Endvidere har en bruger af identitetstegnebogen en lang række rettigheder, som teknisk skal indbygges i identitetstegnebogen, således at brugerens retssikkerhed tilgodeses i selve tegnebogsløsningen.

I forlængelse af ovenstående vurderes lovforslaget ikke at indeholde EU-retlige aspekter.

10. Hørte myndigheder og organisationer m.v.

Et udkast til lovforslag har i perioden fra den 14. maj 2025 til den 17. juni 2025 (31 dage) været sendt i høring hos følgende myndigheder og organisationer m.v.:

ATP, Advokatsamfundet, AE – Arbejderbevægelsens Erhvervsråd, BL – Danmarks almene boliger, Børns Vilkår, Cybersikkerhedsrådet, Danmarks Statistik, Danmarks Nationalbank, Dansk IT, Danske Advokater, Danske A-Kasser, DI Digital, Digital Lead, DKCERT, Erhvervshus Fyn, Erhvervshus Hovedstaden, Erhvervshus Midtjylland, Erhvervshus Nordjylland, Erhvervshus Sjælland, Erhvervshus Sydjylland, Finans Danmark, Finanstilsynet, Fonden Dansk Standard, Forbrugerrådet Tænk, Foreningen Danske Revisorer, FSR – danske revisorer, Forsikring og Pension, GTS-foreningen, Green Power Denmark, Dataetisk Råd, Danske Handicaporganisationer, Dansk Arbejdsgiverforening, Dansk Erhverv, Dansk Industri, Danske Regioner, Danske Universiteter, Datatilsynet, Den Danske Dommerforening, Det Centrale Handicapråd, Fagbevægelsens Hovedorganisation, Institut for Menneskerettigheder, IT-Branchen, IT-Politisk Forening, KL – Kommunernes Landsforening, KOMBIT, Konkurrence- og Forbrugerstyrelsen, Landbrug & Fødevarer, LOS – Landsorganisationen for sociale tilbud, MADE, Red Barnet, Rådet for Digital Sikkerhed, Rådet for Socialt Udsatte, Rigsrevisionen, SMVDanmark, TEKNIQ, Teleindustrien og Ældre Sagen.

11. Sammenfattende skema

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang/hvis nej, anfør »Ingen«)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang/hvis nej, anfør »Ingen«)
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Implementeringskonsekvenser for stat, kommuner og regioner	Ingen	Ingen
Økonomiske konsekvenser for erhvervslivet m.v.	Ingen	Det vurderes, at der vil være økonomiske konsekvenser forbundet med lovforslaget. Konsekvenserne vurderes at være under 10 mio. kr.

Administrative konsekvenser for erhvervslivet m.v.	Ingen	Det vurderes, at der vil være administrative konsekvenser forbundet med lovforslaget. Konsekvenserne vurderes at være under 4 mio. kr.
Administrative konsekvenser for borgerne	Ingen	Ingen
Klimamæssige konsekvenser	Ingen	Ingen
Miljø- og naturmæssige konsekvenser	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget indeholder ingen EU-retlige aspekter.	
Er i strid med de fem principper for implementering af erhvervsrettet EU-regulering (der i relevant omfang også gælder ved implementering af ikke-erhvervsrettet EU-regulering) (sæt X)	Ja	Nej X

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Der findes ikke i gældende ret regler, der regulerer den nationale digitale identitetstegnebog, idet løsningen er ny. Der findes dog adskillige decentrale offentlige applikationsløsninger, jf. pkt. 2.1. i de almindelige bemærkninger.

Det foreslås i § 1, at loven har til formål at understøtte den nationale digitale identitetstegnebog, der består af de tekniske løsninger tegnebogsapplikation, bevisudstedelsesservice og modtagerpartregister.

Den foreslåede bestemmelse vil medføre, at lovforslaget har til formål at understøtte den nationale digitale løsning, »den nationale digitale identitetstegnebog«.

Ved »nationale digitale identitetstegnebog« i den foreslåede bestemmelse forstås, en it-infrastruktur der består af de tre tekniske løsninger: en tegnebogsapplikation, en bevisudstedelsesservice og et modtagerpartregister. De tre løsninger, som tilsammen udgør den nationale digitale identitetstegnebog, er defineret i den foreslåede § 2.

Idet lovforslaget alene regulerer en national digital identitetstegnebog, falder det uden for lovens formål at fastsætte supplerende regulering af en europæisk digital identitetstegnebog, som er reguleret ved eIDAS2.

Ved »tegnebogsapplikation« i den foreslåede bestemmelse forstås en teknisk løsning i den nationale digitale identitetstegnebog bestående af Digitaliseringsstyrelsens mobilapplikation, som gør det muligt for brugeren at lagre, forvalte og validere beviser med henblik på at overføre dem til modtagerparter eller andre brugere, jf. den foreslåede § 2, nr. 9.

Ved »bevisudstedelsesservice« i den foreslåede bestemmelse forstås en teknisk løsning i den nationale digitale identitetstegnebog, hvor Digitaliseringsstyrelsen på vegne af en offentlig myndighed eller et offentligretligt organ med ansvar

for en autentisk kilde kan udstede beviser, jf. den foreslåede § 2, nr. 3.

Ved »modtagerpartregister« i den foreslåede bestemmelse forstås en teknisk løsning i den nationale digitale identitetstegnebog bestående af et register, hvor modtagerparter registrerer sig, jf. den foreslåede § 2, nr. 6.

Lovforslagets formål afgrænses efter den foreslåede bestemmelse til de tre tekniske løsninger i den nationale digitale identitetstegnebog. Lovforslaget opdeler reguleringen af den nationale digitale identitetstegnebog i tre tekniske løsninger, idet der til hver løsning er forskellige rettigheds- og pligtsubjekter. Den tekniske løsning »tegnebogsapplikation« kan anvendes af fysiske personer. Den tekniske løsning »bevisudstedelsesservice« anvendes af offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde, der får udstedt beviser som led i myndighedsudøvelse. Den tekniske løsning »modtagerpartregister« kan anvendes af juridiske enheder, der ønsker at modtage beviser. Formålet med den foreslåede bestemmelse i § 1, er at sikre gennemsigtighed og tydelighed i forhold til lovens foreslåede rettigheds- og pligtbestemmelser, der skal gælde for den nationale digitale identitetstegnebog.

Til § 2

De foreslåede definitioner i § 2, nr. 1-9, indeholder begreber, der for visse af definitionerne allerede eksisterer i gældende ret.

Det foreslås i § 2, nr. 1 - 9, at der med lovforslaget introduceres en række definitioner, som nærmere angivet i de enkelte numre. Med den foreslåede bestemmelse defineres de væsentligste begreber, som anvendes i loven.

Det foreslås i § 2, nr. 1, at autentisk kilde defineres som et register eller et system, som en offentlig myndighed eller et offentligretligt organ har ansvaret for, der indeholder og kan levere attributter om en fysisk person eller genstand, og som anses for at være en primær kilde til disse oplysninger eller

er anerkendt som autentisk i overensstemmelse med dansk ret, herunder administrativ praksis.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 1, vil medføre, at det tekniske begreb »autentisk kilde« defineres. Definitionen svarer i tilpasset form til definitionen af autentisk kilde i eIDAS2 art. 3, nr. 47. Da en privat enhed ikke kan udstede beviser i medfør af den foreslåede lov, og en bruger kun kan være en fysisk person, er definitionen dog tilpasset i forhold hertil.

Forståelsen af begrebet »autentisk kilde« er central for lovforslaget, idet en autentisk kilde udgør den primære kilde til de attributter, som et bevis består af, når det udstedes til tegnebogsapplikationen. En autentisk kilde leverer således de attributter, som lægges til grund i et bevis, hvorved attributterne udgør indholdet af et bevis, der samtidig fastsætter bevisets indhold og dermed bevisværdi, i form af f.eks. rettigheder eller tilladelser.

Det er afgørende, at de oplysninger, som indgår i et bevis, er korrekte. Det er derfor kun oplysninger, der kommer fra en autentisk kilde, der kan indgå i et bevis. En offentlig myndighed eller et offentligretligt organ skal anvende egne autentiske kilder. En autentisk kilde kan dog indeholde oplysninger fra en anden autentisk kilde. F.eks. anvender stort set alle myndigheder CPR-nummer som entydig personidentifikation. CPR-registeret er en autentisk kilde til CPR-numre.

Det er den enkelte offentlige myndighed og offentligretlige organ, der har ansvaret for indholdet i deres egne autentiske kilder. De autentiske kilder indeholder oplysninger om en fysisk person eller genstand. Disse oplysninger lægges til grund som attributter i beviser, der udstedes til en brugers tegnebogsapplikation.

Det foreslås i § 2, nr. 2, at bevis defineres som en elektronisk attestering af attributter, der er udstedt af eller på vegne af en offentlig myndighed eller et offentligretligt organ med ansvar for en autentisk kilde.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 2, vil medføre, at begrebet »bevis« defineres. Forståelsen af begrebet »bevis« er centralt for den nationale digitale identitetstegnebog.

Begrebet »bevis« forstås, som en elektronisk attestering af attributter. Et bevis består således af attributter, leveret fra en autentisk kilde, som en offentlig myndighed eller et offentligretligt organ har ansvaret for, jf. den foreslåede bestemmelse i nr. 1, der definerer autentisk kilde. Bevisets indhold og bevisværdi afhænger derfor af de attributter, der leveres fra en offentlig myndigheds eller et offentligretligt organs autentiske kilde.

Begrebet attribut anvendes om en fysisk persons eller en genstands egenskab, kvalitet, rettigheder eller tilladelser.

Det foreslås i § 2, nr. 3, at bevisudstedelsesservice defineres

som en teknisk løsning i den nationale digitale identitetstegnebog, hvor Digitaliseringsstyrelsen på vegne af en offentlig myndighed eller et offentligretligt organ med ansvar for en autentisk kilde kan udstede beviser.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 3, vil medføre, at begrebet »bevisudstedelsesservice« defineres. Bevisudstedelsesservicen indgår som en teknisk løsning i den nationale digitale identitetstegnebog. Det er bevisudstedelsesservicen, der muliggør, at offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde, som led i deres myndighedsudøvelse kan få udstedt beviser til en brugers tegnebogsapplikation. De foreslåede bestemmelser i lovforslagets kapitel 3, indeholder nærmere regler om bevisudstedelsesservicen.

Det foreslås i § 2, nr. 4, at bruger defineres som en fysisk person, der anvender tegnebogsapplikationen.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 4, vil medføre, at begrebet »bruger« defineres. Begrebet er centralt for forståelsen af tegnebogsapplikationen, som kun kan anvendes af fysiske personer, der efter oprettelsen i tegnebogsapplikationen betegnes som brugere i denne lovs forstand.

Det foreslås i § 2, nr. 5, at modtagerpart defineres som en juridisk enhed med et CVR-nummer eller en juridisk enhed registreret i et register i et andet EU-/EØS-land svarende til Det Centrale Virksomhedsregister, der kan modtage beviser fra en brugers tegnebogsapplikation.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 5, vil medføre, at begrebet »modtagerpart« defineres.

Den foreslåede bestemmelse i § 2, nr. 5, vil tillige medføre, at en juridisk enhed skal have et CVR-nummer eller være registreret i et register i et andet EU-/EØS-land svarende til Det Centrale Virksomhedsregister, for at kunne modtage beviser fra en brugers tegnebogsapplikation.

Juridiske enheder i EU-/EØS-lande kan f.eks. være kapitalelskaber og offentlige myndigheder. For at et register kan anses som svarende til det Det Centrale Virksomhedsregister, skal det pågældende register være autoritativt. Ved autoritativt register skal i denne sammenhæng forstås, at registeret udgør en officiel og anerkendt kilde for registrering af juridiske enheder i det pågældende EU-/EØS-land.

Den foreslåede definition af en juridisk enhed skal sikre overensstemmelse med reglerne om den frie bevægelighed for tjenesteydelser, som fastlagt i Traktaten om Den Europæiske Unions Funktionsmåde (TEUF) og servicedirektivet.

Med bestemmelsen skabes der hjemmel til, at juridiske enheder uden CVR-nummer kan blive modtagerparter, der omfattes af kravet om registrering i modtagerpartregisteret, jf. den foreslåede § 9, såfremt de er registreret i et register i et andet EU-/EØS-land svarende til Det Centrale Virksomhedsregister. Dette vil betyde, at sådanne juridiske enheder,

der ønsker at modtage beviser fra en brugers tegnebogsapplikation, der kræver registrering i modtagerpartregisteret, får mulighed herfor.

Det foreslås i § 2, nr. 6, at modtagerpartregister defineres som en teknisk løsning i den nationale digitale identitetstegnebog bestående af et offentligt register, hvor en modtagerpart registrerer sig.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 6, vil medføre, at begrebet »modtagerpartregister« defineres. Modtagerpartregisteret indgår som en teknisk løsning i den nationale digitale identitetstegnebog. En modtagerpart skal være registreret i modtagerpartregisteret, når en modtagerpart for at modtage beviser anvender en teknologi, hvor beviser overføres via internettet, medmindre der alene er tale om bevis for, om en bruger er over eller under en given aldersgrænse, jf. de foreslåede bestemmelser i § 9, stk. 2 og 3. De foreslåede bestemmelser i lovforslagets kapitel 5, indeholder nærmere regler om modtagerpartregisteret.

Det foreslås i § 2, nr. 7, at offentlig myndighed defineres som statslige, regionale og kommunale myndigheder eller sammenslutninger heraf.

Den gældende bestemmelse i § 24, nr. 28, i udbudsloven, medfører, at der ved ordregiver forstås statslige, regionale og kommunale myndigheder. I udbudslovens forstand udgør statslige myndigheder de ordregivere, der er listet i udbudsdirektivets bilag I, dvs. Folketinget, Rigsrevisionen, Domstolsstyrelsen, samt alle ministerier med underliggende styrelser og institutioner. Regionale myndigheder er myndigheder, der er opført i NUTS 1 og 2, som omhandlet i EP/Rfo 1059/2003, dvs. i Danmark de nuværende 5 regioner, som fastsat i regionslovens § 1. Kommunale myndigheder omfatter efter lovbemærkningerne til udbudsloven alle myndigheder i de administrative enheder, der falder ind under NUTS 3, samt mindre administrative enheder som omhandlet i EU/Rfo 1059/2003. I Danmark omfatter dette kommunerne.

Den foreslåede bestemmelse i § 2, nr. 7, skal forstås i overensstemmelse med udbudslovens definition af offentlige myndigheder i rollen som ordregivere, jf. § 24, nr. 28, i udbudsloven og skal fortolkes i overensstemmelse med gældende udbudsretlig praksis.

Det foreslås i § 2, nr. 8, at offentligretlige organer defineres som organer,

- a. der er oprettet specielt med henblik på at imødekomme almenhedens behov, dog ikke behov af industriel eller kommerciel karakter,
- b. der er juridiske personer, og
- c. som for mere end halvdelen vedkommende finansieres af staten, regionale eller lokale myndigheder eller af andre offentligretlige organer eller er underlagt ledelsesmæssig kontrol af disse myndigheder eller organer eller har en bestyrelse eller direktion eller et tilsynsråd, hvor mere end halvdelen af medlemmerne udpeges af

staten, regionale eller kommunale myndigheder eller andre offentligretlige organer.

Den foreslåede bestemmelse i § 2, nr. 8, skal forstås i overensstemmelse med udbudslovens definition af offentligretlige organer, jf. § 24, nr. 27, i udbudsloven og skal fortolkes i overensstemmelse med gældende udbudsretlig praksis.

Den gældende bestemmelse i § 24, nr. 27, i udbudsloven, medfører, at der ved offentligretlige organer forstås organer, der er oprettet specielt med henblik på at imødekomme almenhedens behov, dog ikke behov af industriel eller kommerciel karakter, der er juridiske personer, og som for mere end halvdelen vedkommende finansieres af staten, regionale eller kommunale myndigheder eller af andre offentligretlige organer eller er underlagt ledelsesmæssig kontrol af disse myndigheder eller organer eller har en bestyrelse eller direktion eller et tilsynsråd, hvor mere end halvdelen af medlemmerne udpeges af staten, regionale eller kommunale myndigheder eller andre offentligretlige organer.

Med bestemmelsens § 24, nr. 27, i udbudsloven defineres begrebet »offentligretlige organer« som organer, der opfylder de tre betingelser i litra a-c.

I henhold til litra a skal det være organer, som er specielt oprettet med henblik på at imødekomme almenhedens behov af ikke-industriel eller ikke-kommerciel karakter.

I henhold til litra b skal det være organer, der er juridiske personer.

Endelig skal det i henhold til litra c være organer, som overvejende finansieres af staten, regionale eller kommunale myndigheder eller af andre offentligretlige organer, eller er underlagt ledelsesmæssig kontrol af disse myndigheder eller organer, eller har en bestyrelse, en direktion, eller et tilsynsråd, hvor mere end halvdelen af medlemmerne udpeges af staten, regionale eller kommunale myndigheder eller andre offentligretlige organer.

Alle tre betingelser skal være opfyldt for at en juridisk enhed kan defineres som et offentligretligt organ i overensstemmelse med udbudslovens § 24, nr. 27.

Det følger af bestemmelsen i udbudslovens § 24, nr. 27, at organet skal være oprettet specielt med henblik på at imødekomme almenhedens behov. Det vil almindeligvis være opgaver som generelt og traditionelt anses for at være opgaver, som det offentlige varetager. Dette kunne f.eks. være opgaver inden for dag- eller døgntilbud til børn og voksne, miljø, sundhed, uddannelse, beskæftigelsesindsats eller opgaver på socialområdet. Kravet om, at et organ skal være oprettet specielt med henblik på at imødekomme almenhedens behov er opfyldt, når organet faktisk udøver aktiviteter med henblik på imødekommelsen af sådanne behov. Et organ kan således blive omfattet af loven som et offentligretligt organ selv om organet ikke imødekommer sådan behov ved dets oprettelse, men på et senere tidspunkt.

I henhold til udbudsdirektivets præambelbetragtning nr. 10 er et organ, der fungerer på normale markedsvilkår, har til formål at skabe gevinst og bærer tab forbundet med udøvelsen af sine aktiviteter, ikke at betragte som et offentligretligt organ, da almenhedens behov, som det er oprettet med henblik på at imødekomme eller har fået til opgave at imødekomme, kan anses for at have industriel eller kommerciel karakter.

At organet skal være en juridisk person betyder, at det pågældende subjekt skal være i stand til at bære rettigheder og forpligtelser. Selskaber med et CVR-nummer vil være at betragte som en juridisk person. Interessentskaber vil også være omfattet.

Da kravet i litra c indebærer, at mere end halvdelen af driften skal være finansieret af offentlige midler, vil organet være omfattet. Finansieringen må dog ikke have karakter af at være en modydelse eller et gensidigt forretningsforhold. Det har ingen betydning, at mere end halvdelen af organets drift kommer fra kontrakter med offentlige myndigheder, altså at organet f.eks. har vundet en række udbud. Det er således kun de ydelser, der finansierer eller støtter det berørte organs aktiviteter ved et økonomisk bidrag uden en særlig kontraktuel præget modydelse, der vil udgøre offentlig finansiering.

At føre kontrol vil sige at være underlagt intensiv offentlig regulering, tilsyn eller lignende. En virksomhed, som er underlagt en offentlig myndigheds kontrol af regnskabsførelse vil ikke være underlagt offentlig kontrol. Det skyldes, at den offentlige myndighed ikke kan påvirke de beslutninger, som virksomheden træffer i forhold til driften af virksomheden. Det er altså ikke tilstrækkeligt, at der er tale om, at driften er underlagt offentlig kontrol, og at det offentlige har en almindelig efterfølgende kontrol af f.eks. regnskab og lignende.

Selvejende institutioner, der er oprettet på privatretligt grundlag, og som har driftsoverenskomst med en kommune, kan være underlagt et sådant kommunalt tilsyn, at de vil være omfattet af begrebet »offentligretligt organ«. Dette gælder, selvom kommunen ikke via ejerskab har mulighed for at udføre bestemmende indflydelse på institutionen. Kommunen skal dog have indflydelse på anden vis f.eks. via kontrol med institutionens vedtægter, budget, personaleforhold m.v.

Det betyder, at selvejende dagtilbud til børn (daginstitutioner, fritidsordninger, skoler), uddannelsesinstitutioner, plejehjem og anden ældreomsorg kan være omfattet af begrebet »offentligretligt organ«.

Ligeledes kan institutioner med tilbud til udsatte grupper (forsorgshjem, kvindekrisecentre, væresteder m.v.), som en kommune har driftsoverenskomst med, være omfattet af begrebet »offentligretligt organ«.

Statslige aktieselskaber, hvor ressortministeren kan vælge flertallet af bestyrelsesmedlemmerne, er også omfattet og vil være at betragte som et offentligretligt organ.

Som eksempler på offentligretlige organer kan nævnes TV2, Sund og Bælt Holding A/S, Metroselskabet I/S, Statens og Kommunernes Indkøbsservice (SKI), Lønmodtagernes Dyr-tidsfond, Naviair, de almene boligorganisationer og universiteterne.

Det foreslås i § 2, nr. 9, at tegnebogsapplikation defineres som en teknisk løsning i den nationale digitale identitetstegnebog stillet til rådighed af Digitaliseringsstyrelsen gennem en mobilapplikation, som gør det muligt for en bruger at lagre, forvalte, validere og dele beviser med henblik på at overføre dem til modtagerparter og andre brugere.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 9, vil medføre, at begrebet »tegnebogsapplikation« defineres. Tegnebogsapplikationen indgår som en teknisk løsning i den nationale digitale identitetstegnebog. Definitionen er ikke til hinder for visuel inspektion af beviser fra tegnebogen. Det er tegnebogsapplikationen, der muliggør, at en bruger kan anvende de beviser, som brugeren vælger at få udstedt til tegnebogsapplikationen. De foreslåede bestemmelser i lovforslagets kapitel 2 indeholder nærmere regler om tegnebogsapplikationen.

Til § 3

Der findes ikke i gældende ret regler, der regulerer tegnebogsapplikationen, idet denne er en del af den nye nationale digitale identitetstegnebog.

Det foreslås i § 3, stk. 1, at Digitaliseringsstyrelsen stiller en tegnebogsapplikation til rådighed for fysiske personer. Digitaliseringsstyrelsen sikrer forvaltning, udvikling, drift og vedligeholdelse af tegnebogsapplikationen.

Den foreslåede bestemmelse vil medføre, at tegnebogsapplikationen kan anvendes af fysiske personer. Det er frivilligt for en fysisk person at anvende tegnebogsapplikationen. Når en fysisk person vælger at anvende tegnebogsapplikationen, og dermed anses som bruger, har brugeren enekontrol over denne, hvilket indebærer, at brugeren selv vælger, hvilke beviser der skal udstedes til tegnebogsapplikationen, og hvornår brugeren ønsker at anvende disse.

Med den foreslåede bestemmelse vil det blive en myndighedsopgave for Digitaliseringsstyrelsen at sikre forvaltningen af tegnebogsapplikationen. Det er forudsat, at Digitaliseringsstyrelsen vil gøre det teknisk muligt for en fysisk person at oprette sig i tegnebogsapplikationen og dele beviser med modtagerparter. Brugeren har også mulighed for at interagere med andre brugere, jf. den foreslåede § 3, stk. 4. Det vil blive en del af Digitaliseringsstyrelsens myndighedsopgave at indhente de oplysninger om den fysiske person, der er nødvendige for, at personen kan oprettes som bruger i tegnebogsapplikationen, og at brugeren får en aktiv tegnebogsapplikation. De nødvendige oplysninger om brugeren indhentes fra Datafordeleren eller NemLog-in, jf. de almindelige bemærkninger pkt. 3. Det er forudsat, at Digitaliseringsstyrelsen vil sikre, at der via support kan tilbydes

vejledning til oprettelse og anvendelse af tegnebogsapplikationen.

Det er desuden en del af forvaltningsopgaven, at Digitaliseringsstyrelsen kan spærre en tegnebogsapplikation, jf. den foreslåede bestemmelse i § 4, stk. 1. Spærringen kan f.eks. foretages i tilfælde af sikkerhedsbrud eller misbrug.

Dertil kommer at det foreslåede vil medføre, at Digitaliseringsstyrelsen sikrer udvikling, drift og vedligeholdelse af tegnebogsapplikationen.

Det foreslås i § 3, stk. 2, at opretter en bruger, der har et CPR-nummer, sig i tegnebogsapplikationen, dannes bevis for brugerens identitet. Denne bruger kan tilføje sit foto til sin tegnebogsapplikation, hvorefter beviset sammen med fotoet vil udgøre et legitimationsbevis. Dette legitimationsbevis tjener samme formål som legitimationskort udstedt i medfør af lov om udstedelse af legitimationskort.

Den foreslåede bestemmelse vil medføre, at når en bruger med et CPR-nummer opretter sig i tegnebogsapplikationen, vil der blive udstedt bevis for brugerens identitet. Identitetsbeviset udgør en forudsætning for at brugeren få udstedt andre beviser, herunder et særskilt aldersbevis. Det er hensigten, at aldersbeviset, kan anvendes i tilfælde, hvor brugeren alene har brug for at kunne dokumentere at være over eller under en given alder. Dette kunne f.eks. være et behov ved køb af aldersbegrænsede produkter som tobak og alkohol i online handel eller i fysiske butikker samt ved aldersverifikation over for sociale medier.

Det foreslås i 2. pkt., at en bruger, der har et CPR-nummer, kan tilføje sit foto til sin tegnebogsapplikation.

Det foreslåede vil indebære at bevis for identitet sammen med fotoet vil udgøre et legitimationsbevis. Det er ikke et krav, at tilføjelsen af foto sker i forbindelse med oprettelsen. Tilføjelsen kan ske på et hvilket som helst senere tidspunkt. Det foreslås i 3. pkt., at legitimationsbeviset kan tjene samme formål som legitimationskortet udstedt i medfør af lov om udstedelse af legitimationskort.

Formålet med 3. pkt., er at skabe et digitalt legitimationsbevis, der kan tjene samme formål som det fysiske legitimationskort, der kan udstedes hos en kommune, jf. lov om udstedelse af legitimationskort.

Som anført i de almindelige bemærkninger pkt. 2.2.1.1. er det Digitaliseringsministeriets vurdering, at der er stort potentiale i, at den nationale digitale identitetstegnebog indeholder et digitalt legitimationsbevis, som kan tjene samme formål som det fysiske legitimationskort, men ligeledes understøtte legitimation i en digital sammenhæng.

Det bemærkes i den forbindelse, at såfremt brugeren sletter sit bevis for identitet, kan tegnebogsapplikationen ikke fungere, uagtet at øvrige beviser ikke slettes af brugeren, jf. de almindelige bemærkninger, pkt. 3.2 og 4.1.

Det foreslås i § 3, stk. 3, at opretter en bruger, der ikke har et CPR-nummer, sig i tegnebogsapplikationen, dannes bevis for brugerens navn og fødselsdato.

Med den foreslåede bestemmelse får en bruger, der ikke har et CPR-nummer, ved oprettelsen i tegnebogsapplikationen udstedt bevis for brugerens navn og fødselsdato. Brugeren har også mulighed for at tilføje sit foto til sin tegnebogsapplikation, som kan anvendes sammen med beviset for navn og fødselsdato. Det er hensigten, at beviset kan anvendes i tilfælde, hvor brugeren har brug for at kunne dokumentere at være over en given alder. Brugeren kan fravælge at dele sit navn, og således vælge alene at dokumentere at være over eller under en given aldersgrænse. Dette kunne f.eks. være relevant ved køb af aldersbegrænsede produkter som tobak og alkohol i onlinehandel eller i fysiske butikker samt ved aldersverifikation i forhold til sociale medier. Beviset for navn og fødselsdato har hverken selvstændigt eller i kombination med et foto en fastsat retsvirkning i medfør af denne lov. En bruger, der ikke har et CPR-nummer, vil ikke kunne få udstedt andre beviser til tegnebogsapplikationen. Den praktiske anvendelse af tegnebogsapplikationen for denne brugergruppe er derfor begrænset til alene at kunne dokumentere alder i de tilfælde, hvor dette er påkrævet, f.eks. som nævnt ovenfor ved køb af aldersbegrænsede produkter. Årsagen til at en bruger, der ikke har et CPR-nummer, ikke kan få udstedt andre beviser, er den manglende sikre identifikation af en bruger, som er en forudsætning for at offentlige myndigheder kan udstede et bevis til en brugers tegnebogsapplikation.

Det bemærkes i den forbindelse, at såfremt brugeren sletter bevis for navn og fødselsdato, kan tegnebogsapplikationen ikke fungere, jf. de almindelige bemærkninger, pkt. 3.2 og 4.1.

Det foreslås i § 3, stk. 4, at Digitaliseringsstyrelsen som led i udviklingen og driften af tegnebogsapplikationen sikrer, at en bruger kan anvende sin tegnebogsapplikation til at interagere med en anden brugers tegnebogsapplikation med henblik på at validere og dele beviser.

Den foreslåede bestemmelse vil medføre, at en bruger kan validere en anden brugers beviser eller dele egne beviser med andre brugere. Der vil således være tale om en brug mellem fysiske personer. Dette svarer til, at en bruger i dag, med den digitale kørekortsapplikation, kan scanne en anden brugers digitale kørekort.

Interaktion vil kunne ske ved visuel inspektion eller via en scanningsfunktionalitet i tegnebogsapplikationen. Scanningsfunktionaliteten vil kunne anvendes både før og efter, at en bruger har oprettet sig i tegnebogsapplikationen, og forudsætter således ikke oprettelse i tegnebogsapplikationen. At scanningsfunktionen ikke forudsætter oprettelse i tegnebogsapplikationen medfører, at en fysisk person, der enten ikke kan eller ønsker at oprette sig, kan drage nytte af at kunne validere beviser fra andre brugere af tegnebogsap-

plikationen. Dette vil tillige tilgodese fysiske personer, der ikke har eller kan få et MitID eller andet eID.

Til § 4

Det foreslås i § 4, stk. 1, at Digitaliseringsstyrelsen kan træffe afgørelse om spærring af tegnebogsapplikationen.

Den foreslåede bestemmelse vil medføre, at Digitaliseringsstyrelsen kan træffe afgørelse om spærring af tegnebogsapplikationen.

Afgørelser, der træffes i medfør af den foreslåede bestemmelse, er forvaltningsretlige afgørelser, og skal således overholde forvaltningslovens bestemmelser, herunder bestemmelserne om partshøring, begrundelse og klagevejledning.

Spærring, der sker på brugerens anmodning, falder uden for den foreslåede bestemmelses anvendelsesområde.

Spærring vil f.eks. være relevant i tilfælde hvor tegnebogsapplikationen er kompromitteret, hvor der er mistanke om, at tegnebogsapplikationen er kompromitteret eller hvis brugeren ikke overholder reglerne for brug af tegnebogsapplikationen. Dette er for at opretholde tilliden til og sikkerheden i den nationale digitale identitetstegnebog. Der skal altid foreligge en saglig begrundelse for at iværksætte en spærring. En saglig grund kan være konstatering af sikkerhedsbrud i tegnebogsapplikationens software eller brugernes hardware eller der er mistanke om trusler eller angreb, hvorved der er risiko for, at en eller flere tegnebogsapplikationer kan blive eller er blevet kompromitteret.

En spærring af tegnebogsapplikationen skal forstås som en spærring af brugerens individuelle tegnebogsapplikation. En spærring hindrer ikke, at brugeren på ny henter tegnebogsapplikationen fra en anvist platform og opretter sig igen.

Det foreslås i § 4, stk. 2, at ministeren for digitalisering fastsætter regler om afgørelser, jf. stk. 1, samt om forvaltningen og anvendelsen af tegnebogsapplikationen, herunder om en brugers oprettelse, en brugers spærring af tegnebogsapplikationen, en brugers sletning af beviser i tegnebogsapplikationen, tekniske krav, krav til foto og inaktivering af tegnebogsapplikationen efter brugerens dødsfald.

Den foreslåede bestemmelse vil medføre, at ministeren for digitalisering fastsætter regler om afgørelser, jf. stk. 1, samt om forvaltningen og anvendelsen af tegnebogsapplikationen, herunder om en brugers oprettelse, en brugers spærring af tegnebogsapplikationen, en brugers sletning af beviser i tegnebogsapplikationen, tekniske krav, krav til foto og inaktivering af tegnebogsapplikationen efter brugerens dødsfald.

Der vil i medfør af den foreslåede bestemmelse blive fastsat regler om de krav, der skal opfyldes for at kunne blive oprettet i tegnebogsapplikationen, samt om de vilkår, der løbende skal overholdes for at besidde og anvende tegnebogsapplikationen.

Der vil desuden blive fastsat nærmere tekniske krav til

anvendelse af tegnebogsapplikationen. Dette omfatter bl.a. krav til understøttede operativsystemer og versioner heraf på brugerens mobile enhed. Det er hensigten, at de understøttede operativsystemer og disses versioner skal svare til de operativsystemer og versioneringer, der til enhver tid understøtter MitID's mobilapplikation. Der vil derudover blive fastsat regler om registrering af identitet og identitetssikring ved oprettelse i tegnebogsapplikationen samt krav til det foto, der kan tilføjes til tegnebogsapplikationen.

I takt med at erfaringsgrundlaget med tegnebogsapplikationen bliver større, kan der opstå behov for at fastsætte yderligere regler om tegnebogsapplikationens forvaltning og anvendelse.

Der vil i medfør af den foreslåede bestemmelse tillige blive fastsat regler om, at en bruger selv kan spærre sin tegnebogsapplikation samt slette beviser i tegnebogsapplikationen.

Endelig forudsættes det, at ministeren for digitalisering fastsætter regler om inaktivering af en brugers tegnebogsapplikation efter brugerens dødsfald.

Til § 5

Der findes ikke i gældende ret regler, der regulerer bevisudstedelsesservicen, idet denne er en del af den nye nationale digitale identitetstegnebog.

Det foreslås i § 5, stk. 1, at Digitaliseringsstyrelsen stiller en bevisudstedelsesservice til rådighed for offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde, der som led i deres myndighedsudøvelse kan levere data fra deres autentiske kilde til brug for udstedelse af beviser til tegnebogsapplikationen. Digitaliseringsstyrelsen sikrer forvaltning, udvikling, drift og vedligeholdelse af bevisudstedelsesservicen.

Den foreslåede bestemmelse vil indebære, at Digitaliseringsstyrelsen stiller bevisudstedelsesservicen til rådighed for offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde, der som led i deres myndighedsudøvelse leverer data fra deres autentiske kilde til brug for udstedelse af beviser til tegnebogsapplikationen. Endvidere pålægges Digitaliseringsstyrelsen med den foreslåede bestemmelse at sikre forvaltning, udvikling, drift og vedligeholdelse af bevisudstedelsesservicen.

Med bestemmelsen muliggøres, at bevisudstedelsesservicen kan udstede beviser på vegne af offentlige myndigheder og offentligretlige organer, der som led i deres myndighedsudøvelse leverer data fra deres autentiske kilde til brug for udstedelse af beviser til tegnebogsapplikationen. Bevisudstedelsesservicen tjener alene som et teknisk værktøj, der understøtter bevisudstedelsen og letter arbejdsbyrden hos den enkelte offentlige myndighed og det offentligretlige organ, som således ikke selv skal anskaffe en bevisudstedelsesservice.

Digitaliseringsstyrelsen skal efter den foreslåede bestemmelse i stk. 1, sikre forvaltning, udvikling, drift og vedligeholdelse af den tekniske løsning bevisudstedelsesservicen. Det er forudsat, at Digitaliseringsstyrelsen ved udbud vil udpege en leverandør, som vil få til opgave på vegne af Digitaliseringsstyrelsen at sikre udvikling, drift og vedligeholdelse af bevisudstedelsesservicen.

Tilrådighedsstillelsen sker alene til offentlige myndigheder og offentligretlige organer, der har ansvar for en autentisk kilde. Dette indebærer, at en offentlig myndighed eller et offentligretligt organ, skal have ansvaret for et register eller et system, der leverer attributter om en fysisk person eller genstand, og som anses for at være en primær kilde til disse oplysninger, eller er anerkendt som autentisk i overensstemmelse med dansk ret herunder administrativ praksis.

Den foreslåede bestemmelse vil indebære, at bevisudstedelsesservicen ikke vil kunne anvendes af private juridiske enheder men alene af offentlige myndigheder og offentligretlige organer.

Digitaliseringsstyrelsen har efter den foreslåede bestemmelse ansvaret for at forvalte bevisudstedelsesservicen. Opgaven med forvaltning af bevisudstedelsesservicen varetages gennem funktionaliteterne nævnt i den foreslåede bestemmelses stk. 2.

Det foreslås i § 5, stk. 2, at Digitaliseringsstyrelsen som led i udviklingen og driften sikrer, at bevisudstedelsesservicen indeholder følgende funktionaliteter:

- 1) Oprettelse, ændring, ajourføring og nedlæggelse af typer af beviser.
- 2) Dannelse og udstedelse af beviser.
- 3) En liste over bevisers gyldighed.
- 4) Logning af beviser, der er udstedt eller forsøgt udstedt, og transmissionskald til og fra offentlige myndigheders og offentligretlige organers it-systemer indeholdende autentiske kilder.
- 5) Identifikation og autentifikation af brugere.

Den foreslåede bestemmelse vil indebære, at Digitaliseringsstyrelsen pålægges at sikre, at bevisudstedelsesservicen indeholder de funktionaliteter, der er oplistet i bestemmelsens nr. 1-5.

Med bestemmelsen vil det blive fastlagt, hvilke konkrete funktionaliteter, som bevisudstedelsesservicen skal indeholde, og som, jf. den foreslåede § 5, stk. 1, således stilles til rådighed for bevisudstedelse på vegne af offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde, der som led i deres myndighedsudøvelse leverer data fra deres autentiske kilde til brug for udstedelse af beviser til tegnebogsapplikationen.

De angivne funktionaliteter, der er oplistet i bestemmelsens nr. 1 - 5, er alle nødvendige for, at beviser kan udstedes til tegnebogsapplikationen og sikre dennes og bevisudstedelsesservicens integritet og uafviselighed. I relation hertil sikrer bevisudstedelsesservicen, at beviser er digitalt signerede

med en signatur, der kan valideres af relevante modtagerparter, når disse anvender en teknologi, der muliggør dette. I praksis betyder det, at Digitaliseringsstyrelsen sikrer, at den offentlige nøgle eller tilsvarende, der hører til den private nøgle eller tilsvarende, som er benyttet til signeringen, stilles til rådighed på en offentlig tilgængelig liste. Tilsvarende sikrer Digitaliseringsstyrelsen, at certifikater benyttet til signering, der ikke længere er gyldige, fremgår af en offentligt tilgængelig spærreliste eller tilsvarende.

Ifølge den foreslåede *stk. 2, nr. 1*, skal Digitaliseringsstyrelsen sikre, at bevisudstedelsesservicen muliggør oprettelse, ændring, ajourføring og nedlæggelse af typer af beviser.

Den foreslåede bestemmelse vil medføre, at der sikres den nødvendige forvaltning og vedligehold i forhold til de enkelte typer af beviser. Typer af beviser skal således forstås som et katalog over beviser, som det er muligt at få udstedt til tegnebogsapplikationen gennem bevisudstedelsesservicen, jf. den foreslåede § 6, stk. 3. Offentlige myndigheder og offentligretlige organer, der leverer data fra deres autentiske kilde til bevisudstedelsesservicen til brug for udstedelse af beviser til tegnebogsapplikationen, har med bestemmelsen mulighed for oprettelse, ændring, ajourføring og nedlæggelse af typer af beviser. I praksis betyder dette, at de pågældende offentlige myndigheder eller offentligretlige organer kan afgive informationer om deres it-systemer herunder angive information om, hvorfra data skal hentes og navngive typerne af beviser. Det skal ligeledes i praksis være muligt for de pågældende offentlige myndigheder og offentligretlige organer, der er omfattet af den foreslåede bestemmelse, at ændre og nedlægge typer af beviser.

Ifølge den foreslåede *stk. 2, nr. 2*, skal Digitaliseringsstyrelsen sikre, at bevisudstedelsesservicen muliggør dannelse og udstedelse af beviser.

Den foreslåede bestemmelse vil medføre, at beviser kan oprettes via bevisudstedelsesservicen, idet dannelsen og udstedelsen er en forudsætning for oprettelsen af beviser. Dannelse og udstedelse af beviser relaterer sig således til konkrete beviser, der skal udstedes til en konkret bruger.

Bevisudstedelsesservicen sikrer både tilrådighedsstillelse af de relevante tekniske snitflader mod tegnebogsapplikationen og mod en autentisk kilde, således at de offentlige myndigheder og offentligretlige organer, der leverer data fra deres autentiske kilde til brug for udstedelse af beviser til tegnebogsapplikationen, ikke skal gøre dette.

Såfremt de tekniske snitflader ændres, er det bevisudstedelsesservicens opgave at sikre, at den nødvendige opdatering sker. Det er ligeledes bevisudstedelsesservicens opgave at tilføje understøttelsen af yderligere tekniske snitflader i det omfang, at dette er nødvendigt for at benytte bevisudstedelsesservicen. Når en opdatering af en eksisterende teknisk snitflade eller tilføjelse af en ny teknisk snitflade medfører et behov for tilpasning af information til et bevis, er den

offentlige myndighed eller det offentligretlige organ selv ansvarlig for at foretage denne tilpasning.

Ifølge den foreslåede *stk. 2, nr. 3*, skal Digitaliseringsstyrelsen sikre, at bevisudstedelsesservicen indeholder en liste over udstedte bevisers gyldighed.

Listen sikrer, at det til enhver tid fremgår, om et bevis er aktivt eller spærret. Den offentlige myndighed eller det offentligretlige organ, der har ansvar for en autentisk kilde, fastsætter gyldighedsperioden for et bevis. Listen anvendes i tilfælde af behov for spærring eller opdatering af beviset inden udløb. Beviser, som udstedes med en gyldighedsperiode på under 24 timer, forventes ikke at gøre brug af spærring. Det er hensigten, at beviser med kort gyldighed automatisk fornyes, såfremt brugerne fortsat opfylder betingelserne for at få udstedt det enkelte bevis. Bevisudstedelsesservicen kan således efterspørge nye versioner af udstedte beviser hos offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde, hvis beviset er ved at udløbe eller er udløbet. For beviser med en kort gyldighedsperiode betyder det i praksis, at bevisudstedelsesservicen på vegne af en tegnebogsapplikation kan efterspørge genudstedelse af beviser, uden at brugeren skal autentificere sig på ny.

Digitaliseringsstyrelsens kan spærre et bevis, hvis der konstateres fejl i et bevis.

Offentlige myndigheder og offentligretlige organer har derudover mulighed for at anmode Digitaliseringsstyrelsen om spærring af beviser, f.eks. i tilfælde af at en bruger ikke længere opfylder de materielle betingelser for at være i besiddelse af beviset. Et eksempel herpå er et bevis, der skal fornyes gennem årlig gebyrbetaling, og hvor retten til at besidde beviset bortfalder grundet manglende gebyrbetaling. På anmodning fra den offentlige myndighed eller det offentligretlige organ, der har ansvar for den pågældende autentiske kilde, markerer Digitaliseringsstyrelsen herefter det pågældende bevis som spærret.

Listen over udstedte bevisers gyldighed tjener tillige det formål, at en modtagerpart ved anmodning om at modtage et bevis, har mulighed for at slå op i listen og få aktuel status på, hvorvidt et givent bevis er aktivt eller spærret. Bevisets indholdsdata eller tilhørsforhold kan ikke udledes af listen, hvorfor der alene kan deles status om beviset er aktivt eller spærret. Dette har særlig betydning i de tilfælde, hvor brugeren anvender et bevis fra sin tegnebogsapplikation uden adgang til internettet. Her vil tegnebogsapplikationen grundet manglende adgang til internettet ikke nødvendigvis korrekt angive om et givent bevis er aktivt eller spærret. Tegnebogsapplikationen udfører således også et tjek mod listen hver gang tegnebogsapplikationen anvendes i online tilstand, hvorved det sikres, at udløbne beviser enten automatisk fornyes eller brugeren bliver påmindet om at anmode om et nyt bevis.

Ifølge den foreslåede *stk. 2, nr. 4*, skal Digitaliseringsstyrelsen sikre, at bevisudstedelsesservicen indeholder en funktio-

nalitet til logning af beviser, der er udstedt eller forsøgt udstedt, og transmissionskald til og fra offentlige myndigheders og offentligretlige organers it-systemer indeholdende autentiske kilder.

Den foreslåede bestemmelse vil medføre, at der i bevisudstedelsesservicen skabes gennemsigtighed i forhold til de interaktioner som offentlige myndigheder og offentligretlige organer har med bevisudstedelsesservicen. Bevisudstedelsesservicen foretager logning af transmissionskald til og fra en offentlig myndigheds eller offentligretligt organs autentiske kilde. Logningen er anonymiseret og anvendes til fejlsøgning, jf. de almindelige bemærkninger pkt. 3.2. Dette vil f.eks. være relevant, hvis en bruger henvender sig om manglende udstedelse af bevis uagtet anmodning herom, hvor årsagen til den manglende udstedelse f.eks. kan være, at transmissionskald fejler eller at udstedelsen fejler. Bevisudstedelsesservicen vil i et sådant tilfælde kunne spore, om der på en given dato har været gennemført transmissionskald til og fra en autentisk kilde, men ikke indholdet af sådanne kald.

Ifølge den foreslåede *stk. 2, nr. 5*, skal Digitaliseringsstyrelsen sikre, at bevisudstedelsesservicen muliggør identifikation og autentifikation af brugere.

Den foreslåede bestemmelse vil medføre, at der ved identifikation og autentifikation opnås sikkerhed for brugerens identitet på sikringsniveau betydelig, således at offentlige myndigheder og offentligretlige organer sikrer sig, at et bevis udstedes til den rette bruger.

Til § 6

Der findes ikke i gældende ret regler, der regulerer bevisudstedelsesservicen, idet denne er en del af den nye nationale digitale identitetstegnebog.

Det foreslås i § 6, *stk. 1*, at en offentlig myndighed eller et offentligretligt organ, med ansvar for en autentisk kilde, skal anvende Digitaliseringsstyrelsens bevisudstedelsesservice, når de som led i deres myndighedsudøvelse vil levere data fra deres autentiske kilde til brug for udstedelse af beviser til tegnebogsapplikationen.

Den foreslåede bestemmelse vil indebære, at offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde har en pligt til at anvende Digitaliseringsstyrelsens bevisudstedelsesservice for at få udstedt beviser til en brugers tegnebogsapplikation. Digitaliseringsstyrelsen er i så henseende bevisudsteder.

Offentlige myndigheder eller offentligretlige organer med ansvar for en autentisk kilde skal således anskaffe bevisudstedelsesservicen fra Digitaliseringsstyrelsen, som stiller denne til rådighed, jf. den foreslåede § 5, *stk. 1*. Da bevisudstedelsesservicen alene stilles til rådighed for offentlige myndigheder og offentligretlige organer, jf. den foreslåede bestemmelse i § 5, *stk. 1*, gælder pligten til at anvende be-

visudstedelsesservicen kun, når udstedelsen af beviser sker som led i myndighedsudøvelsen.

Det vil med den foreslåede ordning være Digitaliseringsstyrelsen, der indkøber og udvikler bevisudstedelsesservicen, hvorefter Digitaliseringsstyrelsen vil være systemejer og varetage de opgaver, som følger hermed. Digitaliseringsstyrelsen har i denne sammenhæng en særlig status som instrument og teknisk tjeneste for hele den offentlige sektor og skal imødekomme alle offentlige myndigheders og offentligretlige organers bestillinger i overensstemmelse med lovens bestemmelser.

Den udbudsretlige relation mellem Digitaliseringsstyrelsen og de offentlige myndigheder og offentligretlige organer er i denne henseende af intern karakter, kendetegnet ved Digitaliseringsstyrelsens underordning og afhængighed af de offentlige myndigheder og offentligretlige organer, når de afgiver deres bestillinger i medfør af loven.

Offentlige myndigheder og offentligretlige organer vil med den foreslåede ordning have en pligt til at anskaffe bevisudstedelsesservicen fra Digitaliseringsstyrelsen og vil skulle anvende bevisudstedelsesservicen, når beviser udstedes til tegnebogsapplikationen som led i myndighedsudøvelse. Dette gælder dog ikke, hvis bevisudstedelsesservicen ikke kan imødekomme en offentlig myndigheds eller et offentligretligt organs særlige behov, jf. den foreslåede bestemmelse i § 6, stk. 2.

Den foreslåede bestemmelse indebærer, at Digitaliseringsstyrelsen gives en eksklusiv rettighed, som omhandlet i § 17 i udbudsloven til at tilrådighedsstille bevisudstedelsesservicen til offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde, som pålægges en pligt til at anvende bevisudstedelsesservicen, når anvendelsen sker som led i myndighedsudøvelsen.

Nærværende lov med tilhørende bekendtgørelser udgør i denne sammenhæng en ensidig retsakt, der alene opstiller betingelser for Digitaliseringsstyrelsen. Eftersom alle regler om tilrådighedsstillelse og anvendelse vil følge af loven, vil der ikke være tale om en gensidigt bebyrdende kontrakt, jf. udbudslovens § 24, nr. 24, og offentlige myndigheder og offentligretlige organer kan således anskaffe bevisudstedelsesservicen fra Digitaliseringsstyrelsen i medfør af loven, uden at skulle gennemføre et udbud, jf. også præambelbetragtning nr. 5 og 34 i udbudsdirektivet.

Anskaffelsespligten for offentlige myndigheder og offentligretlige organer giver Digitaliseringsstyrelsen en eksklusiv rettighed og har til formål at sikre den offentlige orden og sikkerhed, herunder hensynet til de samfundsøkonomiske overvejelser om fælles anskaffelse af it-løsninger i det offentlige. Offentlige myndigheders og offentligretlige organers anvendelse af bevisudstedelsesservicen er vederlagsfri, idet selve tilrådighedsstillelsen finansieres af den samlede bevilling til den nationale digitale identitetstegnebog, som indgår i Digitaliseringsstyrelsens bevilling på finansloven.

Der henvises i øvrigt til de almindelige bemærkninger pkt. 2.2.2.

Det foreslås i § 6, stk. 2, at bestemmelsen i stk. 1 ikke gælder, hvis Digitaliseringsstyrelsens bevisudstedelsesservice ikke kan imødekomme den offentlig myndigheds eller det offentligretlige organs særlige behov. Den offentlige myndighed eller det offentligretlige organ kan i sådanne tilfælde selv udstede beviser til tegnebogsapplikationen. Bevisudstedelsen skal opfylde de regler, der fastsættes i medfør af den foreslåede § 7, stk. 2.

Den foreslåede bestemmelse vil indebære, at en offentlig myndighed eller et offentligretligt organ ikke er forpligtet til at anvende Digitaliseringsstyrelsens bevisudstedelsesservice til udstedelse af beviser, hvis Digitaliseringsstyrelsens bevisudstedelsesservice ikke imødekommer den offentlige myndigheds eller det offentligretlige organs særlige behov. I dette tilfælde kan den offentlige myndighed eller det offentligretlige organ således vælge selv, at udstede beviser til tegnebogsapplikationen. Det er dog efter den foreslåede bestemmelse et krav, at udstedelsen af beviser til tegnebogsapplikationen efter den foreslåede § 6, stk. 2, skal opfylde de regler, der fastsættes i medfør af den foreslåede bemyndigelse i § 7, stk. 2.

Den foreslåede bestemmelse vil således være en undtagelse til pligten i § 6, stk. 1, hvorefter en offentlig myndighed eller et offentligretligt organ med ansvar for en autentisk kilde skal anvende Digitaliseringsstyrelsens bevisudstedelsesservice til at få udstedt beviser til tegnebogsapplikationen som led i deres myndighedsudøvelse.

Det er forudsat, at offentlige myndigheder og offentligretlige organer kun anvender undtagelsen til anskaffelsespligten, når der er et sagligt og proportionalt grundlag for, at Digitaliseringsstyrelsens bevisudstedelsesservice ikke kan anvendes ud fra en vurdering om særlige behov. Det vil f.eks. være tilfældet, hvis omkostningerne forbundet med tilpasning af den offentlige myndigheds eller det offentligretlige organs it-systemer klart overstiger behovet for anvendelse af bevisudstedelsesservicen til at gennemføre udstedelse af beviser. Et andet eksempel på særlige behov kan være, hvis en offentlig myndighed eller et offentligretligt organ har unikke sikkerhedskrav til f.eks. signering, der ikke kan opfyldes af Digitaliseringsstyrelsens tekniske løsning. I disse tilfælde vil den offentlige myndighed eller det offentligretlige organ i stedet have mulighed for selv at udstede digitale beviser til en brugers tegnebogsapplikation, og er i disse tilfælde selv ansvarlige for bevisudstedelsen.

Det foreslås i § 6, stk. 3, at en offentlig myndighed og et offentligretligt organ, som benytter Digitaliseringsstyrelsens bevisudstedelsesservice, sikrer opdatering og ajourføring af typer af beviser samt spærring af beviser.

Den foreslåede bestemmelse vil medføre, at en offentlig myndighed eller et offentligretligt organ selv har ansvaret for, at typer af beviser opdateres og ajourføres. Typer af

beviser skal forstås som et katalog over beviser, som det er muligt at få udstedt gennem bevisudstedelsesservicen, jf. den foreslåede § 5, stk. 2, nr. 1.

Ved »opdatere og ajourføre« i den foreslåede bestemmelse forstås, at den offentlige myndighed eller det offentligretlige organ sikrer, at de typer af beviser, som de pågældende har ansvaret for er opdateret og ajourført.

Ved »spærre« i den foreslåede bestemmelse forstås, at beviset skal markeres som ugyldigt af Digitaliseringsstyrelsen, hvilket sker på anmodning fra den offentlige myndighed eller det offentligretlige organ, der har ansvar for den pågældende autentiske kilde. Der henvises til de specielle bemærkninger til den foreslåede bestemmelse i § 5, stk. 2, nr. 3.

Til § 7

Der findes ikke i gældende ret regler, der regulerer offentlige myndigheders eller offentligretlige organers tilslutning til Digitaliseringsstyrelsens bevisudstedelsesservice, idet bevisudstedelsesservicen er en del af den nye nationale digitale identitetstegnebog.

Det foreslås i § 7, stk. 1, at ministeren for digitalisering fastsætter regler om forvaltningen og anvendelsen af Digitaliseringsstyrelsens bevisudstedelsesservice, herunder om offentlige myndigheders og offentligretlige organers tilslutning til og anvendelse af bevisudstedelsesservicen samt tekniske krav hertil.

Den foreslåede bestemmelse vil medføre, at ministeren for digitalisering bemyndiges til at fastsætte regler om offentlige myndigheders og offentligretlige organers tilslutning til Digitaliseringsstyrelsens bevisudstedelsesservice.

Den foreslåede bestemmelse vil indebære, at alle regler om en offentlig myndigheds og et offentligretligt organs tilslutning til Digitaliseringsstyrelsens bevisudstedelsesservice fastsættes af ministeren for digitalisering, med det formål at reglerne skaber en fuldstændig gennemsigtighed og klarhed over, hvilke konkrete krav der gælder ved tilslutningen til bevisudstedelsesservicen. Krav der knytter sig til tilslutningen, vil primært udgøre tekniske krav, som en offentlig myndighed eller et offentligretligt organ skal opfylde og overholde for at tilslutte sig til bevisudstedelsesservicen og anvende denne. Endvidere vil der blive fastsat nødvendige sikkerhedsmæssige krav for at opretholde sikkerheden i bevisudstedelsesservicen.

Digitaliseringsstyrelsen er, for så vidt angår bevisudstedelsesservicen, en teknisk tjeneste for den offentlige forvaltning i Danmark. Digitaliseringsstyrelsens relation til offentlige myndigheder og offentligretlige organer er ikke af kontraktmæssig karakter. Relationen er i stedet af intern karakter, kendetegnet ved afhængighed og over- underordningsforhold. Således er Digitaliseringsstyrelsen forpligtet til at levere bevisudstedelsesservicen på baggrund af de regler

om tilslutning, som ministeren for digitalisering ved denne bestemmelse bemyndiges til at fastsætte.

Digitaliseringsstyrelsen kan således ikke forhandle om krav til tilslutningen til bevisudstedelsesservicen.

Det foreslås i § 7, stk. 2, at ministeren for digitalisering fastsætter regler om en offentlig myndigheds eller et offentligretligt organs forvaltning og anvendelse af egen bevisudstedelse for beviser, der udstedes til tegnebogsapplikationen, jf. § 6, stk. 2, herunder om tekniske krav til egen bevisudstedelse.

Den foreslåede bestemmelse vil indebære, at ministeren for digitalisering fastsætter regler der sikrer, at den offentlige myndighed eller det offentligretlige organ som vælger, at udstede beviser i medfør af den foreslåede § 6, stk. 2, udsteder beviser, der er kompatible med tegnebogsapplikationen. Endvidere vil der blive fastsat regler om pligt til at spærre beviser, der er udstedt med fejl eller hvor brugeren ikke længere er materielt berettiget til at være i besiddelse af et bevis.

Bemyndigelsen vil omfatte hjemmel til fastsættelse af regler om Digitaliseringsstyrelsens spærring af en offentlig myndigheds eller et offentligretligt organs egen udstedelse af beviser til tegnebogsapplikationen. En spærring vil f.eks. være relevant i tilfælde, hvor bevisudstedelsen til tegnebogsapplikationen er kompromitteret, eller hvis den offentlige myndighed eller det offentligretlige organ ikke overholder de regler for bevisudstedelse til tegnebogsapplikationen, som vil blive fastsat i medfør af bemyndigelsen.

Til § 8

Der findes ikke i gældende ret regler, der regulerer offentlige myndigheders og offentligretlige organers digitalisering af beviser, der udstedes til tegnebogsapplikationen. Der findes desuden ikke i gældende ret regler om retsvirkning af beviser, der er udstedt til tegnebogsapplikationen, idet denne løsning er en del af den nye nationale digitale identitetstegnebog.

Det foreslås i § 8, stk. 1, at vedkommende minister på sit område kan fastsætte regler om digitalisering af beviser til tegnebogsapplikationen og om digitaliseringens retsvirkning, jf. dog stk. 2.

Den foreslåede bestemmelse vil medføre, at den enkelte ressortminister herved får hjemmel til i bekendtgørelsesform at fastsætte nærmere regler om digitalisering af beviser til tegnebogsapplikationen og om retsvirkningen af disse beviser inden for sit ressortområde. Den foreslåede bestemmelse sikrer således en administrativt fleksibel mulighed for at udstede nærmere regler i bekendtgørelsesform.

Det foreslås i § 8, stk. 2, at bestemmelsen i stk. 1 ikke finder anvendelse, hvor der i medfør af anden lovgivning er fastsat regler om digitalisering af beviser og retsvirkningen heraf.

Den foreslåede bestemmelse i § 8, stk. 1, vil således ikke have forrang for anden lovgivning. Det vil være op til det enkelte ressortområde at vurdere, om det er nødvendigt både at fastsætte regler om digitalisering af beviser og om retsvirkningen heraf.

Til § 9

Der findes ikke i gældende ret regler, der regulerer modtagerparten eller modtagerpartregisteret, idet denne løsning er en del af den nye nationale digitale identitetstegnebog.

Det foreslås i § 9, stk. 1, at Digitaliseringsstyrelsen stiller et modtagerpartregister til rådighed for modtagerparten. Digitaliseringsstyrelsen sikrer forvaltning, udvikling, drift og vedligeholdelse af modtagerpartregisteret.

Modtagerpartregisteret er ikke identisk med det modtagerpartregister, der fremgår af eIDAS2, idet den foreslåede bestemmelse udelukkende har til formål at regulere modtagerpartregisteret i den rent nationale digitale identitetstegnebog, jf. også de almindelige bemærkninger pkt. 1. og 2.2.3.

Ved »modtagerpart« i den foreslåede bestemmelse forstås en juridisk enhed med et CVR-nummer eller en juridisk enhed registreret i et register i et andet EU-/EØS-land svarende til Det Centrale Virksomhedsregister, der modtager beviser fra en brugers tegnebogsapplikation, jf. den foreslåede bestemmelse i § 2, nr. 6.

Den foreslåede bestemmelse vil indebære, at modtagerparten kan anvende modtagerpartregisteret. Det er Digitaliseringsstyrelsen, der forestår forvaltningen af modtagerpartregisteret. Forvaltningen af modtagerpartregisteret indebærer bl.a. at modtagerparten entydigt identificeres og autentificeres.

Den foreslåede bestemmelse vil tillige indebære, at Digitaliseringsstyrelsen sikrer den løbende drift, udvikling og vedligeholdelse af modtagerpartregisteret.

Det foreslås i § 9, stk. 2, at en modtagerpart skal være registreret i modtagerpartregisteret, når en modtagerpart anvender en teknologi til at modtage beviser, hvor beviser overføres via internettet, jf. dog stk. 3.

Modtagerpartregisteret har til formål at sikre, at brugerne ved, hvem de interagerer med, når beviser overføres via internettet. Det vil typisk være i et online scenarie, hvor brugeren anvender sin mobile enhed for at tilgå en modtagerparts tjeneste, og hvor modtagerparten ønsker at modtage et bevis fra brugerens tegnebogsapplikation. I onlinescenariet er fysisk nærhed mellem bruger og modtagerpart ikke påkrævet for overførslen af beviser. Det vil dog også kunne være relevant i det fysiske møde mellem brugere og modtagerpart, hvis modtagerparten ønsker at anvende en teknologi, hvor beviser overføres via internettet, jf. den foreslåede bestemmelse i § 9, stk. 3. Dette kan f.eks. være tilfældet i butikker, hvor modtagerparten ønsker, at en bruger indlæser et link eller en QR-kode, hvorved der overføres et bevis til modtagerparten. Registrering i modtagerpartregisteret gi-

ver brugeren vished om modtagerpartens identitet, idet tegnebogsapplikationen sikrer, at modtagerparten autentificerer sig korrekt.

Det foreslås i § 9, stk. 3, at en modtagerpart, som ikke er registreret i modtagerpartregisteret, kan under anvendelse af en teknologi, hvor beviser overføres via internettet alene anmode om at modtage bevis, der bekræfter, hvorvidt en bruger er over eller under en given aldersgrænse.

Den foreslåede bestemmelse er en undtagelse til kravet i det foreslåede stk. 2, om registrering i modtagerpartregisteret ved overførsel af beviser via internettet. Såfremt modtagerparten alene anmoder om bevis for, at brugeren er over eller under en given aldersgrænse, herunder har en bestemt alder, er det ikke et krav, at modtagerparten er registreret i modtagerpartregisteret. Brugeren overfører ikke personoplysninger, der kan identificere brugeren, og hensynet til brugerens vished for hvem brugeren interagerer med, gør sig ikke gældende med samme styrke som ved interaktion med overførsel af personoplysninger, der kan identificere brugeren.

Modtagelse af beviser kan ske på flere måder: Bruger og modtagerpart er i fysisk nærhed af hinanden, hvorved overførsel af beviser f.eks. kan ske ved, at modtagerparten scanner et bevis, der fremvises af brugeren. Overførsel kan ligeledes ske via internettet, hvis modtagerparten vælger dette, hvor modtagerparten danner en QR-kode eller et link, som brugeren skal åbne med sin tegnebogsapplikation. Overførsel via internettet sker ligeledes, hvor brugeren interagerer med modtagerparten via en internetbrowser.

Pligten til at registrere sig i modtagerpartregisteret afhænger af overførselsmetode samt om beviset indeholder andet end et bevis for, at brugeren er over eller under en given aldersgrænse. Et eksempel på registreringspligt kunne være at brugeren indlæser link eller QR-kode, hvorved overførslen af beviset sker via internettet både i fysisk og online scenarier, og beviset indeholder f.eks. uddannelsesoplysninger.

Det foreslås i § 9, stk. 4, at ministeren for digitalisering kan fastsætte regler om, at overførsel via internettet af andre beviser end det bevis, der er nævnt i stk. 3, ikke kræver registrering i modtagerpartregisteret.

Den foreslåede bestemmelse vil give ministeren for digitalisering bemyndigelse til at kunne fastsætte, at overførsel af andre beviser via internettet end bevis for at brugeren er over eller under en given alder, ikke kræver registrering af modtagerparten i modtagerpartregisteret. Bemyndigelsen vil kunne bruges til at undtage modtagerparten for registrering, når de alene anmoder om overførsel af beviser, der ikke kan henføres til en identificerbar person. Et eksempel herpå er bevis for, at en bruger er en fysisk person, hvormed en bruger over for en online tjeneste anonymt kan bevise, at brugeren ikke er en robot eller lignende, »jeg-er-ikke-en-robot« bevis.

Til § 10

Der findes ikke i gældende ret regler, der regulerer modtagerparter eller modtagerpartregisteret, idet denne løsning er en del af den nye nationale digitale identitetstegnebog.

Det foreslås i § 10, at ministeren for digitalisering fastsætter regler om forvaltningen af modtagerpartregisteret, herunder om en modtagerparts registrering i modtagerpartregisteret, om tekniske krav til en modtagerpart samt om tekniske krav til modtagelse af beviser.

Modtagerpartregisteret har bl.a. til formål at sikre entydig identifikation af en modtagerpart.

Den foreslåede bestemmelse vil medføre, at ministeren for digitalisering fastsætter regler om forvaltningen af modtagerpartregisteret, herunder om tekniske krav til modtagerparter samt om tekniske krav til modtagelse af beviser.

Ministeren for digitalisering fastsætter hvilke oplysninger, der til enhver tid skal fremgå om en modtagerpart i registeret. De oplysninger, der som minimum forventes at skulle indgå i modtagerpartregisteret, udgør oplysninger, der kan identificere modtagerparten, f.eks. navn på modtagerparten og kontaktoplysninger. Det vil i medfør af den foreslåede bemyndigelse også være muligt at fastsætte regler om, at modtagerparter skal oplyse, hvilke beviser, som de ønsker at modtage og til hvilket formål.

De tekniske krav vedrører krav til kompatibilitet og sikkerhed i modtagerpartregisteret.

Det er muligt for en modtagerpart at slette sin registrering i modtagerpartregisteret.

Som led i forvaltningen af modtagerpartregisteret kan Digitaliseringsstyrelsen, jf. den foreslåede bestemmelse i § 11 og bemærkningerne hertil, spærre en modtagerpart, herunder for anvendelse af modtagerpartregisteret i strid med regler, der fastsættes i medfør af den foreslåede bemyndigelse.

Til § 11

Der findes ikke i gældende ret regler, der regulerer svigagtig eller anden ulovlig anvendelse, anvendelse i strid med regler fastsat i medfør af § 10 eller i øvrigt mistillidsskabende anvendelse af modtagerpartregisteret eller beviser.

Det foreslås i § 11, stk. 1, at Digitaliseringsstyrelsen kan spærre en modtagerpart, der er registreret i modtagerpartregisteret, hvis denne anvender modtagerpartregisteret eller beviser på en svigagtig eller en anden ulovlig måde, i strid med regler fastsat i medfør af § 10 eller i øvrigt på en måde, der er åbenlyst egnet til at svække tilliden til den nationale digitale identitetstegnebog.

Afgørelser, der træffes i medfør af bestemmelsen, er forvaltningsretlige afgørelser og skal således overholde forvaltningslovens bestemmelser, herunder bestemmelser om parts-høring, begrundelse og klagevejledning.

Den foreslåede bestemmelse vil indebære, at det er muligt

at fratage modtagerparter, der er registreret i modtagerpartregisteret muligheden for at modtage beviser ved at spærre disse i modtagerpartregisteret. Herefter vil modtagerparten ikke længere kunne modtage beviser, som kræver at modtagerparten er registreret i modtagerpartregisteret, jf. den foreslåede bestemmelse i § 9, stk. 2.

Spærring af en modtagerpart vil alene kunne ske, hvis denne anvender modtagerpartregisteret eller beviser på svigagtig eller anden ulovlig måde, i strid med regler fastsat i medfør af § 10 eller i øvrigt på en måde, der er åbenlyst egnet til at svække brugernes tillid til den nationale digitale identitetstegnebog.

Ved ulovlig anvendelse skal forstås, at en endelig retsafgørelse eller myndighedsafgørelse fastslår, at modtagerparten har overtrådt gældende ret. Et eksempel herpå kan være, at en modtagerpart bruger et bevis i markedsføringsøjemed, og domstolene træffer afgørelse om, at anvendelsen er i strid med markedsføringsloven. Det er således ikke Digitaliseringsstyrelsen, som foretager den materielle vurdering af lovligheden, men Digitaliseringsstyrelsen kan reagere på andre instansers afgørelser.

Ved svigagtig anvendelse skal forstås en modtagerparts bevidste fortielse eller afgivelse af urigtige oplysninger over for brugeren, der således overfører et bevis uden korrekt viden om f.eks. formål med overførslen.

Ved anvendelse af modtagerpartregisteret eller beviser i strid med regler fastsat i medfør af § 10 forstås, at modtagerparten ikke overholder regler fastsat af ministeren for digitalisering om forvaltningen af modtagerpartregisteret, herunder om tekniske krav til modtagerparter samt om tekniske krav til modtagelse af beviser, jf. de specielle bemærkninger til den foreslåede § 10.

Ved anvendelse på en måde der åbenlyst er egnet til at svække tilliden til den nationale digitale identitetstegnebog, skal forstås en anvendelse, der i almindeligt omdømme er egnet til at svække tilliden.

Modtagerparter, der ikke er registreret i modtagerpartregisteret, kan ikke spærres, ligesom en spærret modtagerpart fortsat vil kunne modtage beviser, hvis modtagelse ikke kræver registrering i modtagerpartregisteret. Det vil derfor ikke med hjemmel i den foreslåede lov være muligt at spærre modtagerparter, der ikke kræves registreret i modtagerpartregisteret. Modtagerparterne vil stadig skulle behandle overførte beviser i overensstemmelse med øvrig gældende lovgivning. Det betyder f.eks., at en bruger kan anmelde en behandling til Datatilsynet, hvis brugeren mener, at en modtagerpart ikke overholder databeskyttelsesreglerne.

Det foreslås i § 11, stk. 2, at ministeren for digitalisering kan fastsætte regler om betingelser for en modtagerparts genregistrering efter spærring, jf. stk. 1.

Den foreslåede § 11, stk. 2, er en bemyndigelse til ministeren for digitalisering til at fastsætte nærmere regler om

betingelser for en modtagerparts genregistrering efter spærring, jf. den foreslåede stk. 1.

Betingelserne for genregistrering i modtagerpartregisteret efter en spærring skal være proportionale og sagligt begrundet. Et eksempel på en både proportional og saglig betingelse er, at modtagerparten dokumenterer at have afhjulpnet de forhold, der førte til spærring.

Til § 12

Det er i almindelig dansk erstatningsret en betingelse for erstatning, at der er sket en skade, hvorved der er lidt et økonomisk tab, og at der foreligger et ansvarsgrundlag. Det er en betingelse for at ifalde erstatningsansvar, at skadevolder har handlet culpøst enten ved forsætlig eller uagtsom adfærd. Det er endvidere en betingelse for at skadelidte kan opnå erstatning, at der er årsagsforbindelse mellem den culpøse adfærd og tabet. Endvidere skal den indtrådte skade være en påregnelig følge af den culpøse adfærd. Der findes ikke gældende ret, der begrænser Digitaliseringsstyrelsens erstatningsansvar for den nationale digitale identitetstegnebog.

Det foreslås i § 12, at Digitaliseringsstyrelsen alene kan blive erstatningsansvarlig som følge af fejl begået i forbindelse med bevisudstedelse i medfør af § 5, stk. 2, nr. 2 og 5.

Den foreslåede bestemmelse vil medføre, at Digitaliseringsstyrelsens ansvar er begrænset til fejl begået i forbindelse med dannelsen og udstedelse af beviser samt identifikation og autentifikation af brugere i medfør af den foreslåede § 5, stk. 2, nr. 2 og 5. Ansvarsgrundlaget er culpapreglen, hvilket betyder, at Digitaliseringsstyrelsen kan ifalde erstatningsansvar for fejl, der kan henføres til ansvarspådragende adfærd.

For at kunne danne og udstede beviser skal Digitaliseringsstyrelsen modtage data fra en autentisk kilde. Den autentiske kilde har ansvaret for, at data i kilden er korrekte. Digitaliseringsstyrelsen kan ikke efterprøve dette, og hvis et bevis dannes og udstedes på grundlag af ukorrekte data fra den autentiske kilde, kan ansvaret herfor ikke gøres gældende over for Digitaliseringsstyrelsen. Den foreslåede bestemmelse medfører således, at ansvaret herfor ikke kan gøres gældende over for Digitaliseringsstyrelsen.

Den foreslåede bestemmelse vil ligeledes medføre, at Digitaliseringsstyrelsen ikke er erstatningsansvarlig for fejl i de tekniske løsninger tegnebogsapplikation og modtagerpartregister, herunder at beviser ikke kan fremvises, udstedes eller er utilgængelige på grund af nedetid i den nationale digitale identitetstegnebog.

En fysisk person eller juridisk enhed, der gør erstatningskrav gældende i medfør af den foreslåede bestemmelse, skal opfylde de sædvanlige erstatningsbetingelser.

Til § 13

Der findes ikke i gældende ret regler om tilsyn med den nationale digitale identitetstegnebog.

Det foreslås i § 13, stk. 1, at Digitaliseringsstyrelsen fører tilsyn med forvaltning, drift og vedligeholdelse af den nationale digitale identitetstegnebog.

Den foreslåede bestemmelse vil medføre, at Digitaliseringsstyrelsen fører tilsyn med den nationale digitale identitetstegnebog.

Det er de tre tekniske løsninger, tegnebogsapplikation, bevisudstedelsesservice og modtagerpartregister, der vil blive underlagt tilsyn.

Digitaliseringsstyrelsen bliver både systemejer og tilsynsførende med den nationale digitale identitetstegnebog.

Tilsynet påser, at de tre tekniske løsninger bl.a. efterlever gældende lovgivning, herunder den foreslåede lov og standarder for informationssikkerhed, samt at løsningerne er udviklet og driftes i overensstemmelse med de specifikationer, der ligger til grund for løsningerne.

I Digitaliseringsstyrelsen er der ledelsesmæssig og organisatorisk adskillelse mellem tilsyn på den ene side og forvaltning, udvikling, drift og vedligeholdelse på den anden side. Dette sikrer, at tilsyn og forvaltning m.v. bliver udført uafhængigt og forskellige steder i styrelsen med forskellig ledelsesmæssig reference.

Det foreslås i § 13, stk. 2, at Digitaliseringsstyrelsen kan føre tilsyn med offentlige myndigheders og offentligretlige organers overholdelse af regler fastsat i medfør af § 7, stk. 2.

Den foreslåede bestemmelse vil medføre, at Digitaliseringsstyrelsen kan føre tilsyn med offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde, når disse selv udsteder beviser til tegnebogsapplikationen.

Det er forventningen, at tilsynet efter den foreslåede bestemmelse vil blive varetaget som en del af Digitaliseringsstyrelsens forvaltningsopgaver i forbindelse med den nationale digitale identitetstegnebog.

Det er ikke hensigten med bestemmelsen, at Digitaliseringsstyrelsen skal føre aktivt tilsyn med offentlige myndigheder og offentligretlige organer, der selv leverer udstedelse af beviser, idet det forudsættes, at offentlige myndigheder og offentligretlige organers egen bevisudstedelse varetages i henhold til de fastsatte regler. Hvis Digitaliseringsstyrelsen bliver opmærksom på, at udstedelse ikke sker i overensstemmelse med de regler, der fastsættes i medfør af den foreslåede bestemmelse i § 7, stk. 2, kan tilsyn blive iværksat.

Til § 14

Der henvises til de almindelige bemærkninger pkt. 3. vedrørende behovet for en regulering i den foreslåede bestemmelse om de enkelte aktørers dataansvar.

Der findes gældende ret, som regulerer behandlingen af personoplysninger i den nationale digitale identitetstegnebog, herunder i de tekniske løsninger i form af en tegnebogsapplikation, en bevisudstedelsesservice og et modtagerpartregister i form af gældende regler i databeskyttelsesforordningen (2016/679) og databeskyttelsesloven, jf. lovbekendtgørelse nr. 289 af 8. marts 2024.

Med den foreslåede bestemmelse i § 14, stk. 1, fastslås det, at Digitaliseringsstyrelsen er dataansvarlig for behandling af personoplysninger i forbindelse med en brugers oprettelse af sin tegnebogsapplikation.

Efter download af tegnebogsapplikationen til sin mobile enhed, skal brugeren logge ind med et MitID eller andet eID, for at oprette sig. Digitaliseringsstyrelsen er ved login med MitID en tjenesteudbyder, hvis dataansvar følger af lov om MitID og NemLog-in, jf. lov nr. 783 af 4. maj 2021, som ændret ved lov nr. 1559 af 12. december 2023. For at gøre tegnebogsapplikationen operationel, således at den kan anvendes af brugeren til at indhente beviser og overføre disse til modtagerparter eller andre brugere, er det nødvendigt, at der oprettes bevis for brugerens identitet eller bevis for brugerens navn og fødselsdato. Brugeren skal derfor som led i oprettelsen sende anmodning til bevisudstedelsesservicen, om at udstede bevis for identitet eller bevis for navn og fødselsdato. De data, der er nødvendige for at danne bevis for identitet, indhentes af bevisudstedelsesservicen fra Datafordeleren. Hjemlen hertil er databeskyttelsesforordningens artikel 6, stk. 1, litra e. De data, der er nødvendige for at danne bevis for navn og fødselsdato, indhentes fra data, som modtages fra NemLog-in i forbindelse med anvendelse af MitID eller andet eID, i oprettelsesflowet, hvor data fra autentifikationssvaret anvendes med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra e. Der henvises til de specielle bemærkninger til det foreslåede stk. 2, vedrørende dataansvar i bevisudstedelsesservicen. Oprettelse af bevis for identitet eller bevis for navn og fødselsdato er en forudsætning for, at tegnebogsapplikationen kan anvendes efter sin hensigt.

Digitaliseringsstyrelsen muliggør, at en bruger med CPR-nummer kan tilføje sit foto til tegnebogsapplikationen. Anvendelse af foto sammen med bevis for en brugers identitet, kan herefter tjene samme formål som legitimationskort udstedt efter lov om legitimationskort. Der henvises herom til de specielle bemærkninger til § 3. Digitaliseringsstyrelsen er dataansvarlig for behandlingen af foto i tilføjelsesprocessen. Når foto herefter er tilføjet i tegnebogsapplikationen, ophører Digitaliseringsstyrelsens dataansvar.

Digitaliseringsstyrelsen har ikke dataansvar for beviser i brugerens tegnebogsapplikation. Brugeren har enekontrol over indholdet i sin tegnebogsapplikation, og kan overføre eller slette beviser i sin tegnebogsapplikation, ligesom brugeren kan vælge at spærre sin tegnebogsapplikation, og brugeren udøver alle rettigheder i forbindelse hermed.

Med den foreslåede bestemmelse i § 14, stk. 2, fastslås,

at Digitaliseringsstyrelsen er dataansvarlig for behandling af personoplysninger i bevisudstedelsesservicen, samt for behandling af personoplysninger i forbindelse med levering af et udstedt bevis, indtil beviset er leveret til en brugers tegnebogsapplikation.

Digitaliseringsstyrelsen stiller bevisudstedelsesservice til rådighed for andre offentlige myndigheder og offentligretlige organer med ansvar for en autentisk kilde, når disse som led i myndighedsudøvelse vælger at få udstedt beviser på anmodning fra en bruger. Der henvises til de specielle bemærkninger til den foreslåede bestemmelse i § 5. I forbindelse med behandlingen af personoplysninger, der modtages fra en anden offentlig myndighed eller et offentligretligt organ med ansvar for en autentisk kilde, med henblik på bevisudstedelse, er det Digitaliseringsstyrelsen, der bestemmer formål, og afgør med hvilke hjælpemidler, der foretages behandling af personoplysninger. Digitaliseringsstyrelsen er således ansvarlig for korrekt identifikation af brugeren, der anmoder bevisudstedelsesservicen om at udstede et bevis, samt for korrekt dannelse af bevis til brugeren.

Behandlingen af personoplysninger omfatter de personoplysninger, der videregives fra en offentlig myndighed eller et offentligretligt organ med ansvar for en autentisk kilde, der som led i myndighedsudøvelse får udstedt beviser, når en bruger anmoder herom. Det er ikke muligt på forhånd at angive hvilke oplysninger, der behandles, da det helt afhænger af hvilke oplysninger, der skal indgå i et bevis. Det kan således f.eks. dreje sig om helbredsoplysninger eller andre oplysninger omfattet af databeskyttelsesforordningens art. 9, stk. 1. Et eksempel herpå er oplysning i et kørekort om krav til indehaveren om anvendelse af briller eller kontaktlinser under kørslen.

Digitaliseringsstyrelsens dataansvar ophører, når et bevis er leveret til brugerens tegnebogsapplikation, hvor brugeren har enekontrol over beviset.

Med den foreslåede bestemmelse i § 14, stk. 3, fastslås det, at Digitaliseringsstyrelsen er dataansvarlig for behandling af CVR-numre eller tilsvarende registreringer i et register i et andet EU-/EØS-land og kontaktoplysninger i modtagerpartregisteret, der henviser til en personligt ejet virksomhed, jf. § 2, nr. 5.

Digitaliseringsstyrelsens hjemmel til behandling af CVR-nummer eller tilsvarende registrering i et andet EU-/EØS-land, og kontaktoplysninger for personligt ejede virksomheder, er databeskyttelsesforordningens artikel 6, stk. 1, litra e.

Med den foreslåede bestemmelse i § 14, stk. 4, fastslås det, at en modtagerpart er dataansvarlig for de personoplysninger, som er indeholdt i de beviser, der overføres fra den enkelte brugers tegnebogsapplikation.

Bestemmelsen fastslår, at en modtagerpart er dataansvarlig for de personoplysninger, som er indeholdt i de beviser, som overføres fra den enkelte brugers tegnebogsapplikation.

Modtagerparten bliver selvstændigt dataansvarlig for modtagne beviser og skal herunder have hjemmel til behandling. Dette gælder uanset, om modtagerparten er omfattet af krav om registrering i modtagerpartregisteret.

Til § 15

Det foreslås i § 15, at loven træder i kraft den 1. januar 2026.

Den foreslåede bestemmelse fastlægger lovens ikrafttrædelsestidspunkt til den 1. januar 2026.

Til § 16

Bestemmelsen vedrører lovens territoriale gyldighed.

Det foreslås i § 16, at loven ikke gælder for Færøerne og Grønland, men ved kongelig anordning helt eller delvis kan sættes i kraft for Færøerne og Grønland med de ændringer, som henholdsvis de færøske og de grønlandske forhold tilsiger.

Den foreslåede bestemmelse medfører, at loven ikke vil gælde for Færøerne og Grønland, men ved kongelig anordning helt eller delvist kan sættes i kraft for Færøerne og Grønland med de ændringer, som henholdsvis de færøske og de grønlandske forhold tilsiger.