

Udskriftsdato: 13. januar 2025

2020/1 LSF 159 (Gældende)

Forslag til Lov om MitID og NemLog-in

Ministerium: Finansministeriet

Journalnummer: Finansmin.,
Digitaliseringsstyrelsen, j.nr. 2018-489

Forslag

til

Lov om MitID og NemLog-in

Afsnit I

Generelle bestemmelser

Kapitel 1

Lovens anvendelsesområde

§ 1. Loven finder anvendelse på følgende infrastrukturløsninger samt nationale digitale identiteter og elektroniske identifikationsmidler udstedt i medfør heraf:

- 1) Den danske nationale elektroniske identifikationsordning (MitID-løsningen).
- 2) Den fællesoffentlige digitale infrastrukturløsning (NemLog-in).

Kapitel 2

Definitioner

§ 2. I denne lov forstås ved:

- 1) MitID-løsningen: Den danske nationale elektroniske identifikationsordning.
- 2) MitID: Den nationale digitale identitet af en privatperson og tilhørende elektroniske identifikationsmidler, som kan tilknyttes privatpersoners og erhvervsbrugeres digitale identiteter. MitID er den nationale identitetsgarant for privatpersoner.
- 3) Autentifikation: En proces som genkender og verificerer en digital identitet gennem anvendelse af et elektronisk identifikationsmiddel.
- 4) Sikringsniveau: Sikringsniveauet definerer graden af sikkerhed for autentifikation. Der sondres mellem tre forskellige sikringsniveauer for autentifikation, henholdsvis niveau lav, betydelig og høj.
- 5) Sikker autentifikation: Autentifikation på sikringsniveau betydelig eller høj.
- 6) NemLog-in: Den fællesoffentlige digitale infrastrukturløsning, som sætter privatpersoner og erhvervsbrugere med digitale identiteter i stand til at interagere med digitale selvbetjeningsløsninger. NemLog-in er endvidere den nationale identitetsgarant for erhvervsidentiteter. NemLog-in indeholder de serviceområder, som angives i § 8, stk. 2 og 3.
- 7) Privatperson: Fysisk person, der udelukkende agerer på vegne af sig selv uden forbindelse til en juridisk enhed, og som ikke er en erhvervsbruger.
- 8) Erhvervsbruger: Fysisk person, der er associeret med en offentlig myndighed, et offentligretligt organ eller en juridisk enhed, som er oprettet med én eller flere erhvervsidentiteter i serviceområdet Erhvervsadministration i NemLog-in.
- 9) Juridisk enhed: Juridisk enhed med et cvr-nummer, jf. lov om Det Centrale Virksomhedsregister, der hverken er en offentlig myndighed eller et offentligretligt organ.
- 10) Offentlig myndighed: Statslige, regionale og kommunale myndigheder.
- 11) Offentligretligt organ: 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 halvdelens 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.

- 12) Digital selvbetjeningsløsning: Et it-system, hvor privatpersoner eller erhvervsbrugere med digitale identiteter kan tilgå digital selvbetjening efter at være blevet autentificeret.
- 13) Digital identitet: En samling af data, der unikt identificerer en privatperson eller en erhvervsbruger.
- 14) Elektronisk identifikationsmiddel: En materiel enhed, en immateriel enhed eller en kombination af disse, der indeholder personidentifikationsdata, og som bruges til autentifikation i digitale selvbetjeningsløsninger. Et elektronisk identifikationsmiddel består af ét eller flere elementer, der hver især er et elektronisk identifikationsmiddel.
- 15) Tjenesteudbyder: En offentlig myndighed, et offentligretligt organ eller en juridisk enhed, der er ansvarlig for én eller flere digitale selvbetjeningsløsninger.
- 16) Brugerorganisation: En offentlig myndighed, et offentligretligt organ eller en juridisk enhed, der er tilsluttet og anvender serviceområdet Erhvervsadministration i NemLog-in til deres erhvervsbrugere.
- 17) Broker: En offentlig myndighed, et offentligretligt organ eller en juridisk enhed, der videreformidler autentifikation af digitale identiteter.

Afsnit II

MitID-løsningen

Kapitel 3

Tilrådighedsstillelse af MitID-løsningen og MitID

§ 3. Digitaliseringsstyrelsen stiller MitID-løsningen til rådighed for offentlige myndigheder, offentligretlige organer og juridiske enheder. Digitaliseringsstyrelsen sikrer udvikling, drift og vedligeholdelse af løsningen.

Stk. 2. Digitaliseringsstyrelsen stiller MitID til rådighed for privatpersoner og erhvervsbrugere, hvis disse opfylder betingelserne for udstedelse af MitID fastsat i medfør af § 4, stk. 2.

Kapitel 4

Forvaltning af MitID-løsningen og MitID

§ 4. Digitaliseringsstyrelsen sikrer følgende forvaltningsopgaver:

- a) Identitetssikring af privatpersoner, registrering af identiteter, udstedelse, suspension, spærring og genåbning af MitID til privatpersoner efter reglerne fastsat i medfør af stk. 2.
- b) Udstedelse, spærring, suspension og genåbning af identifikationsmidler til erhvervsbrugere efter reglerne fastsat i medfør af stk. 2.

Stk. 2. Finansministeren fastsætter regler om forvaltning af MitID-løsningen og MitID, herunder regler om identitetssikring af privatpersoner, registrering af identiteter, udstedelse, spærring, suspension og genåbning af MitID til privatpersoner og erhvervsbrugere samt om adgang til at klage til Digitaliseringsstyrelsen over afgørelser truffet i medfør af disse regler.

§ 5. Digitaliseringsstyrelsen kan udpege offentlige myndigheder, offentligretlige organer eller juridiske enheder til på vegne af Digitaliseringsstyrelsen at varetage opgaver i medfør af § 3, stk. 1, 2. pkt., samt opgaver i medfør af § 4, stk. 1.

Stk. 2. Kommunalbestyrelsen skal på vegne af Digitaliseringsstyrelsen varetage opgaver i medfør af § 4, stk. 1.

Kapitel 5

Anvendelse af MitID-løsningen og MitID

§ 6. Når offentlige myndigheder og offentligretlige organer anvender digitale selvbetjeningsløsninger til at udføre en myndighedsopgave, skal de sikre, at privatpersoner og erhvervsbrugere med MitID gives adgang til selvbetjeningsløsningen, hvis adgangen kræver sikker autentifikation. MitID-løsningen skal i dette tilfælde anskaffes fra Digitaliseringsstyrelsen.

Stk. 2. Når offentlige myndigheders og offentligretlige organers digitale selvbetjeningsløsninger ikke anvendes til at udføre en myndighedsopgave, eller hvis adgangen til løsningerne ikke kræver sikker autentifikation, kan de offentlige myndigheder og offentligretlige organer give privatpersoner og erhvervsbrugere adgang til løsningerne med MitID. MitID-løsningen kan i dette tilfælde anskaffes fra Digitaliseringsstyrelsen.

§ 7. Juridiske enheder kan i rollen som tjenesteudbydere anvende MitID-løsningen.

Afsnit III

NemLog-in

Kapitel 6

Tilrådighedsstillelse af NemLog-in

§ 8. Digitaliseringsstyrelsen stiller NemLog-in til rådighed for offentlige myndigheder, offentligretlige organer og juridiske enheder. Digitaliseringsstyrelsen sikrer udvikling, drift og vedligeholdelse af NemLog-in.

Stk. 2. NemLog-in indeholder følgende serviceområder til tjenesteudbydere:

- 1) Login og autentifikation, som sikrer den service, at privatpersoner og erhvervsbrugere kan tilgå digitale selvbetjeningsløsninger.
- 2) Digital repræsentation, som sikrer følgende services:
 - a) Digital repræsentation af en privatperson, således at privatpersonen ved anvendelse af en digital selvbetjeningsløsning kan lade sig repræsentere digitalt af en anden privatperson, af en erhvervsbruger eller af en juridisk enhed over for en offentlig myndighed eller et offentligretligt organ, som udbyder en digital selvbetjeningsløsning.
 - b) Digital repræsentation af en juridisk enhed, således at en erhvervsbruger, der selvstændigt kan repræsentere en juridisk enhed, kan repræsentere enheden ved anvendelse af en digital selvbetjeningsløsning over for en offentlig myndighed eller et offentligretligt organ, som udbyder en digital selvbetjeningsløsning.
- 3) Digital signering, som sikrer følgende services:
 - a) At offentlige myndigheder, offentligretlige organer og juridiske enheder kan udstille digital signering af dokumenter i digitale selvbetjeningsløsninger.
 - b) At privatpersoner og erhvervsbrugere kan signere digitale dokumenter og validere signerede dokumenters digitale signatur og integritet.

Stk. 3. NemLog-in indeholder serviceområdet Erhvervsadministration til brugerorganisationer, som sikrer følgende services:

- a) At offentlige myndigheder, offentligretlige organer og juridiske enheder kan oprette, administrere og anvende digitale erhvervsidentiteter samt tildele og administrere elektroniske identifikationsmidler, hvis de opfylder betingelserne for identitetssikring ved oprettelse som brugerorganisation, som nærmere fastsat i medfør af § 9, stk. 4.
- b) At offentlige myndigheder, offentligretlige organer og juridiske enheder kan tildele og administrere rettigheder og certifikater til erhvervsidentiteter.

Kapitel 7

Forvaltning af NemLog-in

§ 9. Digitaliseringsstyrelsen sikrer, at der sker forvaltning af NemLog-in, herunder identitetssikring af offentlige myndigheder, offentligretlige organer og juridiske enheder, når de oprettes som brugerorganisationer i serviceområdet Erhvervsadministration i NemLog-in. Digitaliseringsstyrelsen sikrer, at brugerorganisationers adgang til serviceområdet Erhvervsadministration i NemLog-in samt erhvervsbrugeres digitale identiteter kan spærres og genåbnes efter reglerne fastsat i medfør af stk. 4.

Stk. 2. En privatperson, der skal registreres som erhvervsbruger i serviceområdet Erhvervsadministration, kan anvende sit MitID udstedt til privatbrug, til identitetssikring ved registreringen.

Stk. 3. En erhvervsbruger kan få tilknyttet sit elektroniske identifikationsmiddel, som er tilknyttet privatpersonens MitID-identitet, til sin erhvervsidentitet, således at erhvervsbrugeren kan anvende førnævnte identifikationsmiddel til at autentificere en eller flere erhvervsidentiteter. Tilknytningen er frivillig for erhvervsbrugeren og frivillig for brugerorganisationen, som erhvervsbrugeren er tilknyttet.

Stk. 4. Finansministeren fastsætter regler om forvaltning af NemLog-in, herunder regler for identitetssikring af brugerorganisationer, spærring og genåbning af erhvervsbrugeres digitale identiteter og om adgang til at klage til Digitaliseringsstyrelsen over afgørelser truffet i medfør af disse regler.

§ 10. Digitaliseringsstyrelsen kan udpege offentlige myndigheder, offentligretlige organer eller juridiske enheder til på vegne af Digitaliseringsstyrelsen at varetage opgaver i medfør af § 8, stk. 1, 2. pkt., samt opgaver i medfør af § 9, stk. 1.

Kapitel 8

Anvendelse af NemLog-in

§ 11. Offentlige myndigheder og offentligretlige organer, som anvender en digital selvbetjeningsløsning til at udføre en myndighedsopgave, skal i rollen som tjenesteudbydere anvende følgende serviceområder:

- 1) Login og autentifikation, jf. § 8, stk. 2, nr. 1, hvis adgangen til den digitale selvbetjeningsløsning kræver sikker autentifikation.
- 2) Digital repræsentation, jf. § 8, stk. 2, nr. 2.

Stk. 2. Offentlige myndigheder og offentligretlige organer kan i rollen som tjenesteudbydere anvende følgende serviceområder:

- 1) Login og autentifikation, jf. § 8, stk. 2, nr. 1, hvis adgangen til den digitale selvbetjeningsløsning ikke kræver sikker autentifikation eller hvis der ikke udføres en myndighedsopgave.
- 2) Digital signering, jf. § 8, stk. 2, nr. 3.

Stk. 3. Offentlige myndigheder og offentligretlige organer kan i rollen som brugerorganisationer anvende serviceområdet Erhvervsadministration, jf. § 8, stk. 3.

Stk. 4. Offentlige myndigheder og offentligretlige organer skal i de i stk. 1 anførte tilfælde anskaffe serviceområderne fra Digitaliseringsstyrelsen. Offentlige myndigheder og offentligretlige organer kan i de i stk. 2 og 3 anførte tilfælde anskaffe serviceområderne fra Digitaliseringsstyrelsen.

§ 12. Juridiske enheder kan indgå aftale med Digitaliseringsstyrelsen om anvendelse af serviceområderne nævnt i § 8, stk. 2, nr. 1 og nr. 3, samt stk. 3.

Afsnit IV

Behandling af personoplysninger

Kapitel 9

Behandling af personoplysninger og videregivelse af risikodata

§ 13. Ved en privatpersons anvendelse af MitID eller en erhvervsbrugers anvendelse af det elektroniske identifikationsmiddel i MitID til login og autentifikation kan Digitaliseringsstyrelsen videregive autentifikationssvar, herunder risikodata vedrørende den konkrete og enkelte transaktion, til en broker, der er tilsluttet MitID-løsningen eller NemLog-in.

Stk. 2. En broker kan foretage automatiske afgørelser om log-in på baggrund af risikodata videregivet efter stk. 1.

Stk. 3. En broker, der i medfør af stk. 1 har modtaget autentifikationssvar, kan videregive det modtagne og behandlede autentifikationssvar til en tjenesteudbyder, der modtager autentifikationer fra MitID-løsningen.

Stk. 4. Ved en erhvervsbrugers anvendelse af et elektronisk identifikationsmiddel fra en lokal identitetsgarant tilsluttet NemLog-in kan Digitaliseringsstyrelsen videregive autentifikationssvar vedrørende den konkrete og enkelte transaktion til en broker, der er tilsluttet NemLog-in.

Stk. 5. . En broker, der i medfør af stk. 4 har modtaget autentifikationssvar, kan videregive det modtagne og behandlede autentifikationssvar til en tjenesteudbyder, der gennem en broker modtager autentifikationer fra NemLog-in.

§ 14. Digitaliseringsstyrelsen kan kortvarigt og i et sikret teknisk miljø behandle følsomme personoplysninger, i forbindelse med validering af digitale signaturer i valideringstjenesten i serviceområdet Digital signering.

Afsnit V

Øvrige bestemmelser

Kapitel 10

Opkrævning af gebyr og vederlag

§ 15. Digitaliseringsstyrelsen indgår aftale med juridiske enheder om vederlag for tilslutning til og anvendelse af MitID-løsningen og NemLog-in.

Stk. 2. Offentlige myndigheder og offentligretlige organer betaler for MitID-løsningen og NemLog-in gennem fællesoffentlig finansiering eller ved betaling af vederlag fastsat af finansministeren.

Stk. 3. Finansministeren kan fastsætte regler om opkrævning af gebyr hos privatpersoner for registrering og udstedelse af MitID.

Kapitel 11

Regler om tilrådighedsstillelse og anvendelse for offentlige myndigheder og offentligretlige organer

§ 16. Finansministeren fastsætter regler om tilrådighedsstillelse for offentlige myndigheder og offentligretlige organer, jf. §§ 3 og 8, og om offentlige myndigheder og offentligretlige organers tilslutning til og anvendelse af MitID-løsningen og NemLog-in.

Kapitel 12

Påbud

§ 17. Digitaliseringsstyrelsen kan meddele offentlige myndigheder og offentligretlige organer påbud om at opfylde forpligtelser i henhold til § 6, stk. 1, og § 11, stk. 1.

Kapitel 13

Tilsyn

§ 18. Digitaliseringsstyrelsen fører tilsyn med drift, vedligeholdelse og forvaltning af MitID-løsningen og NemLog-in, herunder at løsningerne overholder nationale standarder for eID-ordninger.

Stk. 2. Finansministeren kan fastsætte nærmere regler om Digitaliseringsstyrelsens tilsyn efter stk. 1, herunder om Digitaliseringsstyrelsens samarbejde med andre tilsynsmyndigheder efter aftale med vedkommende minister.

Kapitel 14

Tavshedspligt

§ 19. Offentlige myndigheders medarbejdere og enhver, der i øvrigt udøver bistand til offentlige myndigheder, er under ansvar efter straffelovens §§ 152-152 f forpligtet til at iagttage tavshed over for uvedkommende med hensyn til oplysninger om den tekniske og sikkerhedsmæssige indretning samt processer for opretholdelse, vedligeholdelse og drift af sikkerhed i MitID-løsningen og NemLog-in.

Kapitel 15

Forvaltningslovens anvendelse

§ 20. Forvaltningsloven finder anvendelse på afgørelser om udstedelse, spærring og genåbning af MitID, jf. § 4, stk. 2, som træffes af juridiske enheder, der er udpeget i medfør af § 5, stk. 1.

Stk. 2. Forvaltningsloven finder anvendelse på afgørelser om identitetssikring af juridiske enheder, spærring af brugerorganisationers adgang til Erhvervsadministration i NemLog-in, samt spærring af digitale identiteter, jf. § 9, stk. 2, som træffes af juridiske enheder, der er udpeget i medfør af § 10.

Kapitel 16

Erstatningsansvar

§ 21. Digitaliseringsstyrelsen er erstatningsansvarlig over for privatpersoner, offentlig myndigheder, offentligretlige organer eller juridiske enheder, som følge af fejl i forbindelse med registrering, udstedelse og håndtering af MitID, anvendelse og autentifikation af en privatperson eller en erhvervsbruger, medmindre at Digitaliseringsstyrelsen kan godtgøre, at Digitaliseringsstyrelsen ikke har handlet forsætligt eller uagtsomt.

Kapitel 17

Delegation

§ 22. Finansministeren kan efter aftale med vedkommende minister bemyndige en anden statslig myndighed til at udøve de beføjelser, der i denne lov er tillagt Digitaliseringsstyrelsen.

Kapitel 18

Tilvejebringelse af fremtidige elektroniske identifikationsordninger

§ 23. Digitaliseringsstyrelsen kan samarbejde med offentlige myndigheder, offentligretlige organer og juridiske enheder om at tilvejebringe fremtidige elektroniske identifikationsordninger svarende til MitID-løsningen eller andre løsninger, der måtte træde i stedet herfor.

Afsnit VI
Ikrafttræden m.v.

Kapitel 19

Ikrafttræden og overgangsregler

§ 24. Finansministeren fastsætter tidspunktet for lovens ikrafttræden og kan bestemme, at forskellige dele af loven træder i kraft på forskellige tidspunkter.

§ 25. Finansministeren kan fastsætte regler om ophævelse af lov nr. 439 af 8. maj 2018, om udstedelse af NemID med offentlig digital signatur til fysiske personer og til medarbejdere i juridiske enheder.

Kapitel 20

Færøerne og Grønland

§ 26. 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 grønlandske forhold tilsiger.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning
2. Lovforslagets hovedpunkter
 - 2.1. MitID og MitID-løsningen
 - 2.1.1. Gældende ret
 - 2.1.2. Finansministeriets overvejelser og den foreslåede ordning
 - 2.1.2.1 Tilrådighedsstillelse af MitID og MitID-løsningen
 - .
 - 2.1.2.2 Forvaltning
 - .
 - 2.2. NemLog-in
 - 2.2.1. Gældende ret
 - 2.2.2. Finansministeriets overvejelser og den foreslåede ordning
 - 2.2.2.1 Tilrådighedsstillelse af NemLog-in
 - .
 - 2.2.2.2 Forvaltning
 - .
 - 2.3. Behandling af personoplysninger
 - 2.3.1. Gældende ret
 - 2.3.2. Finansministeriets overvejelser og den foreslåede ordning
 - 2.3.2.1 Behandling af personoplysninger og videregivelse af risikodata
 - .
 - 2.3.2.1. MitID og MitID-løsningen
 - 1.
 - 2.3.2.1. NemLog-in
 - 2.
 - 2.3.2.2 Dataansvar
 - .
3. Forholdet til databeskyttelsesforordningen og databeskyttelsesretten
4. De økonomiske konsekvenser og implementeringskonsekvenser for det offentlige
5. De økonomiske og administrative konsekvenser for erhvervslivet m.v.
6. De administrative konsekvenser for borgerne
7. De klima- og miljømæssige konsekvenser
8. Forholdet til EU-retten
9. Hørte myndigheder og organisationer m.v.
10. Sammenfattende skema

1. Indledning

Danmark er langt fremme inden for offentlig digitalisering, og har over de seneste år udviklet en unik offentlig digital infrastruktur med en meget høj udbredelse og anvendelse. I takt hermed får den offentlige nationale it-infrastruktur en stadig større rolle i dagligdagen for danskerne, idet den bidrager til at skabe en effektiv offentlig og privat sektor med værdi for privatpersoner og virksomheder. Centrale dele af

den offentlige nationale infrastruktur udgøres af de fællesoffentlige it-systemer NemID og NemLog-in, der sammen udgør rammen for adgang til offentlige digitale selvbetjeningsløsninger. Lovens formål er at skabe rammen for de næste generationer af disse digitale infrastrukturløsninger, hvor NemID bliver til MitID og NemLog-in bliver udviklet i en ny version. Det sker da kontrakterne med de eksisterende leverandører af NemID-løsningen og nuværende NemLog-in udløber i 2021/2022. MitID og NemLog-in vil ligesom NemID-løsningen og den nuværende NemLog-in være kritisk it-infrastruktur.

De digitale selvbetjeningsløsninger erstatter i dag en lang række opgaver, som f.eks. indgivelse af ansøgninger, indsendelse af dokumentation via sikker kommunikation med det offentlige, underskrivelse af aftaler mv., som tidligere kun kunne håndteres ved manuel sagsbehandling og ved privatpersonens eller virksomhedens fysiske fremmøde hos den relevante offentlige myndighed. Derfor er det af afgørende betydning for den offentlige og private sektor samt det danske samfund som helhed, at der eksisterer sikre identifikations- og autentifikationsløsninger, som er en forudsætning for den digitale forvaltning.

Det er en statslig myndighedsopgave at sikre åben og lige adgang for alle til den næste generation af de kritiske it-infrastrukturløsninger MitID og NemLog-in, og at sikre effektiv og sikker drift af disse centrale løsninger. MitID-løsningen og NemLog-in danner ramme for den offentlige digitale it-infrastruktur og sikrer opretholdelse af vitale samfundsmæssige funktioner, menneskers sikkerhed samt økonomiske- og sociale velfærd.

MitID vil ligesom NemID give privatpersoner, virksomheder, offentlige myndigheder, frivillige foreninger mv. adgang til at læse Digital Post fra offentlige afsendere samt give dem adgang til at anvende offentlige digitale selvbetjeningsløsninger. MitID-løsningen indebærer en central ændring i forhold til NemID-løsningen, fordi MitID-løsningen fremadrettet alene vil udgøre en autentifikationsløsning. NemID-løsningen indeholdt ud over autentificeringen også en digital signatur. Digital signering vil fremadrettet ske ved anvendelsen af serviceområdet Digital signering i NemLog-in-infrastrukturen.

Den nye version af NemLog-in vil styrke samspillet mellem digitale selvbetjeningsløsninger på tværs af den offentlige sektor og muliggøre sikker login og autentifikation, administration af erhvervsidentiteter, digital signering samt digital repræsentation. I den nye version af NemLog-in vil der blandt andet blive tilføjet den nye erhvervsidentitetsløsning MitID Erhverv, som erstatning for NemID til erhvervs- og medarbejdersignatur. Herudover vil der blive udviklet en ny samlet signeringsløsning baseret på nye signeringsstandarder samt givet adgang til, at private, der tilbyder digitale selvbetjeningsløsninger, fremover kan anvende dele af NemLog-in. NemLog-in vil efterleve kravene i National Standard for Identiteters Sikringsniveau (herefter NSIS). Standarden er i overensstemmelse med krav fra eIDAS-forordningen og definerer en national ramme for tilliden til digitale identiteter.

Formålet med lovforslaget er at fremtidssikre organiseringen af den myndighedsopgave, som udvikling og tilrådighedsstillelse af disse centrale og kritiske offentlige digitale infrastrukturløsninger udgør. Med et samlet statsligt ejerskab til og dataansvar for MitID-løsningen og NemLog-in, vil disse centrale løsninger løbende og effektivt kunne opdateres i takt med den teknologiske udvikling samt det skiftende digitale trusselsbillede i form af it-nedbrud og -angreb mv.

MitID-løsningen og NemLog-in er desuden omfattet af lokationskravet i lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (herefter databeskyttelsesloven) § 3, stk. 9, og bestemmelser udstedt i medfør heraf, at personoplysninger, der behandles i nærmere bestemte it-systemer, og som føres for den offentlige forvaltning, helt eller delvis alene må opbevares her i landet. Det fremgår af bekendtgørelse nr. 1104 af 30. juni 2020 om helt eller delvis opbevaring her i landet af personoplysninger, der behandles i nærmere bestemte it-systemer, og som føres for den offentlige forvaltning af bilag 1 liste over it-systemer, der skal føres her i landet som med MitID som nr. 2 og NemLog-in3 som nr. 4.

Det er vurderet, at der vil ske behandling af personoplysninger, som på grund af deres karakter eller omfang indebærer en risiko for statens sikkerhed, og it-systemerne skal derfor opbevares i Danmark.

Med lovforslaget foreslås det, at Digitaliseringsstyrelsen pålægges denne myndighedsopgave at tilrådgighedsstille MitID-løsningen og NemLog-in. Placeringen af denne opgave hos Digitaliseringsstyrelsen ligger inden for medlemsstaternes ret til at organisere deres forvaltning i medfør af Europa-Parlamentets og Rådets Forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (herefter eIDAS-forordningen).

Det foreslås, at offentlige myndigheder og offentligretlige organer forpligtes til at anvende MitID-løsningen og de centrale dele af NemLog-in, når de udbyder digitale selvbetjeningsløsninger vedrørende deres myndighedsopgaver, som kræver sikker autentifikation.

Formålet med lovforslaget er tillige at sikre det juridiske grundlag for offentlige myndigheders og offentligretlige organers generelle anvendelse af MitID-løsningen og NemLog-in, med henblik på at give en samlet og ensartet brugerrejse på tværs af den digitale offentlige sektor. Med lovforslaget foreslås det, at når offentlige myndigheder tilbyder selvbetjeningsløsninger, som ikke vedrører myndighedsopgaver eller kun kræver autentifikation på sikringsniveau lav, skal de have ret til at få leveret MitID-løsningen og NemLog-in af Digitaliseringsstyrelsen, hvis de følger de givne regler om tilslutning, der fastsættes i medfør af loven. Det foreslås endvidere, at juridiske enheder kan indgå aftale med Digitaliseringsstyrelsen om at anvende MitID-løsningen og NemLog-in, og at Digitaliseringsstyrelsen også i disse tilfælde er forpligtet til at stille ydelserne til rådighed. Dette giver bl.a. banker og andre virksomheder mulighed for at anvende MitID som autentifikation af brugere på samme måde, som NemID anvendes i dag til netbanker og andre selvbetjeningsløsninger.

Lovforslaget indeholder endvidere hjemmel til at styrke privatpersoners og virksomheders retsstilling gennem et klart retligt grundlag for forvaltningen af centrale løsninger til den fællesoffentlige digitale infrastruktur. Med lovforslaget fremsættes således forslag om, at finansministeren fastsætter nærmere regler om udstedelse, spærring og genåbning af MitID og erhvervsidentiteter i NemLog-in. Derved skabes en gennemsigtig retsstilling for privatpersoner og erhvervsbrugere, herunder om de betingelser, som skal overholdes for at benytte løsningerne.

Desuden indeholder lovforslaget bemyndigelsesbestemmelser, hvorefter finansministeren kan fastsætte nærmere regler om tilslutning til MitID-løsningen samt NemLog-in og dets enkelte serviceområder, opkrævning af gebyrer og tilsyn. Endvidere fremsættes der med lovforslaget klare rammer for dataansvaret.

2. Lovforslagets hovedpunkter

Finansministeriet vil med lovforslaget introducere en række tekniske ændringer til de gældende løsninger NemID og NemLog-in.

Der etableres for det første en ny ordning for erhvervsidentiteter. Hvor MitID er den nationale identitetsgarant for digitale privatidentiteter, etableres NemLog-in parallelt som den nationale identitetsgarant for digitale erhvervsidentiteter. Det betyder, at erhvervsidentiteter fremadrettet findes og oprettes i NemLog-in.

Hvor MitID er den nationale identitetsgarant for digitale identiteter til privatpersoner, etableres NemLog-in parallelt som den nationale identitetsgarant for digitale identiteter til erhvervsbrugere. Det betyder, at erhvervsbrugeres digitale identiteter fremadrettet registreres og oprettes i NemLog-in i serviceområdet Erhvervsadministration. Det er i serviceområdet Erhvervsadministration, at brugerorganisationer kan oprette og tildele erhvervsidentiteter til deres erhvervsbrugere. Brugerorganisationer kan både være offentlige myndigheder, offentligretlige organer eller juridiske enheder, som anvender digitale selvbetjeningsløsninger i erhvervsøjemed.

NemLog-in skal løbende kunne udvikles og tilpasses nye teknologier, ændringer i trusselsbilledet, skiftende slutbrugerbehov og potentielt nye lovgivningsmæssige krav. Det er Finansministeriets vurdering, at loven samt de kontrakter, der er indgået med leverandører af løsningerne, tager hånd om dette.

I modsætning til i dag, hvor det alene er muligt at knytte én identitet til ét specifikt elektronisk identifikationsmiddel, vil det for det andet fremadrettet være teknisk muligt at have en løs kobling mellem identiteter og elektroniske identifikationsmidler. Dette betyder, at det vil være muligt at anvende et MitID-identifikationsmiddel udstedt til en privatperson i sammenhæng med én eller flere erhvervsidentiteter. Herudover vil det være muligt at få udstedt et dedikeret elektronisk identifikationsmiddel til én eller flere erhvervsidentiteter. Det vil også være muligt at have en kombination af ovenstående, hvor der anvendes et MitID-identifikationsmiddel udstedt til en privatperson til én eller flere af personens erhvervsidentiteter samtidig med, at personen har ét eller flere dedikerede elektroniske identifikationsmidler til specifikke erhvervsidentiteter.

I modsætning til i dag, hvor der sker direkte henvendelse til leverandøren af NemID-løsningen for at blive tilsluttet, vil der for det tredje ske den ændring, at udbydere af digitale selvbetjeningsløsninger i fremtiden skal anvende en broker. Brokern fungerer som bindeled mellem tjenesteudbyderen og MitID-løsningen. NemLog-in er Digitaliseringsstyrelsens brokerydelse for MitID.

Ved brokermodellen skal tjenesteudbyderen ikke forholde sig til den tekniske integration til den bagvedliggende identitetsgarant (fx NemID eller MitID). I stedet skal tjenesteudbyderen koble op mod en simplere snitflade hos den valgte broker.

Det forventes, at der overordnet vil være tre kategorier af brokere, der vil betjene tjenesteudbydere i forskellige sektorer; 1) Den offentlige identitetsbroker NemLog-in, 2) brokere til pengeinstitutter og 3) kommercielle brokere til tjenesteudbydere fra andre dele af den private sektor.

2.1. MitID og MitID-løsningen

2.1.1. Gældende ret

NemID er reguleret i lov nr. 439 af 8. maj 2018 om udstedelse af NemID med offentlig digital signatur til fysiske personer og til medarbejdere i juridiske enheder (herefter NemID-loven).

NemID er borgeres og virksomheders sikre log-in til både offentlige og private selvbetjeningsløsninger. NemID blev lanceret den 1. juli 2010 til både privatpersoner og til erhvervsdrivende. Med NemID bruges det samme bruger-id og den samme adgangskode til både netbank, offentlige hjemmesider og en lang række private tjenester på nettet. Det forbedrer servicen i den offentlige sektor samtidig med, at effektiviteten øges.

NemID med offentlig digital signatur til fysiske personer samt NemID til medarbejdere i juridiske enheder (NemID) er blevet udbredt til det meste af befolkningen og til stort set alle virksomheder, offentlige myndigheder, frivillige foreninger mv. med et cvr-nummer. På mange offentlige digitale selvbetjeningsløsninger forudsættes det nu, at borgerne, virksomheder, offentlige myndigheder, frivillige foreninger mv. har og anvender NemID. Dette gælder blandt andet, når en borger eller virksomhed skal have adgang til at læse Digital Post fra offentlige afsendere, og når en borger eller virksomhed skal anvende offentlige digitale selvbetjeningsløsninger.

Loven regulerer administration og udstedelse af NemID samt betingelserne for at få udstedt NemID. Endvidere reguleres fysiske personers og medarbejdere i juridiske enheders adgang til at klage over afslag på udstedelse af NemID eller ved spærring af NemID. Loven indeholder desuden en hjemmel til, at ministeren for offentlig innovation, nu finansministeren, udpeger en privat virksomhed, der administrerer og træffer afgørelse om udstedelse af NemID med offentlig digital signatur til fysiske personer og til medarbejdere i juridiske enheder. Loven fastslår endvidere, at fysiske personer, der er fyldt 15 år og har et cpr-nummer, kan anmode om at få udstedt NemID til fysiske personer, og at juridiske enheder, der har

et cvr-nummer, kan anmode om at få udstedt NemID til medarbejdere i juridiske enheder. Loven sikrer dermed en klar lovgivningsmæssig ramme for pligter og rettigheder i forbindelse med administration og udstedelse af NemID.

Loven indeholder desuden en bemyndigelse til at fastsætte nærmere regler om administration af NemID, herunder regler om udstedelse og spærring og om håndtering af NemID. På baggrund af denne bemyndigelse fastsætter bekendtgørelse nr. 899 af 21. juni 2018 om udstedelse og spærring af NemID med offentlig digital signatur (herefter bekendtgørelse om NemID) de nærmere betingelser for udstedelse og spærring af NemID med offentlig digital signatur for henholdsvis fysiske personer, medarbejdere og juridiske enheder.

Derudover reguleres NemID i dag af en certifikatpolitik for OCES-personcertifikater og en certifikatpolitik for OCES-medarbejdercertifikater. OCES er betegnelsen for Offentlige Certifikater til Elektronisk Service. OCES-certifikatpolitikkerne administreres af Digitaliseringsstyrelsen. Certifikatpolitikken for OCES-personcertifikater og OCES-medarbejdercertifikater udgør i dag grundlaget for udstedelse af NemID til privatpersoner og erhvervsbrugere.

NemID reguleres også af aftaler mellem Nets DanID A/S og registreringsenheder. Registreringsenhederne varetager opgaven med udstedelse af NemID, fx fungerer borgerservicecentre og banker som registreringsenheder og er således beføjet til at udstede NemID. NemID reguleres desuden af aftaler mellem Nets DanID A/S og den enkelte fysiske person eller medarbejder, der har fået udstedt NemID. I disse aftaler reguleres blandt andet, hvordan håndteringen af NemID skal foregå for at hindre snyd og misbrug af NemID.

På en lang række områder er det et krav, at privatpersoner og erhvervsbrugere anvender NemID, når de skal tilgå offentlige digitale selvbetjeningsløsninger. I lovekendtgørelse nr. 801 af 13. juni 2016 om Digital Post fra offentlige afsendere med senere ændringer, er det fastsat, at fysiske personer, der er 15 år eller derover, og som har bopæl eller fast ophold i Danmark, obligatorisk skal tilsluttes Digital Post. Det er endvidere fastsat, at juridiske enheder med cvr-nummer skal tilsluttes Digital Post. En forudsætning for at kunne tilsluttes og tilgå Digital Post er, at den fysiske person har NemID med offentlig digital signatur til fysiske personer, og at den juridiske enhed har NemID til medarbejdere i juridiske enheder til mindst en medarbejder.

Der er indført obligatorisk digital selvbetjening (de såkaldte bølgelove) på en lang række offentlige områder som led i udmøntning af den fælles offentlige digitaliseringsstrategi (2011-2015) ved de fire samlelove om overgang til obligatorisk digital selvbetjening; lov nr. 558 af 18. juni 2012 (bølge 1), lov nr. 622 af 12. juni 2013 (bølge 2), lov nr. 552 af 2. juni 2014 (bølge 3) og lov nr. 742 af 1. juni 2015 (bølge 4).

De fire samlelove indfører i de fagspecifikke love stort set enslydende bestemmelser om, at de privatpersoner, der kan, skal anvende digital selvbetjening, når privatpersonen skal ansøge, anmelde eller anmode mv. om det konkrete forhold, som loven på det pågældende område omhandler. Når en privatperson skal tilgå en offentlig myndigheds digitale selvbetjeningsløsning, vil det oftest forudsætte anvendelse af NemID. Tilsvarende er der på en lang række områder indført obligatorisk digital selvbetjening for virksomheder. Det gælder eksempelvis på Erhvervsministeriets område, hvor blandt andet portalen Virk skal tilgås med NemID til medarbejdere i juridiske enheder.

Elektroniske signaturer, som også foreslås reguleret med lovforslaget, er reguleret af eIDAS-forordningen samt lov nr. 617 af 8. juni 2016 om supplerende bestemmelser til forordning om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked (herefter supplerende lov om eIDAS). Forordningen er nærmere beskrevet i afsnit 8.1.

2.1.2. Finansministeriets overvejelser og den foreslåede ordning

Kontrakten med Nets DanID A/S om NemID udløber, og det har således været nødvendigt for Finansministeriet at overveje videreførelsen af den digitale infrastruktur forbundet med NemID-løsningen.

Overvejelserne har ført til, at der igennem en udbudslignende proces blev oprettet et partnerskab mellem Digitaliseringsstyrelsen på vegne af staten, de danske regioner og kommuner, og FR I af 16. september 2015 A/S, et selskab under Finans Danmark, der er interesseorganisation for bank, realkredit, kapitalforvaltning, værdipapirhandel og investeringsfonde i Danmark. Partnerskabet har samarbejdet om, igennem et EU-udbud, at anskaffe og i fællesskab finansiere en for samfundet kritisk national identitets- og autentifikationsløsning. Partnerskabet har på den baggrund indgået kontrakt med den private virksomhed Nets DanID A/S, som leverandør af udvikling, drift, vedligeholdelse, support og videreudvikling af MitID-løsningen og MitID. Det fremgår af udbudsmaterialet, at den udbudte løsning etableres som en national eID-ordning, som alle offentlige myndigheder og offentligretlige organer kan forpligtes til at anvende ved lov.

Med de nye løsninger ændres infrastrukturen på nogle områder. Den del af NemID, som tidligere var rettet mod privatpersoner, bliver afløst af MitID. Den del af NemID, som tidligere var rettet mod erhvervsbrugere, udvikles som en del af den nye infrastruktur i NemLog-in. Etablering af den erhvervsrettede del i NemLog-in sker af hensyn til at opnå en smidigere og mere sammenhængende og fremtidssikret erhvervsløsning, der kan forbedre brugeroplevelsen særligt på erhvervsområdet. Den del af løsningen, som er rettet mod privatpersoner, fornys ligeledes med MitID.

MitID bliver den danske nationale eID-løsning og vil leve op til kravene i eIDAS-forordningen. Herudover vil MitID-løsningen fremadrettet alene udgøre en autentifikationsløsning, hvor NemID-løsningen udover autentifikation blandt andet også indeholdt digital signatur.

Digital signatur vil med den nye digitale infrastruktur fremadrettet ske ved anvendelsen af serviceområdet Digital signering i NemLog-in. Dette medfører, at hvor der tidligere var lighed mellem NemID og digital signatur, vil der fremadrettet skulle anvendes serviceområdet Digital signering til den digitale underskrift baseret på autentifikation med MitID. NemLog-in indeholder serviceområderne Autentifikation og log-in, Digital repræsentation, Digital signering og Erhvervsadministration. Serviceområder er således en betegnelse for en service som Digitaliseringsstyrelsen i NemLog-in kan tilrådighedsstille for offentlige myndigheder, offentligretlige organer og juridiske enheder.

Med introduktionen af de nye løsninger bliver det muligt at fortsætte udviklingen i retning af en mere fleksibel og fremtidssikret modulær arkitektur i den fællesoffentlige infrastruktur for digitale identiteter. Derudover er løsningerne baseret på fleksibilitet mellem identitet og tilkobling af identifikationsmidler, som særligt for erhvervsbrugere vil opleves som mere fleksibelt. En erhvervsbruger kan fx anvende et identifikationsmiddel til både erhvervsbrug og privatbrug, hvis identifikationsmidlet er koblet til både den private identitet og erhvervsidentiteten. I NemID er det påkrævet, at man skal have særskilte identifikationsmidler til hver identitet.

Med NemID-løsningen kan en tjenesteudbyder henvende sig til leverandøren af NemID-løsningen og blive tilsluttet løsningen. Tilslutningen muliggør implementering af NemID-løsningen til tjenesteudbyderens egen digitale løsning. MitID-løsningen vil fungere anderledes på dette punkt, idet en tjenesteudbyder i stedet skal anvende en broker, der fungerer som bindeled mellem tjenesteudbyderen og MitID-løsningen. I NSIS defineres det som en identitetsbroker, som formidler en autentificeret digital identitet til tredjeparter på baggrund af en autentifikation, der er verificeret af brokern selv eller eventuelt af en anden tredjepart. MitID-løsningen vil således være baseret på et brokerkoncept, som indebærer, at tjenesteudbydere i stedet for at tilgå MitID-løsningen direkte, tilgår løsningen gennem en broker. NemLog-in vil fungere som den fællesoffentlige broker for MitID og vil således være MitID-identitetsbroker.

Ud over den fællesoffentlige identitetsbroker, som omtalt ovenfor, vil der kunne være andre identitets-

brokere koblet til NemLog-in. En identitetsbroker koblet til NemLog-in skal være NSIS-anmeldt. En identitetsbroker koblet til NemLog-in vil kunne interagere med MitID-løsningen gennem NemLog-in og gennem tilkobling til NemLog-in formidle autentificerede identiteter. En MitID-identitetsbroker kan ligeledes formidle digitale identiteter fra en lokal identitetsgarant. En lokal identitetsgarant er en betroet udsteder af lokale elektroniske identiteter, der er associeret med en eller flere brugerorganisationer oprettet i serviceområdet Erhvervsadministration i NemLog-in. En lokal identitetsgarant muliggør blandt andet, at en juridisk enhed kan anvende egne lokale identiteter og identifikationsmidler sammen med erhvervsidentiteter i serviceområdet Erhvervsadministration i NemLog-in. I praksis vil etablering og drift som lokal identitetsgarant medføre, at den juridiske enhed selv kan håndtere følgende processer for deres egne erhvervsbrugere nemlig identitetssikring, udstedelse af lokale identiteter og identifikationsmidler samt autentifikation til lokale it-systemer.

Der eksisterer ikke i dag et marked af brokere, men der gives med loven mulighed for, at et sådant marked vil kunne opstå. Offentlige myndigheder, offentligretlige organer og juridiske enheder vil i henhold til loven således kunne indgå aftale med Digitaliseringsstyrelsen om anvendelse af MitID-løsningen både som tjenesteudbydere og som brokere.

Ved brokermodellen skal tjenesteudbyderen ikke forholde sig til den tekniske integration til den bagvedliggende identitetsgarant. I MitID infrastrukturen vil det dermed ikke længere være muligt for tjenesteudbydere at tilslutte sig MitID-løsningen direkte. I stedet vil de skulle have adgang igennem tilslutning til en certificeret MitID-identitetsbroker, der håndterer selve den tekniske integration til løsningen samt autentifikationsprocessen af slutbrugeren.

Finansministeren har med organiseringen af tilrådighedsstillelse af den kritiske fællesoffentlige digitale infrastruktur blandt andet lagt vægt på, at det i Danmark i overensstemmelse med eIDAS-forordningen er valgt at MitID skal være den nationale eID-ordning. Endvidere har sikkerheden, herunder forsynings-sikkerheden i disse digitale infrastrukturløsninger, hvoraf MitID-løsningen og NemLog-in udgør kernen, haft betydning i overvejelserne om organiseringen af tilrådighedsstillelse af den kritiske fællesoffentlige digitale infrastruktur. Det har også været et hensyn, at tilliden til anvendelsen af offentlige digitale selvbetjeningsløsninger i forbindelse med myndighedsopgaver ikke kompromitteres. Det er ud fra disse overvejelser og betragtninger en myndighedsopgave, at stille MitID-løsningen til rådighed for offentlige myndigheder og at sikre, at løsningen udvikles, vedligeholdes, driftes og forvaltes af Digitaliseringsstyrelsen. Af de samme grunde er det en myndighedsopgave for Digitaliseringsstyrelsen at stille MitID til rådighed for privatpersoner og erhvervsbrugere.

På den baggrund er det Finansministeriets vurdering, at loven skal forpligte offentlige myndigheder og offentligretlige organer til at anvende MitID-løsningen, når de giver privatpersoner og erhvervsbrugere adgang til digitale selvbetjeningsløsninger, som – når de udfører myndighedsopgaver – kræver sikker autentifikation.

Offentlige myndigheder og offentligretlige organer kan således vælge andre leverandører af digitale identiteter og identifikationsmidler til digitale selvbetjeningsløsninger, hvorfra der ikke udføres myndighedsopgaver, eller som alene kræver autentifikation på sikringsniveau lav. Offentlige myndigheder og offentligretlige organer kan anvende andre brokere end NemLog-in til at få adgang til MitID-løsningen i de tilfælde, hvor de ikke har pligt til at anskaffe løsningen fra Digitaliseringsstyrelsen.

Det er Finansministeriets vurdering, at det er i samfundets interesse, at markedet for digitale identiteter og elektroniske identifikationsmidler ikke lukkes for private leverandører i større omfang end nødvendigt. Derudover vil offentlige myndigheder og offentligretlige organer frit kunne vælge at anvende lokale identifikationsmidler. Tilslutningen til NemLog-in giver den lokale identitetsgarant mulighed for at knytte lokale identifikationsmidler til erhvervsidentiteterne i NemLog-in. En virksomhed vil således kunne tilknytte lokale identifikationsmidler til virksomhedens ansatte. Derved kan et lokalt identifikationsmiddel

anvendes til autentifikation internt hos den lokale identitetsgarant fx internt i en virksomhed og til autentifikation over for tjenesteudbydere tilsluttet en broker i NemLog-in.

MitID-løsningen skal løbende kunne udvikles og tilpasses nye teknologier, autentifikationsmetoder, ændringer i trusselsbilledet, skiftende slutbrugerbehov og potentielt nye lovgivningsmæssige krav. Det er Finansministeriets vurdering, at loven samt de kontrakter, der er indgået med leverandører til løsningerne, tager hånd om dette.

2.1.2.1. Tilrådighedsstillelse af MitID og MitID-løsningen

Med introduktion af MitID-løsningen og NemLog-in er det fra offentlig side hensigten at fortsætte udviklingen i retning af en mere fleksibel og fremtidssikret modulær arkitektur i den fællesoffentlige kritiske infrastruktur for digitale identiteter, signering og brugerrettighedsstyring.

For at varetage dette hensyn og for at opnå de øvrige formål, der ligger til grund for lovforslaget, foreslås det, at Digitaliseringsstyrelsen pålægges som myndighedsopgave at stille MitID-løsningen til rådighed for offentlige myndigheder og offentligretlige organer. Digitaliseringsstyrelsen pålægges tilsvarende at stille MitID til rådighed for privatpersoner og erhvervsbrugere.

Digitaliseringsstyrelsen har ansvaret for at implementere regeringens planer om øget digitalisering i den offentlige sektor. En fortsat og løbende modernisering af den fællesoffentlige digitale infrastruktur er med til at sikre, at den offentlige sektor kan levere en sikker og tidssvarende service, der lever op til privatpersoners, erhvervsbrugeres, offentlige myndigheders, offentligretlige organers og juridiske enheders forventninger om effektiv og sammenhængende offentlig digital service. Sikre digitale identiteter og dertil relaterede services er en forudsætning for, at den digitale offentlige forvaltning, derfor pålægges Digitaliseringsstyrelsen, herunder at loven medfører som myndighedsopgave at stille MitID-løsningen til rådighed på vegne af den danske stat for alle offentlige myndigheder og offentligretlige organer for at kunne realisere den fortsatte digitalisering af det danske samfund.

Digitaliseringsstyrelsen har derfor en særlig status som instrument og teknisk tjeneste for hele den offentlige sektor og skal imødekomme alle offentlige myndigheders og offentligretlige organers anmodning om tilslutning i overensstemmelse med denne lovs 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 anmodning om tilslutning i medfør af loven.

Når tilrådighedsstillelsen af ovenstående løsninger sker centralt som led i en myndighedsopgave, sikres grundlaget for en fællesoffentlig it-infrastruktur. Tilrådighedsstillelsen forudsætter, at Digitaliseringsstyrelsen sikrer udvikling, drift, vedligeholdelse og forvaltning af løsningerne. Forsyningen af de centrale it-infrastrukturløsninger er en forudsætning for, at den danske forvaltning følger med den teknologiske udvikling og kan møde privatpersoners og virksomheders behov for sikker digital identifikation og kommunikation med den offentlige sektor. For privatpersoner og erhvervsbrugere betyder dette, at de i mødet med de offentlige digitale selvbetjeningsløsninger vil opleve en ensartet, sikker og genkendelig brugerrejse på tværs af det offentlige digitale landskab.

Det er hensigten, at infrastrukturløsningerne skal være med til at effektivisere den offentlige sektor og sikre besparelser, da løsningerne giver privatpersoner og erhvervsbrugere mulighed for at betjene sig selv, i de tilfælde hvor sagsbehandling med fysisk fremmøde kan erstattes af digital sagsbehandling.

Offentlige myndigheders og offentligretlige organers anskaffelse af MitID-løsningen og NemLog-in fra Digitaliseringsstyrelsen foretages i medfør af loven og uden, at det for offentlige myndigheder og offentligretlige organer er muligt at forhandle om vilkår for løsningernes anvendelse og vederlag. Økonomien for løsningerne bygger på en model, som indebærer, at opkrævning af betaling for anvendelse af løsningerne altid reguleres efter de faktiske omkostninger ved løsningerne.

Offentlige myndigheder og offentligretlige organer, som udfører en myndighedsopgave, har en pligt til at anskaffe MitID-løsningen og serviceområderne Login og autentifikation og Digital repræsentation i NemLog-in fra Digitaliseringsstyrelsen, i det omfang deres digitale selvbetjeningsløsninger kræver sikker autentifikation. Anskaffelsespligten giver Digitaliseringsstyrelsen en eksklusiv rettighed og har til formål at sikre, at den offentlige orden og sikkerhed, herunder hensynet til de samfundsøkonomiske overvejelser om fælles anskaffelse af it-løsninger i staten. Offentlige myndigheders og offentligretlige organers pligt til at anskaffe MitID-løsningen og NemLog-in fra Digitaliseringsstyrelsen udbreder anvendelsen af MitID som elektronisk identifikationsløsning, hvilket sikrer kendskab til løsningen i det danske samfund. Kendskab til løsningerne er afgørende for brugen, sikkerheden og tilliden til den offentlige digitale selvbetjening, hvilket er en forudsætning for den offentlige orden. Hensynet til den offentlige sikkerhed varetages ligeledes gennem denne pligt, idet samlet statslig kontrol med samfundskritisk it-infrastruktur sikres. Herved vil MitID-løsningen og NemLog-in løbende og effektivt kunne opdateres i takt med den teknologiske udvikling samt et skiftende digitalt trusselsbillede. Større sikkerhed opnås således, når myndighederne forpligtes til at anvende disse it-infrastrukturløsninger.

Pligten til at anvende løsningerne er desuden med til at sikre en ensartet brugerrejse for privatpersoner og erhvervsbrugere, når privatpersoner og erhvervsbrugere skal foretage login og autentifikation i mange offentlige myndigheders digitale selvbetjeningsløsninger. På den måde vil privatpersoner og erhvervsbrugere opleve en genkendelighed, når de færdes på de forskellige digitale selvbetjeningsløsninger hos offentlige myndigheder.

For digitale selvbetjeningsløsninger, som enten ikke kræver sikker autentifikation eller ikke vedrører myndighedsopgaver, skaber loven en ret til, at offentlige myndigheder og offentligretlige organer kan anvende MitID-løsningen. Når offentlige myndigheder og offentligretlige organer har en ret til at anskaffe disse dele af MitID-løsningen fra Digitaliseringsstyrelsen, tilstræbes stor anvendelse af og udbredelse af eksisterende fællesoffentlig infrastruktur på tværs af offentlige digitale selvbetjeningsløsninger i stedet for, at enkeltmyndigheder anskaffer og anvender individuelle løsninger. Ligeledes er det i principperne for digitaliseringsklar lovgivning fastsat, at offentlige myndigheder i det omfang, det er muligt og hensigtsmæssigt, bør genbruge digital infrastruktur for derigennem at skabe sammenhæng for privatpersoner og virksomheder på tværs af den offentlige forvaltning.

Den foreslåede løsning indebærer således, at Digitaliseringsstyrelsen gives en eksklusiv rettighed, som omhandlet i § 17 i udbudsloven, lov nr. 1564 af 15. december 2015 (herefter udbudsloven), til at levere MitID-løsningen til offentlige myndigheder og offentligretlige organer, som pålægges pligt til at anvende løsningerne.

I de tilfælde hvor offentlige myndigheder og offentligretlige organer alene har ret til at aftage løsningerne af Digitaliseringsstyrelsen, er Digitaliseringsstyrelsen et instrument og en teknisk tjeneste for myndighederne. Digitaliseringsstyrelsen har således ikke frihed til at bestemme hvilke opgaver, den vil udføre eller til hvilken takst. 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 følger af loven, vil der ikke være tale om en gensidigt bebyrdende kontrakt, jf. udbudslovens § 24, nr. 24, og myndighederne kan således anskaffe løsningerne fra Digitaliseringsstyrelsen i medfør af loven, uden at skulle gennemføre et udbud, jf. også præambel betragtning nr. 5 og nr. 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). Der henvises i øvrigt til afsnit 2.1. og 2.2. nedenfor om de udbud, som Digitaliseringsstyrelsen har gennemført på vegne af hele den offentlige forvaltning ved løsningernes anskaffelse.

Det foreslås også, at Digitaliseringsstyrelsen pålægges at stille MitID-løsningen til rådighed for juridiske enheder. Lovforslaget giver således juridiske enheder en ret til, at disse efter aftale med Digitalise-

ringsstyrelsen kan anvende MitID-løsningen under overholdelse af de regler om tilrådighedsstillelse og anvendelse, som fastsættes af Digitaliseringsstyrelsen.

Ordningen kan for MitID-løsningen i oversigtsform illustreres som følger:

Sikringsniveauer	Offentlige myndigheder og offentligretlige organer, når de udfører en myndighedsopgave	Offentlige myndigheder og offentligretlige organer, når de ikke udfører en myndighedsopgave
Høj eller betydelig (sikker autentifikation)	Pligt	Ret
Lav	Ret	Ret

2.1.2.2. Forvaltning

Med den foreslåede § 4 sikrer Digitaliseringsstyrelsen at der sker identitetssikring af privatpersoner, registrering af identiteter, udstedelse, spærring og genåbning af MitID til privatpersoner efter reglerne fastsat i medfør af bestemmelsens stk. 2. Digitaliseringsstyrelsen sikrer endvidere udstedelse, spærring af identifikationsmidler til erhvervsbrugere efter reglerne fastsat i medfør af stk. 2.

Det foreslås i § 4, stk. 2, at der indføres hjemmel til at finansministeren fastsætter regler om forvaltningen af MitID-løsningen og MitID, herunder regler om udstedelse, suspension, spærring og genåbning af MitID og regler for indbringelse af klage over en afgørelse om udstedelse, suspension og spærring af MitID. Det forventes, at en klage over en afgørelse kan indbringes for Digitaliseringsstyrelsen efter genvurdering hos den registreringsenhed, der har truffet afgørelsen.

Finansministeren vil tillige kunne fastsætte regler med krav, der stilles til privatpersoner og erhvervsbrugere ved løbende håndtering af MitID.

Med en omstilling fra NemID til MitID vil der være en omstilling til en ny eID-løsning, som ikke længere indeholder det analoge identifikationsmiddel, nøglekortet. Med udfasning af nøglekortet følger der en tilvænnning til en ny løsning, som af nogle privatpersoner vil opleves som mere digital. Privatpersoner, som ikke ønsker at anvende MitID-appen som identifikationsmiddel, vil dog fortsat kunne vælge fysiske elektroniske identifikationsmidler, som afløser for nøglekortet.

Endvidere vil der være en høj grad af genkendelighed fra de eksisterende løsninger, hvilket forventeligt på sigt vil bringe antallet af klager fra privatpersoner på niveau med det nuværende antal klager. I den nye løsning reduceres risikoen for snyd med de fysiske og kopierbare nøglekort, hvilket ligeledes forventes at kunne nedbringe antallet af klager. Det vurderes, at lovforslaget indeholder et hjemmelsgrundlag, som sikrer mulighed for at fastsætte klare regler for privatpersoners retsstilling, og hvori det fastslås, at privatpersoner kan klage til Digitaliseringsstyrelsen over afslag på at få udstedt MitID mv.

MitID-løsningen er en ny løsning, og er derfor ikke lovreguleret i dag. Det forventes, at der videreføres regler fra lov om NemID med offentlige digital signatur, om udpegning af offentlige myndigheder, offentligretlige organer eller juridiske enheder til på vegne af Digitaliseringsstyrelsen at varetage opgaven med udvikling, drift, vedligeholdelse og forvaltning af MitID-løsningen.

Det fastslås i § 5 at Digitaliseringsstyrelsen kan udpege offentlige myndigheder, offentligretlige organer eller juridiske enheder til på vegne af Digitaliseringsstyrelsen at varetage opgaver efter § 3, stk. 1, 1. pkt., samt opgaver i medfør af § 4, stk. 1.

Det følger endvidere af bestemmelsens *stk. 2*, at kommunalbestyrelsen skal varetage opgaver på veg-

ne af Digitaliseringsstyrelsen. Dette betyder, at kommunerne forpligtes til at varetage opgaverne med registrering af identiteter, udstedelse, spærring og genåbning af MitID til privatpersoner. Disse opgaver varetages i dag i registreringsenheder, som findes i de fleste kommuner. Registreringsenheder findes i dag primært i forbindelse med kommunale borgerservicecentre.

Kommunerne skal sikre, at det fortsat er let tilgængeligt for privatpersoner at få hjælp til oprettelsen af MitID, fx ved at opgaverne placeres i kommunale borgerservicecentre eller lignende steder i kommunen.

2.2. NemLog-in

2.2.1. Gældende ret

NemLog-in er ikke lovreguleret i dag. Området er derimod reguleret kontraktuelt mellem Digitaliseringsstyrelsen og den private virksomhed NNIT A/S. I dag varetages opgaven med drift af NemLog-in af NNIT A/S.

NemLog-in varetager en central rolle i den nationale digitale infrastruktur, idet NemLog-in gør det muligt for privatpersoner og erhvervsbrugere at varetage opgaver i de offentlige digitale selvbetjeningsløsninger på en let måde, hvor der tidligere krævedes fysisk fremmøde hos fx kommunen. NemLog-in anvendes til at skabe sikker adgang til offentlige digitale selvbetjeningsløsninger.

Det fremgår af tekstanmærkning nr. 124, stk. 1 ad 07.12.02 til § 7 på finansloven fra 2020, at ministeren for offentlig innovation, nu finansministeren, bemyndiges til at indføre de myndigheder mv., der fremgår af bilag 1a, 1b og bilag 1c i bekendtgørelse nr. 1078 af 3. oktober 2014 om offentlige afsendere i Offentlig Digital Post og desuden domstolene, KL, Danske Regioner, Metroselskabet I/S, Udviklingselskabet By Havn I/S, Odense Letbane P/S og Aarhus Letbane I/S som parter i Digitaliseringsstyrelsens aftale med leverandøren af NemLog-in. Derudover fremgår det af tekstanmærkning nr. 124, stk. 2, at de offentlige myndigheder, selvejende institutioner mv. kan vælge at gøre brug af aftalen.

NemLog-in udgør således den løsning, som en privatperson eller en erhvervsbruger i dag mødes af, når de vil foretage et login på en offentlig digital selvbetjeningsløsning, som kræver autentifikation af privatpersonens eller erhvervsbrugerens digitale identitet. Her anvendes NemLog-in til at sikre autentifikation af privatpersonen eller erhvervsbrugeren, førend pågældende lukkes ind i den selvbetjeningsløsning, der ønskes adgang til. Samtidig muliggør NemLog-in, at privatpersoner og nogle erhvervsbrugere kan anvende den digitale repræsentationsløsning, såfremt de skal repræsentere andre digitalt eller lade sig repræsentere digitalt. Visse væsentlige funktioner i NemLog-in er alene tilgængelige for den offentlige sektor. En af disse er funktionen Single sign-on, som sikrer en ubrudt og sammenhængende brugerrejse på tværs af de offentlige løsninger, således at en privatperson eller en erhvervsbruger alene afkræves et enkelt login ved adgangen til flere tilsluttede offentlige selvbetjeningsløsninger.

2.2.2. Finansministeriets overvejelser og den foreslåede ordning

Kontrakten med NNIT A/S om NemLog-in udløber, og det har således været nødvendigt for Finansministeriet at overveje, hvordan den del af den digitale infrastruktur, som NemLog-in udgør, skal videreføres.

Overordnet har overvejelserne ført til, at NemLog-in videreføres i sin nuværende form, men der tilføjes ny funktionalitet samt sker tilpasninger til den eksisterende funktionalitet.

Digitaliseringsstyrelsen har på baggrund af et EU-udbud indgået kontrakt med den private virksomhed Nets DanID A/S som leverandør af udvikling og forvaltning af NemLog-in. Det fremgik af udbudsmaterialet, at den udbudte løsning fremover ville blive anvendt af de offentlige myndigheder, der var anført på vedlagte bilagslister, og alle øvrige myndigheder, som senere ved lov ville blive forpligtet til at anvende løsningen.

Derudover har Digitaliseringsstyrelsen på baggrund af et EU-udbud indgået kontrakt med NNIT A/S om driften af NemLog-in.

I forhold til ny funktionalitet, bliver de væsentligste tilføjelser, at der oprettes en ny erhvervsløsning i serviceområdet Erhvervsadministration, som er introduceret i afsnit 2 og som uddybes nedenfor i afsnit 2.2.2.1., i NemLog-in, som også vil blive kaldt MitID Erhverv. Dele af erhvervsløsningen har hidtil været en del af NemID-løsningen. Der vil hertil ske en opgradering af signeringsløsningen, som vil blive moderniseret i henhold til nye signeringsstandarder m.v., ligesom NemLog-in i fremtiden vil være certificeringscenter (CA), og varetage udstedelse af OCES-certifikater og kvalificerede certifikater på vegne af den danske stat. Nets DanID A/S varetager i dag opgaven som certificeringscenter. OCES-certifikater får en mere begrænset anvendelse, idet de tidligere certifikater for personer (POCES) og for systemer (FOCES) ikke vil fortsætte. Af hensyn til forsyningssikkerheden for private tjenesteudbydere vil der blive åbnet op for, at private tjenesteudbydere kan benytte dele af NemLog-in infrastrukturen, herunder serviceområdet Login og autentifikation i NemLog-in.

NemLog-in udgør et centralt element i den fællesoffentlige digitale infrastruktur og sikrer den fællesoffentlige brugerstyring, når privatpersoner og erhvervsbrugere skal have adgang til offentlige digitale selvbetjeningsløsninger. Finansministeren har i forbindelse med organiseringen af tilrådighedsstillelsen af den offentlige digitale kritiske infrastruktur haft overvejelser om sikkerheden, herunder forsyningssikkerheden i disse digitale løsninger, hvoraf MitID-løsningen og NemLog-in udgør kernen. Det er her væsentligt, at tilliden til anvendelsen af offentlige digitale selvbetjeningsløsninger i forbindelse med myndighedsopgaver ikke kompromitteres. Det er ud fra disse overvejelser og betragtninger en myndighedsopgave at stille NemLog-in til rådighed for offentlige myndigheder, offentligretlige organer og juridiske enheder samt at sikre udvikling, vedligeholdelse, drift og forvaltning af løsningen.

På den baggrund er det Finansministeriets vurdering, at loven skal forpligte offentlige myndigheder og offentligretlige organer til at anskaffe serviceområdet Login og autentifikation i NemLog-in fra Digitaliseringsstyrelsen, når de skal give privatpersoner og erhvervsbrugere adgang til digitale selvbetjeningsløsninger, der vedrører myndighedsopgaver og kræver sikker autentifikation. Endvidere er det Finansministerens vurdering, at det er i samfundets interesse, at markedet for autentifikation ikke lukkes for private leverandører i større omfang end nødvendigt. Således kan offentlige myndigheder og offentligretlige organer vælge andre leverandører af autentifikationsydelser til digitale selvbetjeningsløsninger, der ikke vedrører myndighedsopgaver, eller alene kræver autentifikation på sikringsniveau lav.

NemLog-in skal på sigt tillige kunne anvendes af private tjenesteudbydere, som skal kunne vælge at anvende NemLog-in, når de har en digital selvbetjeningsløsning, som kræver login.

NemLog-in vil således fremadrettet være den offentlige identitetsbroker for MitID. Det medfører, at offentlige tjenesteudbydere, som har behov for at kunne autentificere en fysisk persons digitale identitet eller en erhvervsbrugers digitale identitet, som udgangspunkt skal anvende NemLog-in som broker for MitID til deres digitale selvbetjeningsløsninger. NemLog-in vil også kunne anvendes af private tjenesteudbydere, som ønsker at tilgå sikker autentifikation gennem NemLog-in og ikke har en anden privat broker. Ved private tjenesteudbyderes brug af NemLog-in vil disse skulle indgå en aftale med Digitaliseringsstyrelsen herom og betale et vederlag for anvendelsen, der dækker Digitaliseringsstyrelsens omkostninger. Prisen vil være ikke-diskriminerende og skal sikre, at der ikke sker konkurrencefordrejning.

Serviceområdet Login og autentifikation er reguleret i § 8, stk. 2, nr. 1. Det håndterer NemLog-in autentifikation af brugeren over for fx MitID-løsningen, når brugeren vil logge på en digital selvbetjeningsløsning. Det betyder i praksis, at når en fysisk person eller en erhvervsbruger, som har fået udstedt en elektronisk identitet og et eller flere elektroniske identifikationsmidler, logger ind på en digital selvbetjeningsløsning, sender NemLog-in en digital autentifikationsanmodning til MitID-løsningen. Mi-

tID-løsningen sender herefter svar tilbage til NemLog-in, som videresender autentifikationssvaret til selvbetjeningsløsningen.

Hvor MitID er den nationale identitetsgarant for digitale identiteter til fysiske personer, etableres NemLog-in parallelt som den nationale identitetsgarant for digitale identiteter til erhvervsbrugere. Det betyder, at erhvervsbrugeres digitale identiteter fremadrettet findes og oprettes i NemLog-in i serviceområdet Erhvervsadministration. Det er i serviceområdet Erhvervsadministration, at brugerorganisationer kan oprette og tildele erhvervsidentiteter til deres erhvervsbrugere. Brugerorganisationer kan både være offentlige myndigheder, offentligretlige organer eller juridiske enheder, som anvender digitale selvbetjeningsløsninger i erhvervsøjemed.

NemLog-in skal løbende kunne udvikles og tilpasses nye teknologier, ændringer i trusselsbilledet, skiftende slutbrugerbehov og potentielt nye lovgivningsmæssige krav. Det er Finansministeriets vurdering, at loven samt de kontrakter, der er indgået med leverandører af løsningerne, tager hånd om dette.

2.2.2.1. Tilrådighedsstillelse af NemLog-in

Med introduktion af NemLog-in er det fra offentlig side hensigten at fortsætte udviklingen i retning af en mere fleksibel og fremtidssikret modulær arkitektur i den fællesoffentlige kritiske infrastruktur for digitale identiteter, signering og brugerrettighedsstyring.

For at varetage dette hensyn og for at opnå de øvrige formål, der ligger til grund for lovforslaget, foreslås det, at Digitaliseringsstyrelsen pålægges som myndighedsopgave at stille NemLog-in til rådighed for offentlige myndigheder og offentligretlige organer. Digitaliseringsstyrelsen pålægges tilsvarende at stille MitID til rådighed for privatpersoner og erhvervsbrugere, se desuden afsnittet herom ovenfor afsnit 2.1.2.1.

Digitaliseringsstyrelsen pålægges med loven som myndighedsopgave at stille NemLog-in til rådighed på vegne af den danske stat for alle offentlige myndigheder og offentligretlige organer for at kunne realisere digitaliseringen af det danske samfund. 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.

Når tilrådighedsstillelsen af NemLog-in sker centralt som led i en myndighedsopgave, sikres grundlaget for en fællesoffentlig it-infrastruktur. Tilrådighedsstillelsen forudsætter, at Digitaliseringsstyrelsen sikrer udvikling, drift, vedligeholdelse og forvaltning af løsningerne. Forsyningen af de centrale it-infrastruktur-løsninger er en forudsætning for, at den danske forvaltning følger med den teknologiske udvikling og kan møde privatpersoners og virksomheders behov for sikker digital identifikation og kommunikation med den offentlige sektor. For privatpersoner og erhvervsbrugere betyder dette, at de i mødet med de offentlige digitale selvbetjeningsløsninger vil opleve en ensartet, sikker og genkendelig brugerrejse på tværs af det offentlige digitale landskab.

Det er hensigten, at infrastrukturløsningerne skal være med til at effektivisere den offentlige sektor og sikre besparelser, da løsningerne giver privatpersoner og erhvervsbrugere mulighed for at betjene sig selv, i de tilfælde hvor sagsbehandling med fysisk fremmøde kan erstattes af digital sagsbehandling.

Offentlige myndigheders og offentligretlige organers anskaffelse NemLog-in fra Digitaliseringsstyrelsen foretages i medfør af loven og uden, at det for offentlige myndigheder og offentligretlige organer er muligt at forhandle om vilkår for løsningernes anvendelse og vederlag. Økonomien for løsningerne bygger på en model, som indebærer, at opkrævning af betaling for anvendelse af løsningerne altid reguleres efter de faktiske omkostninger ved løsningerne.

Offentlige myndigheder og offentligretlige organer, som udfører en myndighedsopgave, har en pligt til at anskaffe serviceområderne Login og autentifikation og Digital repræsentation i NemLog-in fra Digitaliseringsstyrelsen, i det omfang deres digitale selvbetjeningsløsninger kræver sikker autentifikation. Anskaffelsespligten 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 staten. Offentlige myndigheders og offentligretlige organers pligt til at anskaffe NemLog-in fra Digitaliseringsstyrelsen udbreder anvendelsen af MitID som elektronisk identifikationsløsning, hvilket sikrer kendskab til løsningen i det danske samfund. Kendskab til løsningerne er afgørende for brugen, sikkerheden og tilliden til den offentlige digitale selvbetjening, hvilket er en forudsætning for den offentlige orden. Hensynet til den offentlige sikkerhed varetages ligeledes gennem denne pligt, idet samlet statslig kontrol med samfundskritisk it-infrastruktur sikres. Herved vil MitID-løsningen og NemLog-in vil løbende og effektivt kunne opdateres i takt med den teknologiske udvikling samt et skiftende digitalt trusselsbillede. Større sikkerhed opnås således, når myndighederne forpligtes til at anvende denne it-infrastrukturløsning.

Pligten til at anvende løsningerne er desuden med til at sikre en ensartet brugerrejse for private personer og erhvervsbrugere, når private personer og erhvervsbrugere skal foretage login og autentifikation i mange offentlige myndigheders digitale selvbetjeningsløsninger. På den måde vil private personer og erhvervsbrugere opleve en genkendelighed, når de færdes på de forskellige digitale selvbetjeningsløsninger hos offentlige myndigheder.

For digitale selvbetjeningsløsninger, som enten ikke kræver sikker autentifikation eller ikke vedrører myndighedsopgaver, skaber loven en ret til, at offentlige myndigheder og offentligretlige organer kan anvende NemLog-in. Når offentlige myndigheder og offentligretlige organer har en ret til at anskaffe disse dele af NemLog-in fra Digitaliseringsstyrelsen, tilstræbes stor anvendelse af og udbredelse af eksisterende fællesoffentlig infrastruktur på tværs af offentlige digitale selvbetjeningsløsninger i stedet for, at enkeltmyndigheder anskaffer og anvender individuelle løsninger. Ligeledes er det i principperne for digitaliseringsklar lovgivning fastsat, at offentlige myndigheder i det omfang, det er muligt og hensigtsmæssigt, bør genbruge infrastruktur for derigennem at skabe sammenhæng for privatpersoner og virksomheder på tværs af den offentlige forvaltning.

Da NemLog-in indeholder flere forskellige serviceområder, er der en differentieret forpligtelse til at aftage de enkelte serviceområder fra Digitaliseringsstyrelsen.

For offentlige myndigheder og offentligretlige organer gælder der en pligt til at anvende serviceområdet Login og autentifikation, når de udfører en myndighedsopgave og deres selvbetjeningsløsning kræver sikker autentifikation. Kræver den pågældende selvbetjeningsløsning ikke sikker autentifikation eller anvendes den ikke til at udføre myndighedsopgaver, gælder der alene en ret for offentlige myndigheder og offentligretlige organer til at anvende serviceområdet Login og autentifikation. En offentlig myndighed eller et offentligretlig organ agerer i rollen som tjenesteudbyder, når de anvender serviceområdet Login og autentifikation i NemLog-in. I praksis betyder det, at den offentlige myndighed eller det offentligretlige organ tilbyder brugerne en adgang til deres digitale selvbetjeningsløsninger, hvor brugerne benytter sig af serviceområdet Login og autentifikation for at kunne tilgå selvbetjeningsløsningen.

For serviceområdet Digital repræsentation gælder der for offentlige myndigheder og offentligretlige organer en pligt til anvendelse, når de udfører myndighedsopgaver. Serviceområdet kan alene tilgås ved autentifikation på sikringsniveau betydelig eller høj. Når en offentlig myndighed eller et offentligretligt organ vil anvende serviceområdet Digital repræsentation, agerer de i rollen som tjenesteudbyder. Det indebærer i praksis, at en offentlig myndighed eller et offentligretligt organ skal tilbyde brugere af deres digitale selvbetjeningsløsninger at anvende Digital repræsentation. Digital repræsentation kan kun anvendes, hvor myndigheden eller det offentligretlige organ udfører en myndighedsopgave.

For serviceområdet Digital signering gælder der for offentlige myndigheder og offentligretlige orga-

ner en ret til anvendelsen. Serviceområdet kan alene tilgås ved sikker autentifikation. Det blev ved lovforslagets udarbejdelse overvejet at indføre en pligt for offentlige myndigheder og offentligretlige organer til at anvende serviceområdet Digital signering, når de udfører en myndighedsopgave. Da der imidlertid eksisterer et velfungerende marked for digitale signeringsløsninger, der efterlever gældende sikkerhedsstandarder, forslås det ud fra et proportionalitetshensyn alene at indføre en ret. Når en offentlig myndighed eller et offentligretligt organ vil anvende serviceområdet Digital signering, agerer de i rollen som tjenesteudbydere. Det indebærer i praksis, at en offentlig myndighed eller et offentligretligt organ kan tilbyde brugere af deres digitale selvbetjeningsløsninger at anvende Digital signering.

I forhold til serviceområdet Erhvervsadministration har offentlige myndigheder og offentligretlige organer en ret til at anvende dette serviceområde. Til forskel fra de andre serviceområder i NemLog-in agerer de som brugerorganisationer, når de anvender serviceområdet Erhvervsadministration. Offentlige myndigheder og offentligretlige organer udfører ikke myndighedsopgaver i rollen som brugerorganisation.

Den foreslåede løsning indebærer således, at Digitaliseringsstyrelsen gives en eksklusiv rettighed, som omhandlet i § 17 i udbudsloven, til at levere NemLog-in til offentlige myndigheder og offentligretlige organer, som pålægges pligt til at anvende løsningen.

I de tilfælde hvor offentlige myndigheder og offentligretlige organer alene har ret til at aftage løsningerne af Digitaliseringsstyrelsen, er Digitaliseringsstyrelsen et instrument og en teknisk tjeneste for myndighederne. Digitaliseringsstyrelsen har således ikke frihed til at bestemme, hvilke opgaver, den vil udføre eller til hvilken takst. 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 følger af loven, vil der ikke være tale om en gensidigt bebyrdende kontrakt, jf. udbudslovens § 24, nr. 24, og myndighederne kan således anskaffe løsningerne fra Digitaliseringsstyrelsen i medfør af loven, uden at skulle gennemføre et udbud, jf. også præambel betragtning nr. 5 og nr. 34 i udbudsdirektivet. Der henvises i øvrigt til afsnit 2.1.2. og 2.2.2. ovenfor om de udbud, som Digitaliseringsstyrelsen har gennemført på vegne af hele den offentlige forvaltning ved løsningernes anskaffelse.

Det foreslås også, at Digitaliseringsstyrelsen pålægges at stille NemLog-in til rådighed for juridiske enheder. Lovforslaget giver således juridiske enheder en ret til, at disse efter aftale med Digitaliseringsstyrelsen kan anvende NemLog-in under overholdelse af de regler om tilrådighedsstillelse og anvendelse, som fastsættes af Digitaliseringsstyrelsen.

Juridiske enheder har ingen forpligtelse i forhold til at anvende serviceområderne i NemLog-in, og omvendt har de heller ikke et retskrav på anvendelsen.

Ordningen kan i oversigtsform for NemLog-in for tjenesteudbydere illustreres som følger:

Serviceområder	Sikringsniveauer	Offentlige myndigheder og offentligretlige organer, når de udfører en myndighedsopgave	Offentlige myndigheder og offentligretlige organer, når de ikke udfører en myndighedsopgave
Login + autentifikation	Høj eller betydelig (sikker autentifikation)	Pligt	Ret

	Lav	Ret	Ret
Digital repræsentation	Høj eller betydelig (sikker autentifikation)	Pligt	N/a
Digital Signering	Høj eller betydelig (sikker autentifikation)	Ret	Ret

NemLog-in for brugerorganisationer:

Serviceområder	Sikringsniveauer	Offentlige myndigheder og offentligtretlige organer
Erhvervsadministration	Høj eller betydelig (sikker autentifikation)	Ret

2.2.2.2. Forvaltning

Med den foreslåede § 9, stk. 1, 1. pkt., sikrer Digitaliseringsstyrelsen, at der sker forvaltning af NemLog-in, herunder identitetssikring af offentlige myndigheder, offentligretlige organer og juridiske enheder, når de oprettes som brugerorganisationer i serviceområdet Erhvervsadministration i NemLog-in.

Når der oprettes en brugerorganisation i serviceområdet Erhvervsadministration sker der en registrering af, hvordan denne har identificeret sig og efter identitetssikring kan den oprettes som brugerorganisation i Erhvervsadministration.

Når offentlige myndigheder, offentligretlige organer og juridiske enheder er oprettet som brugerorganisation kan de efterfølgende benytte de funktioner, som er indeholdt i serviceområdet Erhvervsadministration.

Det indebærer, at den offentlige myndighed, det offentligretlige organ eller den juridiske enhed blandt andet kan tildele digitale identiteter til deres erhvervsbrugere, typisk medarbejdere, men også andre erhvervsbrugere, der har en tilknytning til den offentlige myndighed, det offentligretlige organ eller den juridiske enhed, jf. den foreslåede § 8, stk. 3.

Offentlige myndigheder, offentligretlige organer og juridiske enheder har ligeledes mulighed for at udstede og spærre erhvervsidentiteter til erhvervsbrugere tilknyttet til dem.

Digitaliseringsstyrelsen sikrer endvidere i medfør af § 9, stk. 1, 2. pkt., at brugerorganisationers adgang til serviceområdet Erhvervsadministration i NemLog-in samt erhvervsbrugeres digitale identiteter kan spærres og genåbnes efter reglerne fastsat i medfør af stk. 4.

Det er Digitaliseringsstyrelsens opgave at sikre, at brugerorganisationers adgang til Erhvervsadministration i NemLog-in samt erhvervsbrugeres digitale identiteter kan spærres og genåbnes.

De nærmere regler for identitetssikring af offentlige myndigheder, offentligretlige organer og juridiske enheder, når disse oprettes som brugerorganisationer i serviceområdet Erhvervsadministration og regler for spærring af erhvervsbrugeres digitale identiteter vil blive fastsat i regler med hjemmel i § 9, stk. 4.

I medfør af § 9, stk. 2. kan en privatperson, der skal registreres som erhvervsbruger i serviceområdet

Erhvervsadministration, anvende sit MitID, der er udstedt til privatbrug, til identitetssikring ved registreringen.

En erhvervsbruger kan således anvende sit MitID-identifikationsmiddel udstedt til privatbrug, til identitetssikring ved registreringen af en erhvervsidentitet. Herved sikres, at der kan ske en digital identitetssikring af privatpersonen i forbindelse med oprettelse af erhvervsidentiteten, inden denne kan agere som erhvervsbruger.

Identitetssikring af en erhvervsidentitet ved brug af et MitID-identifikationsmiddel udstedt til privatbrug, vil være muligt for både erhvervsbrugere i offentlige myndigheder, offentligretlige organer og juridiske enheder. Det vil endvidere være muligt for erhvervsbrugeren at anvende brugerorganisationens udstyr, eget udstyr eller en kombination af dette til at foretage identitetssikring af erhvervsidentiteten med MitID-identifikationsmidlet udstedt til privatbrug. Dette medfører, at identitetssikring fx kan ske fra vedkommendes egen mobil, computer eller tablet.

Derudover kan en lokal identitetsgarant, som er oprettet som brugerorganisation i NemLog-in, selv foretage identitetssikring. En lokal identitetsgarant fastsætter selv, hvordan der skal foretages identitetssikring i overensstemmelse med NSIS.

Bestemmelsen styrker en fælles høj tillid og sikkerhed på tværs af den offentlige og private sektor, ved at skabe fælles grundlag for sikker elektronisk interaktion mellem privatpersoner, juridiske enheder og offentlige myndigheder og derved øge effektiviteten i de offentlige og private digitale selvbetjeningsløsninger.

Med den foreslåede § 9, stk. 3, 1. pkt. kan en erhvervsbruger få tilknyttet sit elektroniske identifikationsmiddel, som er tilknyttet privatpersonens MitID-identitet, til sin erhvervsidentitet, således at erhvervsbrugeren kan anvende førnævnte identifikationsmiddel til at autentificere en eller flere erhvervsidentiteter.

Med bestemmelsen gøres det muligt for erhvervsbrugere, at anvende deres MitID-identifikationsmiddel udstedt til privatbrug, til at autentificere en eller flere erhvervsidentiteter.

Hvor bestemmelsens stk. 2, gør det muligt at identitetssikre en erhvervsidentitet med et MitID-identifikationsmiddel udstedt til privatbrug, i forbindelse med registreringen, sikrer stk. 3, at en erhvervsbruger løbende kan anvende deres private MitID-identifikationsmiddel til login og autentifikation af en erhvervsidentitet i forbindelse med login i selvbetjeningsløsninger.

§ 9, stk. 3, 2. pkt. indebærer, at tilknytningen af en erhvervsbrugers elektroniske identifikationsmiddel, som er tilknyttet privatpersonens MitID-identitet grundlæggende hviler på et princip om frivillighed. Det er således frivilligt for erhvervsbrugeren, om erhvervsbrugeren vil foretage en tilknytning af erhvervsbrugers elektroniske identifikationsmiddel, som er tildelt denne i regi af privatperson. En arbejdsgiver kan således ikke påtvinge sine medarbejdere denne tilknytning.

Ligeledes er tilknytningen også frivillig for brugerorganisationen. Dette indebærer, at en arbejderstager ikke kan påtvinge sin arbejdsgiver, at der skal ske en tilknytning af arbejderstagerens MitID-identitet, som er tildelt i privat regi.

I medfør af den foreslåede stk. 4 kan finansministeren fastsætter regler om forvaltning af NemLog-in, herunder regler for identitetssikring af brugerorganisationer, spærring og genåbning af erhvervsbrugers digitale identiteter og om adgang til at klage til Digitaliseringsstyrelsen over afgørelser truffet i medfør af disse regler.

2.3. Behandling af personoplysninger

2.3.1. Gældende ret

Det følger af den nugældende lov, at Nets DanID A/S er udpeget som udsteder af NemID på baggrund af et EU-udbud. Nets DanID A/S anses for dataansvarlig i forhold til administration af NemID-løsningen.

Digitaliseringsstyrelsen er for NemID kun dataansvarlig for personnummeret og PID/RID-nummeret. Nets er dataansvarlig for alle andre personoplysninger i NemID-løsningen.

Digitaliseringsstyrelsen er dataansvarlig for alle personoplysninger i NemLog-in-løsningen.

2.3.2. Finansministeriets overvejelser og den foreslåede ordning

2.3.2.1. Behandling af personoplysninger og videregivelse af risikodata

2.3.2.1.1. MitID og MitID-løsningen

For så vidt angår MitID-løsningen sker der behandling af personoplysninger i forbindelse med migrering fra NemID-løsningen til MitID-løsningen, ved nyudstedelse af MitID samt ved den løbende drift og forvaltning. Der sker ligeledes behandling af personoplysninger ved den enkelte fysiske persons anvendelse af sit MitID. Som en del af behandlingen indgår indhentning af oplysninger fra centrale offentlige registre som eksempelvis pas/kørekort registret, cpr-registret og Danmarks adresseregister. For en udførlig liste over legitimationsdokumenter, henvises der til regler fastsat i medfør af denne lovs § 4, stk. 2. Migrering, nyudstedelse og anvendelse af MitID sker på privatpersonens og erhvervsbrugerens eget initiativ.

Oplysninger om e-mailadresse og mobilnummer er ikke nødvendige for, at MitID kan udstedes, dog er mobilnummer en forudsætning for at kunne anvende MitID-app'en. E-mailadresse og mobilnummer er også en forudsætning for, at MitID-løsningen hurtigt kan udsende advisering til den pågældende indehaver af et MitID, hvis der indtræffer en hændelse, som det er vigtigt, at den pågældende hurtigt får besked om. Det kan for eksempel dreje sig om, at den pågældendes elektroniske identifikationsmiddel er blevet spærret. Den fysiske person vil derfor blive anmodet om at angive e-mailadresse og mobilnummer i forbindelse med udstedelse af MitID. I de følgende afsnit vil en fysisk person både omfatte en privatperson og en erhvervsbruger, der har fået udstedt et MitID.

Personoplysningerne i MitID-løsningen kan grupperes således: Identitetsdata, kontaktdata, registreringsdata, identitetsdokumentation, identifikationsmiddeldata, identifikationsmiddelhemmeligheder, identifikationsmiddelverifikationsdata, midlertidige autentifikationsdata, midlertidige registreringsdata, risikodata, logdata, faktureringsdata for transaktioner, faktureringsdata for elektroniske identifikationsmidler og betalingsdata.

De ovenfor anførte personoplysninger udgør tilsammen de personoplysninger, der er nødvendige for at skabe sikkerheden for, at en person er registreret og indrulleret korrekt, samt at denne korrekthed kan efterprøves ved personens efterfølgende anvendelse af sit MitID for at hindre misbrug.

Overgangen fra NemID-løsningen til MitID-løsningen vil i mange tilfælde basere sig på den privatpersons login med NemID. Det vil i disse tilfælde betyde, at en privatperson, der logger ind i sin netbank eller i mobilbank, eller på MitID.dk, med NemID, vil blive ledt igennem et flow, der fører til, at pågældende på baggrund af en validering med NemID bliver registreret i MitID-løsningen og får det dertilhørende MitID, som privatpersonen herefter kan anvende ved autentifikation. For at sikre at privatpersoner på den mest smidige måde bliver oprettet korrekt i MitID-løsningen, og med det rette sikringsniveau, anvendes NemID-løsningen til at validere identiteten på den pågældende privatperson.

Der indgår ikke behandling af biometriske data i MitID-løsningen. En fysisk persons anvendelse af ansigtsgenkendelse, fingeraftryk og lignende på egne fysiske enheder, herunder smartphones som led i autentifikationen med MitID-app'en, lagres ikke i MitID-løsningen og kræves ikke for at få udstedt MitID.

Dog vil hensynet til løbende at bevare løsningens høje sikkerhed kunne bevirke, at indsamling af biometriske data på et senere tidspunkt bliver relevant for at imødegå sikkerhedsmæssige trusler. Dette

kunne for eksempel være indsamling af tastemønstre, når personen anvender MitID med henblik på at kunne afvise forsøg på misbrug. Sådanne data vil i givet fald være en del af de risikodata, der indsamles om den enkelte person.

Biometriske data udgør følsomme personoplysninger, og omfattes af behandlingsforbuddet i databeskyttelsesforordningens art. 9, stk. 1, medmindre betingelserne for behandling efter artikel 9, stk. 2 litra a, c, d, e eller f er opfyldt.

Det er Finansministeriets vurdering, at den eventuelle behandling af biometriske oplysninger ikke kan henføres under disse hjemmelsbestemmelser, men vil skulle henføres under forordningens art. 9, stk. 2, litra b, g og h. Artikel 9, stk. 2, litra b, g og h giver under nærmere betingelser mulighed for behandling af følsomme personoplysninger, herunder biometriske data. Såfremt, man vurderer at betingelser i litra b, g eller h er til stede, vil en hjemmel kunne tilvejebringes ved lovhjemmel eller ved databeskyttelseslovens § 7, stk. 5. Bestemmelsen indebærer, at finansministeren efter forhandling med justitsministeren og inden for databeskyttelsesforordningens rammer kan fastsætte nærmere regler om behandling af personoplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1 uden for de i § 7, stk. 1-4 nævnte tilfælde. Der foreligger imidlertid ikke på nuværende tidspunkt et behov for indsamling af biometriske data. Såfremt behovet måtte opstå for at imødegå sikkerhedsrisici eller sikkerhedstrusler, kan der være behov for enten en lovændring af denne lov eller udstedelse af en bekendtgørelse i medfør af databeskyttelseslovens § 7, stk. 5.

Dog vurderer Finansministeriet, at indsamlingen af biometriske oplysninger også vil kunne ske med den eksisterende hjemmel i databeskyttelseslovens § 7, stk. 5. Det fremgår af bemærkningerne til bestemmelsen i databeskyttelsesloven, at bemyndigelsesbestemmelsen er tænkt anvendt i situationer, hvor det kan være vanskeligt på forhånd fuldstændigt at forudse behovet for at kunne behandle personoplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1. Det fremtidige trusselsbillede er uforudsigeligt og behovet for indsamling af biometriske data kan ikke forudses på nuværende tidspunkt, men det kan blive relevant at indhente biometriske data både ved udstedelse af MitID og ved løbende anvendelse heraf af hensyn til løsningens generelle sikkerhed, samt af hensyn til den enkelte MitID brugers sikkerhed mod misbrug af vedkommendes digitale identitet.

For til stadighed at opretholde løsningens sikkerhed, herunder at sikre mod misbrug af MitID, vil der i forbindelse med anvendelse af MitID blive indsamlet såkaldte risikodata til brug for vurdering af risikoen ved hver enkelt transaktion, der skal gennemføres. Det drejer sig blandt andet om følgende oplysninger: Lokation – GeoIP koordinater, Netværk – IP nummer, Device – Information om den anvendte mobiltelefon eller browser og Identitet – Information om identiteten og sidste anvendelse. Risikodata indsamles ved hvert enkelt login og videregives sammen med tidligere observerede risikodata fra et antal logins i autentifikationssvaret til den broker, der formidler autentifikation til en given selvbetjeningsløsning i forbindelse med login. Formålet er at give brokern, der modtager risikodata, mulighed for at vurdere og afgøre om risikodataene af sikkerhedsmæssige årsager skal umuliggøre login på den pågældende tjeneste. Hensynet til sikkerheden i MitID-løsningen kan tilsige, at nye typer af risikodata skal indsamles.

Digitaliseringsstyrelsen videregiver autentifikationssvar, herunder risikodata, til en broker. Brokern behandler svaret og har mulighed for at berige dette med egne data. Efter nærmere aftale med en given tjenesteudbyder, videreformidler brokern det behandlede autentifikationssvar til denne. Formålet med videregivelsen er, at risikoen for den enkelte og konkrete transaktion kan vurderes. Digitaliseringsstyrelsens videregivelse og brokernes formidling er de helt centrale elementer i, at MitID-løsningen fungerer efter sit formål. Det er derfor Finansministeriets vurdering, at videregivelse og behandling af autentifikationssvar ligger inden for rammerne af Digitaliseringsstyrelsens myndighedsudøvelse, jf. databeskyttelsesforordningens art. 6, stk. 1, litra e). Der henvises til de specielle bemærkninger til § 14.

Finansministeriet har i forbindelse med overvejelserne om videregivelse af risikodata overvejet om videregivelse af data er i overensstemmelse med dataminimeringsprincippet i databeskyttelsesforordningens

art. 5, stk. 1, litra c) herunder om videregivelse i form af en risikoscore ville opfylde formålet med videregivelsen.

Det er Finansministeriets vurdering, at formålet med videregivelsen ikke kan opfyldes med en videregivelse af en risikoscore, idet et enkelt risikoelement ville kunne påvirke en score på en u hensigtsmæssig måde.

2.3.2.1.2. NemLog-in

Rollen som central fællesoffentlig infrastrukturløsning, herunder fællesoffentlig broker, betyder, at NemLog-in behandler en række formålsbestemte personoplysninger.

Digitaliseringsstyrelsen har indgået kontrakt med henholdsvis Nets DanID A/S om udvikling, vedligeholdelse, support og videreudvikling af MitID og NNIT A/S om drift og support af NemLog-in. Nets DanID A/S og NNIT A/S agerer som databehandlere på vegne af Digitaliseringsstyrelsen og forestår den konkrete behandling af personoplysninger i NemLog-in.

Med udgangspunkt i specifikke serviceområder leverer NemLog-in en række services til privatpersoner og erhvervsbrugere, der sikrer, at tilsluttede digitale selvbetjeningsløsninger kan anvendes, og at sikker elektronisk kommunikation med MitID og udvalgte øvrige identifikationsmidler understøttes. Der henvises til bemærkningerne til denne lovs § 8 for en detaljeret gennemgang af serviceområderne i NemLog-in. Hvilke personoplysninger, som behandles i NemLog-in, afhænger af det enkelte serviceområde.

Ved levering af autentifikationssvaret i serviceområdet Login og autentifikation, behandler NemLog-in navn, mailadresse, eventuelt personnummer og identifikationsnummer på den elektroniske identitet (UUID). Hvis MitID anvendes sker behandling af slutbrugerens MitID-nummer samt risikodata relateret til autentifikationssvaret.

Af hensyn til løbende at kunne opretholde en høj grad af sikkerhed i NemLog-in og sikre mod misbrug kan NemLog-in ud over den behandling af risikodata, der foretages i tilknytning til MitID-løsningen, ligeledes foretage en særskilt behandling heraf med henblik på vurdering af risici ved handlinger i relation til den generelle brug af serviceområderne.

Ved autentifikation af erhvervsbrugere vil der herudover ske behandling af erhvervsidentiteten, herunder navnet på den juridiske enhed, som erhvervsbrugeren er associeret med, og eventuelt registrerede brugerrettigheder. Endelig behandles data om hvilken digital selvbetjeningsløsning, som den fysiske person eller erhvervsbrugeren autentificerer sig overfor.

I serviceområdet Erhvervsadministration behandles navn, personnummer, e-mailadresse, telefonnummer, virksomhedsnavn og tilknyttede rettigheder. Rettigheder omfatter både de interne systemrettigheder i serviceområdet Erhvervsadministration, rettigheder til anvendelse af specifikke digitale selvbetjeningsløsninger hos tjenesteudbydere og rettigheder til at repræsentere andre erhvervsbrugere. Der behandles ligeledes oplysninger om hvilke identifikationsmidler, der er udstedt til den pågældende erhvervsbruger, samt oplysninger om hvorvidt der er tilknyttet identifikationsmidler fra en lokal identitetsgarant.

I forbindelse med udstedelse af certifikater i serviceområdet Erhvervsadministration og serviceområdet Digital signering behandles oplysninger om hvilken privatperson eller erhvervsbruger, der har fået udstedt et bestemt certifikat. Oplysningerne omfatter blandt andet navn, e-mailadresse, personnummer, og hvis certifikatet udstedes til en erhvervsbruger, oplysninger om hvilken juridisk enhed, offentlig myndighed eller offentligt organ, som erhvervsbrugeren er associeret med.

Ved en privatperson eller en erhvervsbrugers afgivelse af en digital signatur i serviceområdet Digital signering behandles tillige oplysninger om hvilken tjenesteudbyder og digital selvbetjeningsløsning, der er afgivet en signatur til. Der behandles ingen oplysninger om indhold af de data, der signeres. I forbindelse med en efterfølgende validering af en digital signatur i serviceområdets valideringstjeneste, foretages der en kortvarig automatisk behandling i et sikret miljø af de data, der er underskrevet. Behand-

lingen sker med henblik på at kontrollere integriteten af de pågældende data ved at sammenligne disse i klartekst med den checksum/hash-værdi, der blev genereret på underskriftstidspunktet, og som er koblet til den digitale signatur. Alle data slettes, når den pågældende session er afsluttet ved meddelelse om resultatet af valideringen. Behandling af data i forbindelse med validering er særskilt reguleret i dette lovforslags § 14. Der henvises til de specielle bemærkninger hertil.

I serviceområdet Digital repræsentation behandles oplysninger om navn, personnummer og e-mailadresse på fuldmagtsgiver og fuldmagtstager. Det registreres ligeledes hvilke digitale selvbetjeningsløsninger, der er afgivet fuldmagt til. Et værgemål kan, som beskrevet i de specielle bemærkninger til § 8, stk. 2, danne grundlag for digital repræsentation. Der foretages dog i NemLog-in alene en registrering af, at den pågældende fuldmagt foreligger, samt eventuel dokumentation for fuldmagten, der måtte være indsendt af fuldmagtstager eller fuldmagtsgiver.

I det omfang juridiske enheder, offentlige myndigheder og offentligretlige organer benytter services med vederlag eller gebyr i NemLog-in, behandles ligeledes fakturerings- og betalingsdata med henblik på at sikre korrekt afregning. Der henvises til de specielle bemærkninger til § 15, stk. 2 og 3, for en nærmere beskrivelse af hvilke services, der er underlagt betaling.

Ligesom i MitID-løsningen indgår der ikke behandling af biometriske data. Dog vil hensynet til løsningens høje sikkerhed kunne medføre, at behandling af biometriske data på et senere tidspunkt bliver relevant for at imødegå sikkerhedsmæssige trusler. Der henvises til beskrivelsen af biometriske oplysninger ovenfor.

I forbindelse med overgangen fra den eksisterende erhvervsløsning og tilknyttede tjenester hos Nets DanID A/S til den NemLog-in løsning, som lovforslaget vedrører, sker der behandling af erhvervsbrugeres personoplysninger, herunder ved indhentning af oplysninger fra Nets DanID A/S. Dette omfatter navn, mailadresse, stilling, virksomhedsnavn og tilknyttede rettigheder, jf. nærmere ovenfor under beskrivelse af Erhvervsadministration i afsnit 2.2.2.1. Som en del af behandlingen indgår indhentning og validering af oplysninger fra cvr-registret og cpr-registret for at sikre, at erhvervsbrugernes oprettes med korrekte data. 2.3.2.2. Dataansvar

Med dette lovforslag bliver Digitaliseringsstyrelsen dataansvarlig for infrastrukturløsningerne MitID-løsningen og NemLog-in, idet Digitaliseringsstyrelsen bestemmer formål og afgør med hvilke hjælpemidler, der må foretages behandling af personoplysninger i begge infrastrukturløsninger. Det gælder i forbindelse med tilrådighedsstillelse af løsningerne for offentlige myndigheder, offentligretlige organer og juridiske enheder, jf. § 3 og § 8, herunder når Digitaliseringsstyrelsen sikrer udvikling, drift, vedligeholdelse og forvaltning af løsningerne i medfør af § 4, § 5, stk. 2, § 9 og § 10.

Dataansvaret er omfattet af reglerne i den til enhver tid gældende databeskyttelseslovgivning i Danmark, databeskyttelsesforordningen og databeskyttelsesloven.

Begrebet dataansvarlig skal forstås i overensstemmelsen med databeskyttelsesforordningens artikel 4, nr. 7, der er defineret som en, "(...) der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger".

Det fremgår af databeskyttelsesforordningens artikel 24, stk. 1, at den dataansvarliges ansvar indebærer en "(...) hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder [som] gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning. "

Som følge af Digitaliseringsstyrelsens pligt til at tilrådighedsstille infrastrukturløsningerne MitID-løsningen og NemLog-in, er det således Digitaliseringsstyrelsen, der alene afgør til hvilket formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger. Digitaliseringsstyrelsen bliver

derfor i medfør af databeskyttelsesforordningen art. 4, nr. 7 anses som dataansvarlig for infrastrukturløsningerne.

Digitaliseringsstyrelsen får således ansvaret for at sikre, at infrastrukturløsningerne lever op til de sikkerhedskrav, der i databeskyttelsesforordningen stilles til behandling af personoplysninger samt de øvrige forpligtelser, der efter databeskyttelsesforordningen påhviler den dataansvarlige, herunder oplysningspligt over for de registrerede privatpersoner og erhvervsbrugere, om hvilke oplysninger, der behandles.

De personoplysninger, der indsamles i forbindelse med oprettelse af MitID og senere, når MitID anvendes, er almindelige personoplysninger, som fx navn, adresse, personnummer, eller lignende. De almindelige personoplysninger er nødvendige for at sikre identiteten af en privatperson eller erhvervsbruger både ved oprettelse og senere anvendelse af deres MitID.

Digitaliseringsstyrelsen vil behandle personoplysninger i form af navn, adresse, personnumre, cvr-numre eller lignende i forbindelse med tilrådighedsstillelse af løsningerne for offentlige myndigheder, offentligtretlige organer og juridiske enheder, jf. § 3 og § 8, herunder når Digitaliseringsstyrelsen sikrer udvikling, drift, vedligeholdelse og forvaltning af løsningerne i medfør af § 4, § 5, stk. 2, § 9 og § 10.

Det er nødvendigt for Digitaliseringsstyrelsen og i overensstemmelse med formålet, at behandle personoplysningerne, for at sikre infrastrukturløsningernes sikkerhed og integriteten af de udstedte elektroniske identifikationsmidler til privatpersoner MitID og erhvervsbrugere MitID Erhverv. Herunder for at kunne sikre, at en privatpersons identitet registreres og valideres korrekt, er det nødvendigt at behandle personoplysninger om vedkommende.

Digitaliseringsstyrelsen foretager identitetssikring af de privatpersoner og erhvervsbrugere, der bliver registreret i MitID-løsningen.

Digitaliseringsstyrelsens behandlingshjemmel til behandling af navn, adresse og cvr-nummer eller lignende er databeskyttelsesforordningens artikel 6, stk. 1, litra e, og for personnummer er behandlingshjemlen databeskyttelseslovens § 11, stk. 1. Behandlingshjemlen for at behandle følsomme personoplysninger i medfør af § 15 er artikel 9, stk. 2, litra g.

For så vidt angår MitID-løsningen sker anskaffelse af løsningen sammen med de danske pengeinstitutter, jf. de almindelige bemærkninger afsnit 2.1.2. Henset til, at MitID-løsningen er den danske nationale eID-ordning, der skal anmeldes til EU-kommissionen, og idet der med loven pålægges Digitaliseringsstyrelsen et myndighedsansvar for MitID-løsningen, påhviler dataansvaret for MitID-løsningen alene Digitaliseringsstyrelsen.

Der er indgået kontrakt med Nets DanID A/S om udvikling, drift, vedligehold og forvaltning af MitID-løsningen. Den behandling af personoplysninger, der finder sted hos Nets DanID A/S, udføres således af Nets DanID A/S, som databehandler for Digitaliseringsstyrelsen.

Når en privatperson og en erhvervsbruger ønsker at få udstedt et MitID, indsamler og registrerer registreringsenhederne personoplysninger om den privatpersonen og erhvervsbrugeren. For erhvervsbrugere sker indsamlingen i regi af NemLog-in. De oplysninger som en virksomhed indfører om sine ansatte vil dermed fremgå af NemLog-in.

Denne indsamling sker på vegne af Digitaliseringsstyrelsen som dataansvarlig. Registreringsenheder og supportenheder indgår en aftale om varetagelsen af registreringsopgaven hhv. supportopgaver med Nets DanID A/S på vegne af Digitaliseringsstyrelsen. Aftalen fastlægger blandt andet krav til overholdelse af sikkerhed, uddannelse samt krav om revision og afgivelse af årlig revisionserklæring. Den del af aftalen, som vedrører behandling af personoplysninger, er særskilt reguleret i en underdatabehandleraftale. Registreringsenhederne og supportenhederne anses derfor som underdatabehandlere til Nets DanID A/S, der er databehandler for Digitaliseringsstyrelsen i MitID-løsningen.

En certificeret broker i MitID-løsningen skal indgå en aftale med Nets DanID A/S på vegne af Digitaliseringsstyrelsen, for at blive tilsluttet MitID-løsningen. Aftalen fastlægger blandt andet krav til overhol-

delse af sikkerhed, certificering samt krav om revision og afgivelse af årlig revisionserklæring. Hvis en broker ikke overholder aftalen, kan brokerens adgang til MitID-løsningen i særligt alvorlige tilfælde lukkes.

En broker i MitID-løsningen, som tilsluttes løsningen, har en rolle som formidler af adgang til MitID-løsningen, således at en fysisk person kan autentificere sig over for en tjenesteudbyder. I den forbindelse indsamler MitID-løsningen autentifikationsdata på vegne af Digitaliseringsstyrelsen om den privatperson, der autentificerer sig. Som led i sikkerheden for, at det er den rigtige privatperson, der anvender sit MitID, indsamles desuden risikodata fra brokieren til MitID-løsningen. I disse tilfælde er det af tekniske årsager brokieren, der indsamler risikodata og autentifikationsdata på vegne af Digitaliseringsstyrelsen til MitID-løsningen. I denne sammenhæng er brokieren underdatabehandler efter indgåelse af en databehandlaftale med for Nets DanID A/S, der er databehandler for Digitaliseringsstyrelsen.

Når brokieren derimod modtager oplysninger fra MitID-løsningen bliver denne selvstændigt dataansvarlig for viderebehandlingen af disse personoplysninger.

Digitaliseringsstyrelsen er dataansvarlig for personoplysninger der behandles i serviceområdet Erhvervsadministration, herunder for registrering af erhvervsbrugere og administratorer samt personoplysninger ved oprettelse af juridiske enheder som brugerorganisationer i serviceområdet Erhvervsadministration i NemLog-in.

3. Forholdet til databeskyttelsesforordningen og databeskyttelsesretten

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 lov nr. 502 af 23. maj 2018 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.

Databeskyttelsesforordningen og databeskyttelsesloven gælder dog bl.a. ikke for behandling af personoplysninger, som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter, jf. forordningens artikel 2, stk. 2, litra c.

I databeskyttelsesforordningens kapitel II findes de relevante bestemmelser om, hvornår personoplysninger må behandles, herunder indsamle, udveksles og viderebehandles. Det følger af forordningens artikel 6, stk. 1, at behandling af almindelige personoplysninger kun er lovlig, hvis og i det omfang mindst ét af de i bestemmelsen nævnte forhold gør sig gældende, herunder hvis behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige, eller hvis behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlige myndighedsudøvelse, som den dataansvarlige har fået pålagt. Efter databeskyttelsesforordningens artikel 6, stk. 2 og 3, er det desuden muligt at opretholde og indføre mere specifikke bestemmelser for at tilpasse anvendelsen af artikel 6, stk. 1, litra c og e.

Det følger desuden af databeskyttelsesforordningens artikel 9, stk. 1, at behandling af følsomme personoplysninger som udgangspunkt er forbudt. Efter bestemmelserne i artikel 9, stk. 2, kan der gøres undtagelse til forbuddet i stk. 1. Det kan f.eks. ske, 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, jf. forordningens artikel 9, stk. 2, litra g. Dette er også tilfældet, hvis behandling er

nødvendig af hensyn til samfundsinteresser på folkesundhedsområdet, f.eks. beskyttelse mod alvorlige grænseoverskridende sundhedsrisici eller sikring af høje kvalitets- og sikkerhedsstandarder for sundhedspleje og lægemidler eller medicinsk udstyr på grundlag af EU-retten eller medlemsstaternes nationale ret, som fastsætter passende og specifikke foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder, navnlig tavshedspligt, jf. forordningens artikel 9, stk. 2, litra i. Det bemærkes, at behandling af følsomme oplysninger også kræver hjemmel i forordningens artikel 6, stk. 1.

De grundlæggende principper i forordningens artikel 5 skal altid iagttages. Det følger bl.a. heraf, at personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (lovlighed, rimelighed og gennemsigtighed), jf. forordningens artikel 5, stk. 1, litra a. Endvidere skal personoplysninger indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål (formålsbegrænsning), jf. forordningens artikel 5, stk. 1, litra b. Herudover skal personoplysninger være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (dataminimering), jf. forordningens artikel 5, stk. 1, litra c.

Finansministeriet vurderer, at Digitaliseringsstyrelsens behandling af de almindelige personoplysninger, kan henføres under databeskyttelsesforordningens art. 6, stk. 1, litra e om offentlig myndighedsudøvelse, idet behandlingen sker for, at Digitaliseringsstyrelsen kan varetage den pligt til tilrådighedsstillelse og forvaltning af MitID-løsningen og NemLog-in, som lovforslaget pålægger Digitaliseringsstyrelsen.

Det foreslås i § 13, at Digitaliseringsstyrelsen i stk. 1, ved en privatpersons anvendelse af MitID eller en erhvervsbrugers anvendelse af det elektroniske identifikationsmiddel i MitID til login og autentifikation, kan videregive autentifikations svar, herunder risikodata vedrørende den konkrete og enkelte transaktion, til en broker, der er tilsluttet MitID-løsningen eller NemLog-in.

Det foreslås desuden i § 13, stk. 2, at en broker kan foretage automatiske afgørelser om log-in på baggrund af risikodata videregivet efter stk. 1.

Det foreslås endvidere i § 13, stk. 3, at en broker, der i medfør af stk. 1 har modtaget autentifikations svar, kan videregive det modtagne og behandlede autentifikations svar til en tjenesteudbyder, der modtager autentifikationer fra MitID-løsningen.

Det foreslås også i § 13, stk. 4, at Digitaliseringsstyrelsen ved en erhvervsbrugers anvendelse af et elektronisk identifikationsmiddel fra en lokal identitetsgarant tilsluttet NemLog-in, kan videregive autentifikations svar vedrørende den konkrete og enkelte transaktion til en broker, der er tilsluttet NemLog-in.

Det foreslås endeligt i § 13, stk. 5, at en broker, der i medfør af stk. 4 har modtaget autentifikations svar, kan videregive det modtagne og behandlede autentifikations svar til en tjenesteudbyder, der gennem en broker, modtager autentifikationer fra NemLog-in.

Det foreslås i § 14, at Digitaliseringsstyrelsen kortvarigt og i et sikret teknisk miljø kan behandle følsomme personoplysninger, i forbindelse med validering af digitale signaturer i valideringstjenesten i serviceområdet Digital signering.

Den behandling af personoplysninger, der vil kunne finde sted på baggrund af de pågældende regler, vil skulle ske inden for rammerne af databeskyttelsesreglerne.

Som også nævnt ovenfor er det efter databeskyttelsesforordningens artikel 6, stk. 2 og 3, muligt at opretholde og indføre mere specifikke bestemmelser for at tilpasse anvendelsen i forbindelse med artikel 6, stk. 1, litra c eller e.

Behandlingen af almindelige personoplysninger, som kan ske i medfør af de regler, som fastsættes i de foreslåede bestemmelser i § 13 og 14, vurderes at have hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra e, idet behandlingen vil være nødvendig af hensyn til opgaver i samfundets interesse.

Det vurderes, at det er i overensstemmelse med databeskyttelsesforordningen og dennes rammer for fastsættelse af nationale særregler om behandling af personoplysninger at indføre de med lovforslaget

foreslåede bestemmelser. Det er fx forudsat at såfremt behandlingen er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til en medlemsstats generelle samfundsinteresser, kan der indføres særregler, der præciserer og varetager de opgaver som Digitaliseringsstyrelsens behandling af personoplysninger indebærer for at sikre den samfundsmæssige it-infrastruktur på tværs af såvel offentlige myndigheder, offentligretlige organer og juridiske enheder som MitID og NemLog-in muliggør.

Vurderingen af lovforslaget har taget udgangspunkt i de kriterier, som fremgår af betænkning nr. 1565 om databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning i forhold til indførelse af nye nationale særregler for behandling af ikke-følsomme personoplysninger, jf. betænkning nr. 1565, del I – bind 1, side 168 ff.

Der vurderes desuden, at der vil kunne ske en behandling af særlige kategorier af personoplysninger i medfør af de pågældende bestemmelser. Det vurderes, at der med lovforslaget er hjemmel hertil, idet behandlingen af personoplysninger vil være nødvendig af hensyn til væsentlige samfundsinteresser, jf. databeskyttelsesforordningens artikel 9, stk. 1, litra g.

Det følger af forordningens artikel 9, stk. 2, litra g, at der i forbindelse med fastsættelsen af nationale regler skal tages hensyn til det væsentligste indhold af retten til databeskyttelse, og at der skal sikres passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser. Det bemærkes i den forbindelse, at de pågældende bestemmelser skal sikre, at identiteten på en privatpersons anvendelse af MitID eller en erhvervsbrugers anvendelse af MitID Erhverv er den samme, som også fik udstedt det elektroniske identifikationsmiddel i § 13. Herunder ved kortvarigt og i et sikret teknisk miljø at behandle følsomme personoplysninger, for at sikre at de elektroniske identifikationsmidler, der indgår i MitID-løsningen bruges af den samme privatperson eller erhvervsburger, der har fået udstedt identifikationsmidlet. MitID-løsningen og NemLog-in udgør samfundskritisk digital infrastruktur, der er med til at holde Danmark i gang, især også efter den øgede brug af digitale selvbetjeningsløsninger under COVID-19 krisen.

Det følger i den forbindelse af databeskyttelseslovens § 11, stk. 1, at offentlige myndigheder kan behandle oplysninger om personnummer med henblik på en entydig identifikation eller som journalnummer.

Finansministeriet har overvejet behovet for selvstændige hjemler til regulering af det materielle indhold af de foreslåede bestemmelser i §§ 13 og 14.

Det er Finansministeriets vurdering, at begge bestemmelser kan fastsættes i medfør af databeskyttelsesforordningens artikel 6, stk. 2 og stk. 3, jf. artikel 9, stk. 2, litra g for så vidt angår lovforslagets § 14.

Finansministeriet har endvidere overvejet, om bestemmelsernes materielle indhold allerede er hjemlet gennem den myndighedsudøvelse, som Digitaliseringsstyrelsen pålægges med lovforslaget. Videregivelse af autentifikationssvar, jf. § 13, herunder en brokers videreformidling er en helt central forudsætning for, at MitID-løsningen kan fungere efter sit formål. Det er endvidere et nødvendigt led i en tidssvarende signeringstjeneste, at der kan ske en automatisk og maskinel verifikation af sikring mod ændringer, jf. § 8, stk. 2, nr. 3 og § 14. Det vurderes derfor, at de foreslåede bestemmelser kan henføres under Digitaliseringsstyrelsens myndighedsudøvelse.

Finansministeriets videre overvejelser har imidlertid ført til, at det er fundet hensigtsmæssigt at indføre bestemmelserne i de foreslåede §§ 13 og 14 af hensyn til at sikre gennemsigtighed i forhold til de aktører, der direkte omfattes af bestemmelserne, herunder hensynet til gennemsigtighed for de registrerede samt nødvendigheden i at sikre, at det er de samme privatpersoner og erhvervsbrugere, der benytter MitID ved løbende log-in og autentifikationer. Dette er især nødvendigt og proportionalt, idet MitID-løsningen og NemLog-in udgør samfundskritisk digital infrastruktur, som man skal kunne stole på uanset om man er en offentlig myndighed, en juridisk enhed eller en MitID bruger.

4. De økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Lovforslaget indebærer økonomiske konsekvenser for det offentlige, idet det udgør lovhjemmel til implementering og drift af næste generation af statens it-infrastrukturløsninger, MitID-løsningen og Nem-Log-in. Omkostningerne til udvikling af MitID-løsningen deles ligeligt mellem FR I og Digitaliseringsstyrelsen. Driften af MitID-løsningen finansieres af de transaktioner, der foretages gennem anvendelse af løsningen.

Af den fællesoffentlige finansiering af drift og udvikling, finansierer staten 40 procent, kommunerne 40 procent og regionerne 20 procent. Budgettet for løsningerne er forelagt Folketingets finansudvalg og således også medtaget på budgettet for finansloven 2020. Udvikling og drift af løsningerne er senest blevet fastlagt mellem parterne i Aftale om kommunernes og regionernes økonomi for 2020.

De samlede projektkomkostninger til udbud og udvikling af de kommende løsninger forventes at udgøre 661,1 mio. kr. i perioden 2014-2022, heraf 169,3 mio. kr. i 2014-2019. Driftsomkostningerne for de to løsninger forventes efter endt idriftsættelse at udgøre ca. 84 mio. kr. årligt. Det bemærkes, at omkostningsniveauet afhænger af anvendelsen af løsningerne, da der afregnes delvist transaktionsbaseret for både udgifter og indtægter.

Den tekniske omstilling til de kommende løsninger forventes for hele den offentlige sektor at udgøre i størrelsesordenen 50-130 mio. kr. Det understreges, at der er tale om et estimat, idet omstillingsopgaven og de relaterede omkostninger er genstand for løbende analyse. Det er aftalt ved økonomiforhandlingerne med kommuner og regioner, at omstillingsomkostninger, herunder både tekniske, organisatoriske og andre omstillingsomkostninger, afholdes decentralt. Omstillingsomkostninger dækker blandt andet tilpasning af lokale it-løsninger, kompetenceudvikling af medarbejdere samt intern omstilling og udarbejdelse af nye processer.

I omstillingsperioden vil infrastrukturløsningerne NemID og nuværende NemLog-in være understøttet samtidig med MitID og det nye NemLog-in, hvilket resulterer i midlertidigt overlappende driftsomkostninger. Det er ved lovforslagets fremsættelse ikke endeligt besluttet, hvornår de ældre infrastrukturløsninger udfases. Beslutning om udfasningen af NemID og NemLog-in er blandt andet afhængig af, hvor hurtigt privatpersoner og virksomheder overgår fra de gamle løsninger til de nye løsninger.

Herudover indeholder lovforslagets § 15 bemyndigelse til, at finansministeren kan fastsætte regler for opkrævning af vederlag for tilslutning og anvendelse af MitID-løsningen og NemLog-in. De nærmere regler om opkrævning af gebyrer hos privatpersoner for registrering og udstedelse af MitID vil blive fastsat i bekendtgørelse i medfør af § 15, stk. 1. Fra idriftsættelse af MitID-løsningen er det hensigten at fastsætte regler om, at en privatperson gebyrfrit kan få op til tre MitID-identifikationsmidler, det bemærkes dog, at gebyrfrihed ikke gælder ved anskaffelse af identifikationsmiddel ved sikringsniveau høj som privatperson, der henvises i øvrigt til de specielle bemærkninger til § 15, stk. 3. Ud over de tre MitID-identifikationsmidler er det tiltænkt, at MitID-appen kan anvendes som MitID-identifikationsmiddel uden brugerbetaling.

Digitaliseringsstyrelsen vil med lovforslaget fortsat skulle behandle klager og træffe afgørelse, hvis privatpersoner klager over, at deres MitID er blevet spærret eller suspenderet eller over et afslag på udstedelse af MitID. Klageadgangen sikres med en hjemmel fastsat i en bekendtgørelse, som forventes at indeholde rammerne for forvaltningen af MitID. Ligeledes fastsættes en hjemmel til at etablere en klageadgang for serviceområdet Erhvervsadministration i NemLog-in. Klageadgangen gælder for myndigheder og juridiske enheder i rollen som brugerorganisationer, der fx ikke kan blive oprettet i serviceområdet Erhvervsadministration i NemLog-in.

For så vidt angår NemID har Nets DanID A/S over for Digitaliseringsstyrelsen oplyst, at de erfaringsmæssigt modtager mellem 20-25 klager om året om udstedelse, spærring og genåbning af NemID. Ho-

vedparten håndteres ved simpel information samt oplysning om, at der kan klages til Digitaliseringsstyrelsen.

Digitaliseringsstyrelsen modtager cirka 20-30 klager om året. Det er vurderingen, at bestemmelserne om klageadgang til Digitaliseringsstyrelsen ikke vil medføre øget administration i form af flere klager. Det forventes, at antallet af klager kan stige kortvarigt i implementeringsperioden for de nye løsninger, idet privatpersoner og erhvervsbrugere skal skifte til de nye infrastrukturløsninger. Dog vurderes det, at de økonomiske konsekvenser efter fuld migrering til løsningerne vil blive reduceret, så offentlige myndigheder fremadrettet ikke får øgede administrative opgaver. Ændringerne for erhvervsbrugere indebærer, at der muligvis i implementeringsperioden kan forventes flere klager på grund af den omstilling, som erhvervsbrugere skal gennemgå. På sigt forventes det, at klageantallet reduceres til samme niveau, som i dag, idet erhvervsbrugere i de nye løsninger vil have adgang til mindst de samme funktioner som i de eksisterende løsninger.

Lovforslaget vurderes at leve op til de syv principper for digitaliseringsklar lovgivning og har været i høring i Digitaliseringsstyrelsens sekretariat for digitaliseringsklar lovgivning. Idet lovforslaget udgør lovhjemlen for næste generation af centrale dele af statens fællesoffentlige digitale infrastruktur, der muliggør digital selvbetjening, sagsbehandling mv., anses lovforslaget som værende af central betydning for digitaliseringen af den offentlige sektor som helhed, og dermed afgørende for realiseringen af princip nr. 6 om anvendelse af offentlig digital infrastruktur.

5. De økonomiske og administrative konsekvenser for erhvervslivet mv.

Lovforslaget har væsentlige økonomiske og administrative konsekvenser for erhvervslivet.

5.1. Administrative konsekvenser for erhvervslivet

Et udkast til lovforslaget har været forelagt Erhvervsstyrelsens Område for Bedre Regulering (OBR), der vurderer, at lovforslaget medfører væsentlige administrative konsekvenser for erhvervslivet. De administrative konsekvenser består dels i løbende administrative lettelser som følge af én samlet og simplere administration af erhvervsidentiteter, identifikationsmidler, rettighedsstyring og certifikater. Dertil vil den nye infrastruktur muliggøre en simplere og mere fleksibel model, hvor erhvervsbrugere kan anvende deres private MitID, dedikeret MitID eller identifikationsmidler udstedt af en lokal identitetsgarant i sammenhæng med en eller flere erhvervsidentiteter. Nedenfor er de administrative konsekvenser beskrevet, samt estimeret i det omfang det har været muligt.

Det vurderes, at der er betydelige administrative konsekvenser forbundet med, at erhvervsbrugere i juridiske enheder fremadrettet kan få tildelt og administrere deres digitale erhvervsidentiteter gennem serviceområdet Erhvervsadministration i NemLog-in. Der lægges i vurderingen særligt vægt på, at processen for oprettelse og administration af erhvervsidentiteter fremover forsimples, og at der skabes en bedre og mere sammenhængende løsning for erhvervsbrugere.

De administrative byrder og lettelser for erhvervslivet er senest estimeret i 2017, og dermed før afslutningen af udbuddene af de næste generationer af de digitale infrastrukturløsninger MitID og NemLog-in, som omfattes af denne lov. Det medfører, at estimererne af de administrative konsekvenser, som fremgår af dette afsnit, er forbundet med en vis usikkerhed. Der vil blive foretaget en ex-post måling af de administrative konsekvenser.

De overordnede områder som vil lette administrationsbyrden for erhvervsbrugere i medfør af det nye serviceområde Erhvervsadministration i NemLog-in er følgende:

5.1.1. En samlet tilslutning og administration

Med videreudviklingen af NemLog-in vil det blive lettere for en juridisk enhed at tilslutte sig serviceområdet Erhvervsadministration som brugerorganisation og efterfølgende administrere brugerorganisatio-

nens opsætning. Én samlet aftaleindgåelse muliggør blandt andet, at en tegningsberettiget for en juridisk enhed kan indgå én samlet aftale om anvendelse af de serviceområder, som udstilles gennem MitID-løsningen og NemLog-in til brugerorganisationer, samt om administration af tilslutning og oprettelse i næste generation Digital Post. Aftalen vil efterfølgende kunne administreres i takt med, at den juridiske enheds behov ændrer sig. Det vurderes, at én samlet aftaleindgåelse vil medføre administrative lettelser på ca. 71 mio. kr. årligt. Det understreges, at beregningen også inkluderer næste generation Digital Post og dermed ikke er begrænset til løsningerne, der reguleres i dette lovforslag.

Ved tilslutning til serviceområdet Erhvervsadministration bliver det muligt at differentiere i de juridiske enheders overordnede behov. Små og mellemstore juridiske enheder vil fx kunne vælge en simpel opsætning, så ikke al funktionalitet, som udbydes af NemLog-in, udstilles i serviceområdet Erhvervsadministration. Herimod vil juridiske enheder med avancerede behov kunne detailspecificere ønsket funktionalitet i tilslutningsforløbet. I begge tilfælde vil en brugerorganisation efterfølgende kunne ændre opsætningen, hvis den juridiske enheds forhold og behov ændrer sig.

5.1.2. En samlet og mere brugervenlig Erhvervsadministration

MitID-løsningen og NemLog-in vil som nye digitale infrastrukturløsninger blandt andet føre til lettelser for erhvervslivet som følge af ændringer i tidsforbruget ved oprettelse og administration af erhvervsidentiteter, identifikationsmidler, certifikater og rettighedsstyring for erhvervsbrugere gennem serviceområdet Erhvervsadministration i NemLog-in, idet tilsluttede brugerorganisationer fremover vil kunne tilgå og administrere væsentlige forhold igennem én applikation frem for flere.

Serviceområdet Erhvervsadministration udvikles med fokus på brugervenlighed med et let forståeligt design, med let tilgængelig hjælp og med vejledning af brugeren i applikationen. Designet af applikationen imødekommer også it-udfordrede brugere eller brugere med forskellige typer handicap.

Ændringen i tidsforbrug som følge af samling af funktionalitet omkring erhvervsidentiteter og rettighedsstyring vurderes at være ca. 10 minutter pr. oprettelse for den normaleffektive juridiske enhed. Der oprettes ca. 600.000 erhvervsidentiteter årligt. De løbende administrative lettelser for juridiske enheder vurderes på den baggrund at udgøre ca. 34 mio. kr. årligt.

Ved overgang til det nye serviceområde Erhvervsadministration vil brugerorganisationer have brug for tid til at lære den nye løsning at kende. Tidsforbruget ved ibrugtagning forventes at udgøre ca. 30 minutter for den normal-effektive juridiske enhed. Det forventes, at knap 500.000 juridiske enheder skal omstille sig til at anvende det nye serviceområde Erhvervsadministration. På den baggrund vurderes de samlede administrative omstillingsomkostninger ved omstilling til serviceområdet Erhvervsadministration, herunder erhvervsidentiteter, identifikationsmidler, certifikater og rettighedsstyring til ca. 85 mio. kr.

5.1.3. Fleksibel anvendelse af identifikationsmidler

I det nye serviceområde Erhvervsadministration har brugerorganisationer og deres erhvervsbrugere mulighed for at tilknytte og anvende forskellige typer identifikationsmidler til oprettede erhvervsidentiteter. Det bliver muligt at anvende 1) MitID-identifikationsmidler udstedt til privatpersoner, såfremt den juridiske enhed og privatpersonen giver samtykke til dette, 2) dedikerede MitID-identifikationsmidler til erhvervsbrug med mulighed for at anvende disse på vegne af flere juridiske enheder og 3) lokale identifikationsmidler til erhvervsbrugere tilknyttet en lokal identitetsgarant. Samlet set giver dette en langt større fleksibilitet og administrativ lettelse for erhvervsbrugere. Endvidere er det vurderingen, at sikkerheden for erhvervsidentiteter øges betragteligt.

Med MitID-løsningen bliver det også muligt for de juridiske enheder, som i dag anvender NemID-medarbejdersignatur eller nøglekort, at overgå til en erhvervsrettet mobilløsning i lighed med NemID-nøgleappen til privatpersoner. Denne mulighed kan opsættes i serviceområdet Erhvervsadministration i NemLog-in. Det forventes for disse juridiske enheder at give en reduktion i tidsforbrug på tre minutter

pr. login. Der foretages årligt ca. 4,06 mio. NemID logins hos erhvervsbrugerne med nøglekort, og det forventes, at 70 pct. af disse fremover vil foregå med MitID-appen. På den baggrund vurderes det, at den nye loginfunktion vil medføre løbende administrative lettelser for erhvervslivet på ca. 48 mio. kr. årligt.

Juridiske enheder, som ønsker at overgå til en MitID-appen, vil have en omstillingsomkostning forbundet hermed. Omstillingen består i at få opsat og at lære at bruge mobilløsningen. Mange privatpersoner er allerede overgået til brug af NemID-mobilløsningen, og det må forventes, at denne gruppe vil få lavere tidsforbrug til at lære at anvende den nye mobile MitID-loginløsning. I 2016 havde 523.080 juridiske enheder oprettet i gennemsnit fire medarbejdersignaturer. Af disse havde ca. 37 pct. tilknyttet et nøglekort, og 70 pct. af dem forventes at overgå til mobilløsning. Det bemærkes, at nogle af disse medarbejdersignaturer kan være tilknyttet samme erhvervsbruger, men at det ikke har været muligt at tage højde herfor i estimatet af de administrative konsekvenser. På den baggrund vurderes omstillingsomkostningerne ved ibrugtagning af MitID-appen til mellem 4 mio. kr. og 59 mio. kr.

5.1.4. Omstillingsomkostninger til MitID

Med lovforslaget om MitID vil der være omkostninger til migrering for samtlige juridiske enheder, når de skal overgå til de nye løsninger. Hver juridisk enhed vil skulle anvende 5-30 min. på at migrere til de nye løsninger, og den enkelte erhvervsbruger vil derefter skulle bruge 5-15 min. på at opsætte deres nye loginmiddel. Omstillingsomkostningerne hertil forventes at udgøre ca. 97 mio. kr. – 195 mio. kr.

Lovforslaget vurderes foreløbigt at medføre administrative omstillingskonsekvenser for erhvervslivet for mellem 186 mio. kr. - 339 mio. kr., samt løbende administrative lettelser på ca. 153 mio. kr. årligt.

5.2. Øvrige økonomiske konsekvenser for erhvervslivet

Derudover vurderes lovforslaget at medføre økonomiske konsekvenser for erhvervslivet i form af gebyrer for anvendelse af serviceområderne i NemLog-in og autentifikationstransaktioner i MitID-løsningen. Gebyrer, der opkræves fra juridiske enheder, skal dække Digitaliseringsstyrelsens omkostninger, være ikkediskriminerende og skal sikre, at der ikke sker konkurrencefordrejning. Gebyrerne vil blive fastsat på bekendtgørelsesniveau. Se nærmere herom i lovforslagets specielle bemærkninger til § 15.

5.3. Principper for agil erhvervsrettet regulering

MitID og Nemlog-in lovgivning og de underliggende løsninger skaber en it-infrastruktur i Danmark, som i høj grad understøtter de fem principper for agil erhvervsrettet regulering.

5.3.1. Muliggør anvendelse af nye forretningsmodeller

Det er Digitaliseringsstyrelsens vurdering, at lovforslaget bidrager til, at nye forretningsmodeller kan realiseres, idet både MitID-løsningen og NemLog-in opdateres.

5.3.1.1. eIDAS-forordningen

Det forventes, at serviceområdet Digital signering i NemLog-in vil opnå status som en kvalificeret tillidstjeneste i henhold til eIDAS-forordningens art. 21, stk. 2. Kvalificerede digitale signaturer skal, jf. eIDAS-forordningens art. 25, sidestilles med håndskrevne underskrifter i samtlige EU-stater. At serviceområdet Digital signering opnår status som en kvalificeret tillidstjeneste, betyder, at erhvervsbrugere såvel som privatpersoner ved anvendelse af serviceområdet Digital signering opnår en ensartet retstilstand på tværs af EU, hvilket forbedrer mulighederne for elektronisk forretningsførelse og elektronisk handel i EU.

5.3.1.2. Broker-model

Et andet aspekt, der muliggør nye forretningsmodeller, er MitID-brokermodellen. MitID-brokermodellen giver fremadrettet mulighed for, at juridiske enheder kan udvikle og anvende brokerløsninger til

private tjenesteudbydere. I dag implementerer en tjenesteudbyder NemID-løsningen ved henvendelse til leverandøren af NemID-løsningen, som gennem en tilslutning muliggør implementering af NemID-løsningen til tjenesteudbyderens egen selvbetjeningsløsning.

MitID-løsningen vil fungere anderledes på dette punkt, idet en tjenesteudbyder i stedet skal anvende en broker, der fungerer som bindeled mellem tjenesteudbyderen og MitID-løsningen. Broker-modellen medfører, at juridiske enheder skal tilslutte sig MitID-løsningen gennem en broker. En broker er en formidler af autentifikationer fra MitID-løsningen og til den enkelte juridiske enhed. Brokern er en juridisk enhed, der skal gennemgå en certificering for at blive broker. Brokern vil gøre det lettere for juridiske enheder, der udbyder digitale selvbetjeningsløsninger, at benytte MitID-løsningen, fordi brokern varetager den tekniske tilslutning til MitID-løsningen. Det vil for en juridisk enhed, der udbyder digitale selvbetjeningsløsninger, blive en mindre opgave at tilslutte sig en broker end at implementere en log-in løsning direkte i egne systemer. Det vil i forlængelse heraf kun være brokerne, der skal forholde sig til ændringer i MitID-snitfladerne. Indførelsen af brokere vil dermed medføre betydelige administrative lettelser for erhvervslivet, når juridiske enheder benytter MitID-løsningen til kontakt med den offentlige sektor. Der vil også være løbende byrder i form af betalinger for brokerns ydelser og omstillingsomkostninger i forbindelse med overgangen fra NemID-løsningen til MitID-løsningen. Der eksisterer ikke i dag et marked af brokere, men implementeringen af MitID-løsningen åbner op for, at et sådant marked vil kunne opstå. Juridiske enheder vil i henhold til lovforslaget således kunne indgå aftale med en certificeret broker.

Mens NemLog-in vil varetage rollen som offentlig broker, vil juridiske enheder kunne udvikle brokerløsninger til pengeinstitutter samt til tjenesteudbydere i andre dele af den private sektor. For mere herom, henvises der til lovforslagets almindelige bemærkninger afsnit 2.2.1.

5.3.1.3. Differentierede muligheder som lokal identitetsgarant

Med lovforslaget får juridiske enheder mulighed for at etablere sig som lokal identitetsgarant og tilslutte denne til NemLog-in. En lokal identitetsgarant muliggør blandt andet, at en juridisk enhed kan anvende egne lokale identiteter og identifikationsmidler sammen med erhvervsidentiteter i serviceområdet Erhvervsadministration i NemLog-in.

I praksis vil etablering og drift som lokal identitetsgarant medføre, at den juridiske enhed selv kan håndtere følgende processer for deres egne erhvervsbrugere: Identitetssikring, udstedelse af lokale identiteter og identifikationsmidler samt autentifikation til lokale it-systemer.

Det forventes, at få juridiske enheder vil etablere sig som lokale identitetsgaranter, idet det kræver teknisk kapacitet og investering.

Dette lovforslag regulerer ikke forholdene for lokale identitetsgaranter, men sikrer alene at lokale identitetsgaranter, som overholder gældende standarder, kan tilslutte sig NemLog-in.

5.3.2. Mere enkel og formålsbestemt

Lovforslaget har et klart fokus på at stille løsninger til rådighed for offentlige myndigheder og juridiske enheder. Der er udelukkende fremført detaljerede og specifikke krav og beskrivelser i det omfang, at det tjener lovforslagets formål og privatpersoners beskyttelse. Konkrete beskrivelser af løsningerne tjener i høj grad til at gøre løsningernes muligheder og anvendelse klar. Når løsningerne bliver beskrevet præcist, giver det juridiske enheder bedre betingelser for at udvikle andre løsninger, som kan fungere enten sammen med eller på tværs af MitID og NemLog-in. Det tekniske omfang af løsningerne, der bliver stillet til rådighed ved denne lov, skal fremgå klart for juridiske enheder.

Det er håndteret i lovforslaget ved, at tilrådighedsstillelsen af de enkelte løsninger reguleres efter hver sin bestemmelse og kapitel. Kapitlerne for hver løsning, henholdsvis MitID-løsningen og NemLog-in, indledes med en bestemmelse om tilrådighedsstillelse af løsningerne, og i de specielle bemærkningerne er

der beskrivelser af den nærmere regulering af løsningerne. Herudover er tilrådgivelsesstillelse af NemLog-in inddelt i de serviceområder, som NemLog-in indeholder.

5.3.3. Teknologineutral

Juridiske enheder forpligtes ikke til at anvende lovforslagets løsninger. Det er Digitaliseringsstyrelsens vurdering, at lovforslaget er teknologineutralt, og at juridiske enheder fremadrettet kan følge med den teknologiske udvikling af lovens omfattede løsninger.

5.3.4. Helhedstænkende

Digitaliseringsstyrelsen vurderer, at lovforslaget er i tråd med andre relevante reguleringsområder og ikke hæmmer anvendelsen af nye teknologier og forretningsområder. Som eksempel herpå har styrelsen indgået et partnerskab med, FR I af 16. september 2015 A/S, under pengeinstitutternes interesseorganisation Finans Danmark om udvikling af den nye MitID-løsning.

5.3.5. Sikrer brugervenlig digitalisering

Log-in og autentifikation gennem MitID-løsningen og NemLog-in er en grundlæggende forudsætning for digitalisering. Serviceområder i NemLog-in, såsom Digital repræsentation, har i højere grad karakter af serviceområder, der varetager og muliggør erhvervsrettede funktioner. Serviceområdet Digital repræsentation understøtter partsrepræsentation for blandt andet enkeltmandsvirksomheder, mens det med serviceområdet Erhvervsadministration vil være muligt at tilknytte og administrere rettigheder til en erhvervsidentitet, herunder for de områder en erhvervsbruger kan tilgå i digitale selvbetjeningsløsninger på vegne af deres organisation. Der henvises til lovforslagets almindelige bemærkninger afsnit 2.2.2. for yderligere information om NemLog-in. Med serviceområderne i NemLog-in sikres der samspil og sammenhæng med øvrige offentlige digitale tjenester, og det er Digitaliseringsstyrelsens vurdering, at lovforslaget derved sikrer brugervenlig digitalisering.

6. De administrative konsekvenser for borgerne

Med en omstilling fra NemID til MitID vil der være en omstilling til en ny eID-løsning, som ikke længere indeholder det analoge identifikationsmiddel, nøglekortet. Med udfasning af nøglekortet følger der en tilvænning til en ny løsning, som af nogle privatpersoner vil opleves som mere digital. Privatpersoner, som ikke ønsker at anvende MitID-appen som identifikationsmiddel, vil dog fortsat kunne vælge fysiske elektroniske identifikationsmidler, som afløser for nøglekortet.

Endvidere vil der være en høj grad af genkendelighed fra de eksisterende løsninger, hvilket forventeligt på sigt vil bringe antallet af klager fra privatpersoner på niveau med det nuværende antal klager. I den nye løsning reduceres risikoen for snyd med de fysiske og kopierbare nøglekort, hvilket ligeledes forventes at kunne nedbringe antallet af klager. Det vurderes, at lovforslaget indeholder et hjemmelsgrundlag, som sikrer mulighed for at fastsætte klare regler for privatpersoners retsstilling, og hvori det fastslås, at privatpersoner kan klage til Digitaliseringsstyrelsen over afslag på at få udstedt MitID mv.

7. De klima- og miljømæssige konsekvenser

Lovforslaget har indirekte positive klima- og miljømæssige konsekvenser, idet det sikres, at MitID og NemLog-in fortsat vil understøtte bred anvendelse af obligatorisk digital selvbetjening. Digital selvbetjening medfører mindsket papirforbrug og reduceret transport, hvilket leder til et mindre miljømæssigt aftryk og lavere udledning af drivhusgasser.

8. Forholdet til EU-retten

8.1. eIDAS-forordningen

Lovforslagets indhold er på en række punkter påvirket af 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). eIDAS-forordningen indeholder et fælles regelgrundlag for tillidstjenester til brug for elektroniske transaktioner, og forpligter medlemsstaterne til gensidigt at anerkende udenlandske identifikationsordninger (eID), som i henhold til eIDAS-forordningen er anmeldt til EU-Kommissionen på sikringsniveau betydelig eller høj, i deres offentlige digitale selvbetjeningsløsninger.

Idet serviceområdet Digital signering i NemLog-in indeholder tillidstjenester til brug for elektroniske transaktioner, særligt i forbindelse med elektronisk signering og tidsstempling, og MitID-løsningen vil blive anmeldt som den danske nationale elektroniske identifikationsordning i henhold til eIDAS-forordningen, er løsningerne underlagt bestemmelser i eIDAS-forordningen. I eIDAS-forordningen sættes således delvist rammen for lovforslaget. Forordningen regulerer blandt andet erstatning, gensidig anerkendelse af eID, diverse formelle og tekniske sikkerhedskrav samt tilsyn med og retsvirkninger af elektroniske tillidstjenester. Dette lovforslag regulerer kun aspekter, der ikke allerede er berørt i eIDAS-forordningen.

Efter eIDAS-forordningen skal der ske gensidig anerkendelse af elektroniske identifikationsmidler på sikringsniveau betydelig eller høj, som er udstedt i en medlemsstat, og som er anmeldt til EU-Kommissionen, når der i en anden medlemsstat stilles krav om autentifikation som betingelse for adgang til en onlinetjeneste. Den nationale eID-gateway udgør Danmarks tekniske implementering af kravet i forordningen og er derfor ikke reguleret yderligere i dette lovforslag. Fordi eIDAS-forordningen er gældende i Danmark, er det således muligt gennem eID-gatewayen at få adgang til danske onlinetjenester med eID'er svarende til MitID, som er udstedt i andre medlemsstater, hvis betingelserne i forordningen er opfyldt. Det skal dog bemærkes, at eIDAS-forordningen ikke finder anvendelse på de elektroniske selvbetjeningsløsninger og dermed forbundne infrastrukturer, der er etableret i medlemsstaterne. Det medfører, at medlemsstaterne har respekteret kravet om gensidig anerkendelse i forordningen, når det i eID-gatewayen er konstateret, at en fysisk person har et anerkendt eID, mens øvrige led i sagsbehandlingen, herunder indsamling og vurdering af ansøgerens ID-beviser, skal behandles efter national ret og efter gældende forpligtelser efter EU-forordningen om Single Digital Gateway (EU-forordningen om oprettelse af en fælles digital portal, der giver adgang til oplysninger, procedurer og bistands- og problemløsningstjenester, og om ændring af forordning (EU) nr. 1024/2012).

8.1.1. Den Nationale Standard for identiteters sikringsniveauer

Den Nationale Standard for identiteters sikringsniveauer (NSIS-standarden), er en dansk standard, som fastlægger en national ramme for tillid til digitale identiteter i tråd med eIDAS-forordningens regler for digitale identiteter.

Kravene i NSIS-standarden tager udgangspunkt i og lever som minimum op til eIDAS-forordningen, således at en dansk elektronisk identifikationsordning, som opfylder et givet sikringsniveau i denne standard, også må forventes at kunne opfylde kravene til samme niveau i forhold til eIDAS-forordningen. I den forbindelse skal det dog bemærkes, at NSIS-standarden er tilpasset nationale forhold og er mere detaljeret end den gennemførelsesretsakt (EU-Kommissionens gennemførelsesforordning (EU) 2015/1501 af 8. september 2015 om interoperabilitetsrammen i henhold til artikel 12, stk. 8, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked), som definerer de tilsvarende sikringsniveauer under eIDAS-forordningen.

Hovedformålet med NSIS-standarden er at skabe rammerne for tillid til digitale identiteter samt iden-

titetstjenester nationalt. NSIS-standarden definerer krav til styrken af en autentifikationsproces, den underliggende identitetssikring og det anvendte elektroniske identifikationsmiddel, udtrykt som et samlet sikringsniveau. NSIS-standarden indeholder en række krav til ID-tjenesters autentifikation på tre forskellige sikringsniveauer benævnt 'lav', 'betydelig' og 'høj'. Niveauerne 'betydelig' og 'høj' betegnes i denne lov samlet som 'sikker autentifikation', jf. den foreslåede § 2, nr. 5. De tre niveauer i NSIS-standarden implementerer de tre tilsvarende niveauer i eIDAS-forordningens artikel 8. Kravene til de tre sikringsniveauer omfatter både tekniske, organisatoriske og økonomiske forhold, idet mange faktorer har indflydelse på tilliden til digitale identiteter og identitetstjenester. Sikringsniveauerne er opgjort på baggrund af tekniske specifikationer, standarder og hertil knyttede procedurer, hvis formål er at mindske risici for misbrug eller ændring ved anvendelse af en digital identitet.

NSIS-standarden er gældende for nationale, offentlige elektroniske identifikationsordninger og identitetsbrokere, der håndterer digitale identiteter for privatpersoner, juridiske enheder og privatpersoner associeret med en juridisk enhed. Den er gældende for såvel stat, kommuner som regioner og på tværs af domæner (fx sundhed og uddannelse) og omfatter både private og offentlige udbydere af elektroniske identifikationsordninger samt identitetsbrokere, som ønsker at anvende den fællesoffentlige infrastruktur.

NSIS-standarden er afgrænset til at vedrøre forhold i relation til udstedelse og brug af elektroniske identifikationsmidler og identitetsbrokere.

Det er de enkelte tjenesteudbydere, som har ansvaret for at vurdere, hvilket sikringsniveau en digital identitet skal være udstedt på for at få adgang til deres digitale selvbetjeningsløsninger. For tjenesteudbydere, som behandler personoplysninger, vil afdækning af risici og kontroller ofte ligge i naturlig forlængelse af forpligtelserne i henhold til den til enhver tid gældende regulering om behandling af personoplysninger.

8.2. Regler om fri bevægelighed og udbudsretten

Leveringen af MitID-løsningen og NemLog-in er i lovforslaget organiseret med henblik på at sikre, at offentlige myndigheder og offentligretlige organer kan anskaffe disse ydelser fra Digitaliseringsstyrelsen i medfør af loven. Det foreslås således, som nærmere beskrevet i henholdsvis afsnit 2.1.2.1 og 2.2.2.1., at Digitaliseringsstyrelsen pålægges at stille MitID-løsningen og NemLog-in til rådighed for offentlige myndigheder og offentligretlige organer. Endvidere pålægges Digitaliseringsstyrelsen at stille MitID til rådighed for privatpersoner og erhvervsbrugere. Offentlige myndigheder og offentligretlige organer forpligtes i et vist omfang med lovforslaget til at anskaffe MitID-løsningen og NemLog-in fra Digitaliseringsstyrelsen, mens de uden for denne forpligtelse har en ret til at anskaffe løsningerne fra Digitaliseringsstyrelsen. Denne organisering er i overensstemmelse med gældende EU-ret og praksis fra EU-Domstolen.

Det bemærkes, at den frie konkurrence er sikret gennem de behørigt gennemførte EU-udbud for udvikling og drift af MitID-løsningen, MitID og NemLog-in.

Lovforslaget anses følgelig for at være proportionalt og i overensstemmelse med Traktaten om Den Europæiske Unions Funktionsmåde.

9. Hørte myndigheder og organisationer mv.

Et udkast til lovforslaget har i perioden fra den 20. august 2020 til den 17. september 2020 været sendt i høring hos følgende myndigheder og organisationer mv.:

ATP, Advokatsamfundet, AE – Arbejderbevægelsen Erhvervsråd, BL – Danmarks almene boliger, Danmarks Statistik, Danmarks Nationalbank, Dansk IT, Dansk standard, Forum for digital sikkerhed, Danske advokater, DI Digital, Danske Handicaporganisationer, Dansk Arbejdsgiverforening, Dansk Byggeri, Dansk Erhverv, Dansk Industri, Danske Regioner, Datatilsynet, Den Danske Dommerforening, Det centrale Handicapråd, Håndværksrådet, DKCERT, FDIH – Foreningen for Danske Internethandel,

Finans Danmark, Finanstilsynet, Forbrugerrådet Tænk, Foreningen Danske Revisorer, Foreningen af Registrerede Revisorer, Forsikring og Pension, Landsforeningen Ældre Sagen, Landbrugsrådet, IBIZ-center, IT-Brancheforeningen, Institut for menneskerettigheder, IT-Politisk Forening, KMD, KL, KOMBIT, Konkurrence- og forbrugerstyrelsen, Prosa, Forbundet af IT-Professionelle, Rigsombudsmanden i Grønland, Landsforeningen for førtidspensionister, LOS – De private Sociale tilbud, Microsoft Danmark, Nets DanID A/S, Rådet for digital sikkerhed, Rådet for Socialt Udsatte, Telekommunikationsindustrien i Danmark, Psykiatrifonden, Rigsombudsmanden på Færøerne, Rigsrevisionen, Danske Universiteter, Fagbevægelsens Hovedorganisation, Justitia og Socialrådgiverforeningen.

10. 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 af betydning.	Ja. Udbud og udvikling af de kommende løsninger forventes at udgøre 661,1 mio. kr. i perioden 2014-2022. Driften forventes at koste ca. 84 mio. kr. årligt.
Implementeringskonsekvenser for stat, kommuner og regioner	Ingen	Ja. Omstillingsomkostningerne anslås at udgøre i størrelsesordenen af 50-130 mio. kr.
Økonomiske konsekvenser for erhvervslivet	Ingen	Ja. Lovforslaget forventes at medføre økonomiske konsekvenser for erhvervslivet i form af gebyrer for anvendelse af serviceområderne i NemLog-in og autentifikationstransaktioner i MitID-løsningen.
Administrative konsekvenser for erhvervslivet	Ja. Der forventes løbende administrative byrdelettelser på ca. 238 mio. kr. årligt, blandt andet som følge af det reducerede tidsforbrug ved login og autentificering, herunder en mere fleksibel administration af erhvervsidentiteter og rettigheder i NemLog-in serviceområdet Erhvervsadministration.	Ja. Lovforslaget vurderes foreløbigt at medføre administrative omstillingskonsekvenser for erhvervslivet for mellem 186 og 339 mio. kr. i engangsomkostninger.
Administrative konsekvenser for borgerne	Ingen	Ingen.
Klima og miljømæssige konsekvenser	Ja. Lovforslaget har indirekte positive klima- og miljømæssige konsekvenser, idet det sikres, at MitID-løsningen og NemLog-in fortsat vil	Ingen

	understøtte bred anvendelse af obligatorisk digital selvbetjening.	
Forholdet til EU-retten	<p>Lovforslagets indhold er på en række punkter påvirket af 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). eIDAS-forordningen regulerer tillidstjenester samt elektronisk identifikation (eID) og finder derved anvendelse på MitID samt dele af NemLog-in. eIDAS-forordningen sætter tillige ramme for NSIS-standarden. Dette lovforslag regulerer kun aspekter, der ikke allerede er berørt i eIDAS-forordningen og NSIS-standarden.</p> <p>For så vidt angår reglerne om fri bevægelighed og udbudsretten bemærkes det, at den frie konkurrence er sikret gennem de behørigt gennemførte EU-udbud for udvikling og drift af MitID-løsningen, MitID og NemLog-in. Lovforslaget anses derfor for at være proportionalt og i overensstemmelse med Traktaten om Den Europæiske Unions Funktionsmåde/EUF-traktaten.</p>	
Er i strid med de principper for implementering af erhvervsrettet EU-regulering/ Går videre end minimumskrav i EU-regulering (sæt X)	Ja	Nej X

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

I den gældende lov nr. 493 af 18 maj 2018, om udstedelse af NemID med offentlig digital signatur til fysiske personer og til medarbejdere i juridiske enheder (herefter benævnt lov om NemID), reguleres NemID-løsningen, som erstattes af MitID-løsningen og med dette lovforslag. Gældende ret om NemID er beskrevet nærmere i afsnit 2.1.1. i de almindelige bemærkninger. I forhold til NemLog-in, har denne løsningen ikke tidligere været lovreguleret. De foreslåede bestemmelser om NemLog-in er således ny regulering.

Den foreslåede bestemmelse i lovforslagets § 1, stk. 1, vil medføre, at loven finder anvendelse på infrastrukturløsninger, som nævnt i § 1, stk. 1, nr. 1 og nr. 2, samt nationale digitale identiteter og elektroniske identifikationsmidler udstedt i medfør heraf.

Infrastrukturløsningerne stilles til rådighed af Digitaliseringsstyrelsen, som det fremgår af de foreslåede bestemmelser i § 3, stk. 1, og § 8, stk. 1.

Det skal bemærkes, at loven ikke finder anvendelse på de elementer i de enkelte infrastrukturer, der er reguleret 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) eller af lov nr. 617 af 8. juni 2016 om supplerende bestemmelser til forordning om elektronisk identifikation og tillidstjenester til brug for

elektroniske transaktioner på det indre marked (supplerende lov om eIDAS). Se nærmere herom i afsnit 8.1 i den almindelige bemærkninger.

Den foreslåede bestemmelse i lovforslagets § 1, stk. 1, nr. 1, vil medføre, at loven finder anvendelse på den danske nationale elektroniske identifikationsordning (MitID-løsningen).

MitID-løsningen vil således udgøre den danske nationale elektroniske identifikationsordning (eID-løsning), som vil blive anmeldt i henhold til eIDAS-forordningen.

Med MitID-løsningen stiller Digitaliseringsstyrelsen de danske nationale digitale identiteter til rådighed for privatpersoner, men det udelukker ikke, at der kan eksistere andre digitale identiteter, fx digitale identiteter udviklet til private selvbetjeningsløsninger. Endvidere stiller Digitaliseringsstyrelsen de til løsningen hørende elektroniske identifikationsmidler til rådighed for privatpersoner og erhvervsbrugere. Lovforslaget regulerer alene de danske nationale digitale identiteter og ikke andre typer af digitale identiteter eller andre elektroniske identifikationsordninger. MitID-løsningen defineres i den foreslåede § 2, nr. 1 og løsningen er reguleret i lovforslagets afsnit II.

Den foreslåede bestemmelse i lovforslagets § 1, stk. 1, nr. 2, vil medføre, at loven finder anvendelse på den fællesoffentlige digitale infrastrukturløsning (NemLog-in).

NemLog-in vil således være den fællesoffentlige digitale infrastrukturløsning, som blandt andet muliggør og varetager interaktion mellem digitale brugere og tilsluttede digitale selvbetjeningsløsninger. NemLog-in indeholder en række serviceområder, som er reguleret i den foreslåede § 8, stk. 2 og 3. NemLog-in defineres i den foreslåede § 2, nr. 6 og løsningen er reguleret i lovforslagets afsnit III.

Til § 2

Den foreslåede bestemmelse i lovforslagets § 2, nr. 1 - nr. 17, vil medføre, at der anføres en række definitioner, som nærmere angivet i de enkelte punkter.

Med den foreslåede bestemmelse defineres de væsentlige begreber, som anvendes i loven.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 1 medfører, at MitID-løsningen defineres som den danske nationale elektroniske identifikationsordning.

Det er forventningen, at MitID-løsningen vil blive anmeldt i henhold til eIDAS-forordningen. MitID-løsningen kan også betegnes som en eID-ordning eller eID-løsning. En elektronisk identifikationsordning dækker hele livscyklus for en identitet og et elektronisk identifikationsmiddel.

En anmeldelse af MitID til EU-Kommissionen i henhold til eIDAS-forordningen vil på sigt muliggøre, at MitID kan benyttes til autentifikation i offentlige digitale selvbetjeningsløsninger med grænseoverskridende interesse, der udbydes af andre EU-medlemsstater.

Med løsningen kan der foretages elektronisk identifikation. Løsningen fungerer derved som en autentifikationstjeneste af privatpersoners digitale identiteter. Derudover kan erhvervsbrugere få MitID-identifikationsmidler. Erhvervsbrugere kan dog ikke have en digital identitet i MitID-løsningen, idet erhvervsbrugernes digitale identiteter oprettes i serviceområdet Erhvervsadministration i NemLog-in, jf. § 8, stk. 3. MitID-løsningen er den nationale identitetsgarant for identiteter udstedt til privatpersoner og NemLog-in er den offentlige identitetsgarant for erhvervsidentiteter.

En identitetsgarant foretager blandt andet udstedelse af digitale identiteter. MitID-løsningen foretager således som identitetsgarant udstedelse af digitale identiteter, som sker på baggrund af en udstedelsesproces, hvor personidentifikationsdata indhentes for at sikre entydig sammenhæng mellem en privatperson og den udstedte digitale identitet. MitID-løsningen skal som den danske nationale elektroniske identifikationsordning, således sikre, at det i den digitale verden er muligt entydigt at fastslå den digitale identitet af privatpersoner og i nogle situationer erhvervsbrugere.

Det bemærkes, at MitID-løsningen afløser den hidtidige NemID-løsning, dog ikke for så vidt angår erhvervs-løsningen NemID for erhverv, som i stedet afløses af serviceområdet Erhvervsadministration i

NemLog-in, også kaldet MitID Erhverv, som i denne lov omtales som Erhvervsadministration, jf. § 8, stk. 3.

Begrebet MitID-løsningen refererer til selve den tekniske infrastruktur og ikke til enkelte digitale MitID-identiteter eller MitID-identifikationsmidler.

Det skal bemærkes, at der ved overgangen fra NemID til MitID er sket en række ændringer i den fællesoffentlige digitale infrastruktur, som ikke kan læses direkte af den foreslåede definition. En central ændring medfører, at MitID-løsningen fremadrettet alene vil udgøre en autentifikationsløsning, hvor NemID-løsningen også indeholdt digital signatur. Digital signering vil med den nye digitale infrastruktur fremadrettet ske ved anvendelsen af serviceområdet Digital signering i NemLog-in. Dette medfører, at hvor der tidligere var lighed mellem NemID og digital signatur, vil der fremadrettet skulle anvendes serviceområdet Digital signering til den digitale underskrift baseret på autentifikation med MitID. Ovenstående ændrer ikke på, at det fortsat vil være muligt at anvende private signeringsløsninger.

I den gældende lov om NemID, reguleres NemID-løsningen, som erstattes af MitID-løsningen og med dette lovforslag. Gældende ret om NemID er beskrevet nærmere i afsnit 2.1.1. i de almindelige bemærkninger. Der findes ikke gældende ret, som definerer MitID. Loven regulerer ikke andre typer af elektronisk ID end MitID.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 2, 1. pkt., medfører, at der med MitID forstås den nationale digitale identitet af en privatperson og tilhørende elektroniske identifikationsmidler, som kan tilknyttes privatpersoners og erhvervsbrugeres digitale identiteter.

MitID anvendes således som betegnelse for den nationale digitale identitet af en privatperson og tilhørende elektroniske identifikationsmidler, som kan tilknyttes privatpersoner og erhvervsbrugeres digitale identiteter. En digital identitet er defineret særskilt i denne bestemmelses foreslåede nr. 13. Elektroniske identifikationsmidler er defineret særskilt i denne bestemmelses foreslåede nr. 14.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 2, 2. pkt., medfører, at MitID er den nationale identitetsgarant for privatpersoner.

Når MitID er den nationale identitetsgarant indebærer det, at løsningen kan forsyne privatpersoner med digitale identiteter. Udstedelse af MitID-identiteter med tilhørende elektroniske identifikationsmidler sker som et resultat af den registrerings- og indrulleringsproces, som en privatperson skal gennemgå for at få udstedt sin digitale identitet, og som resulterer i udlevering af et eller flere MitID-identifikationsmidler, der alene eller i kombination anvendes i forbindelse med autentifikation. MitID-løsningen fungerer således som identitetsgarant for privatpersoners digitale identitet.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 3, medfører, at autentifikation defineres som en proces, som genkender og verificerer en digital identitet gennem anvendelse af et elektronisk identifikationsmiddel.

Ved autentifikation bliver en privatpersons eller en erhvervsbrugers digitale identitet bekræftet ved, at denne anvender et eller flere elektroniske identifikationsmidler. Autentifikation af privatpersoners identiteter udgør den centrale elektroniske proces i MitID-løsningen, da MitID-autentifikation blandt andet giver adgang til digitale selvbetjeningsløsninger tilsluttet brokere for MitID-løsningen. Autentifikation af erhvervsbrugere sker i serviceområdet Login og autentifikation i NemLog-in i kombination med enten MitID eller en lokal identitetsgarant. Identitetsgaranten indestår for identiteten, koblingen mellem identiteten og det elektroniske identifikationsmiddel og verificerer identifikationsmidlet, mens NemLog-in formidler den digitale erhvervsidentitet koblet til identifikationsmidlet til den digitale selvbetjeningsløsning.

I den gældende NSIS-standard anvendes der tre niveauer for sikkerheden af identiteter (Levels of assurance) til ID-tjenester, benævnt som niveau lav, betydelig og høj. De tre sikringsniveauer i NSIS svarer til de tre niveauer i eIDAS-forordningen.

Ifølge den gældende eIDAS-forordning er det op til de enkelte medlemsstater at stille nærmere krav til de sikringsniveauer, som de vil anvende. Sikringsniveauer bør ifølge eIDAS-forordningens præambel afspejle graden af tillid til, at et elektronisk identifikationsmiddel kan fastslå identiteten på en person og således give sikkerhed for, at den person, der gør krav på en specifik identitet, faktisk er den person, hvortil identiteten er blevet knyttet. NSIS benyttes som referenceramme til beskrivelse af sikringsniveauerne i MitID og NemLog-in samt for lokale identitetsgaranter. Sikringen af identiteter kan i henhold til NSIS ligeledes ske på tre sikringsniveauer: lav, betydelig og høj. Denne inddeling af niveauer er nødvendig for at beskrive graden af tillid, som indehaveren af en digital selvbetjeningsløsning (en tjenesteudbyder) kan have til en autentificeret digital identitet.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 4, 1. pkt., medfører, at sikringsniveauet defineres som graden af sikkerhed for autentifikation.

I forbindelse med overgangen til MitID-løsningen, overlades det til de individuelle offentlige myndigheder, offentligretlige organer og juridiske enheder at vurdere det sikringsniveau for autentifikation, som deres digitale selvbetjeningsløsning kræver.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 4, 2. pkt., medfører, at der sondres mellem tre forskellige sikringsniveauer for autentifikation, henholdsvis niveau lav, betydelig og høj.

Den foreslåede sondring mellem de forskellige sikringsniveauer anvendes for sikring af digitale identiteter. Kravene til sikringsniveauerne udspringer af NSIS-standarden og eIDAS-forordningen og er nærmere reguleret i disse.

I overensstemmelse med ovenstående er det med MitID muligt at autentificere på de tre sikringsniveauer, henholdsvis niveau lav, betydelig og høj.

Sikringsniveauerne er opgjort på baggrund af tekniske specifikationer, standarder og hertil knyttede procedurer, hvis formål er at mindske risici for misbrug eller ændring ved anvendelse af en digital identitet.

Der findes ikke gældende ret, som anvender betegnelsen ”sikker autentifikation”. I den gældende NSIS-standard anvendes i stedet sikringsniveauerne lav, betydelig og høj.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 5, medfører, at der med sikker autentifikation forstås autentifikation på sikringsniveau betydelig eller høj.

Med den foreslåede bestemmelse udgør sikker autentifikation en proces, der genkender og verificerer en digital identitet på sikringsniveau betydelig eller høj.

Betegnelsen sikker autentifikation udgør alene en fællesbetegnelse i denne lov for autentifikation på sikringsniveau betydelig eller høj. Sikringsniveau lav vil derfor fortsat skulle leve op til NSIS-standardens krav til autentifikation på dette sikringsniveau.

Der findes ikke gældende ret, som definerer NemLog-in.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 6, 1. pkt. medfører, at NemLog-in forstås som den fællesoffentlige digitale infrastrukturløsning, som sætter privatpersoner og erhvervsbrugere med digitale identiteter i stand til at interagere med digitale selvbetjeningsløsninger.

NemLog-in defineres således som den fællesoffentlige digitale infrastrukturløsning, som muliggør og varetager interaktion mellem på den ene side digitale selvbetjeningsløsninger og på den anden side privatpersoner med digitale identiteter oprettet i MitID-løsningen samt erhvervsbrugere med digitale identiteter oprettet i NemLog-in.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 6, 2. pkt. medfører, at NemLog-in endvidere er den nationale identitetsgarant for erhvervsidentiteter.

I praksis er NemLog-in den fællesoffentlige broker for MitID og identitetsgarant for digitale erhvervsidentiteter i Danmark. Når NemLog-in er den fællesoffentlige broker for MitID og identitetsgarant for

digitale erhvervsidentiteter i Danmark, indebærer det, at løsningen kan forsyne erhvervsbrugere med digitale identiteter.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 6, 3. pkt. medfører, at NemLog-in indeholder de serviceområder, som angives i § 8, stk. 2 og 3.

NemLog-in indeholder en række serviceområder: Login og autentifikation, Digital repræsentation, Digital signering og Erhvervsadministration. Serviceområdet Erhvervsadministration kaldes også MitID Erhverv. Serviceområderne er nærmere beskrevet i § 8, stk. 2 og 3. NemLog-in er således en for samfundet kritisk infrastrukturløsning og indgang til den offentlige digitale selvbetjening, idet serviceområderne indeholder centrale services, som er væsentlige for anvendelse og sammenhæng i den fællesoffentlige infrastruktur.

Begrebet privatperson anvendes med forskellige betydninger i gældende ret afhængig af, hvilket lovgrundlag, som der anvendes.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 7, medfører, at en privatperson defineres som en fysisk person, der udelukkende agerer på vegne af sig selv uden forbindelse til en juridisk enhed, og som ikke er en erhvervsbruger.

Begrebet privatpersoner udgør i hovedreglen borgere, men er dog ikke begrænset til danske statsborgere.

En privatperson kan have en national digital identitet i MitID-løsningen, hvor en erhvervsbruger har en digital identitet i NemLog-in. Erhvervsbrugere, jf. bestemmelsens foreslåede nr. 8 er ikke en delmængde af begrebet privatpersoner i bestemmelsens foreslåede nr. 7, selvom en fysisk person i praksis både kan agere i rollen som privatperson og erhvervsbruger. Erhvervsbrugere defineres således som et selvstændigt begreb.

Begrebet erhvervsbruger er ikke defineret i gældende ret i relation til NemLog-in.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 8, medfører, at en erhvervsbruger defineres som en fysisk person, der er associeret med en offentlig myndighed, et offentligretligt organ eller en juridisk enhed, som er oprettet med én eller flere erhvervsidentiteter i serviceområdet Erhvervsadministration i NemLog-in.

Begrebet ”associeret med” skal forstås i overensstemmelse med NSIS og eIDAS-forordningen, og udgør således en videreførelse af definitionerne fra eIDAS-forordningen og NSIS, hvoraf det fremgår, at associationen blandt andet dækker medarbejdere ansat i en virksomhed, men også anden tilknytning, hvor der ikke foreligger et ansættelsesforhold. Associationen beskriver således, at der er en relation mellem den fysiske person og den offentlige myndighed, det offentligretlige organ eller den juridiske enhed, som danner grundlag for en erhvervsidentitet.

En erhvervsbrugers digitale identitet er oprettet i NemLog-in i serviceområdet Erhvervsadministration, jf. § 8, stk. 3. En erhvervsbruger kan desuden vælge at anvende det elektroniske identifikationsmiddel, som denne har fået udstedt som privatperson, til at autentificere sin erhvervsidentitet. En erhvervsbrugers elektroniske identifikationsmiddel kan således oprettes i MitID som et dedikeret MitID, jf. princippet om dobbelt frivillighed, som nærmere beskrevet i § 9, stk. 4, og i bemærkningerne til § 4, stk. 1. Når betegnelsen erhvervsbruger anvendes i loven, er der tale om én eller flere oprettede erhvervsidentiteter, som tilhører erhvervsbrugeren. En erhvervsbruger kan således have tilknyttet flere erhvervsidentiteter. Til forskel fra definitionen af en privatperson, som har fået udstedt en privat digital identitet tilknyttet til privatpersonen, er erhvervsbrugers digitale identitet tilknyttet til denne i medfør af erhvervsbrugers associering med en offentlig myndighed, et offentligretligt organ eller en juridiske enhed.

I den gældende lovebekendtgørelse nr. 1052 af 16. oktober 2019 om Det Centrale Virksomhedsregister (herefter cvr-loven) er begrebet juridisk enhed defineret.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 9, medfører, at begrebet juridisk enhed defineres

som en juridisk enhed med et cvr-nummer, jf. cvrloven, der ikke enten er en offentlig myndighed, jf. nr. 10 eller et offentligretligt organ, jf. nr. 11. Til definitionen af begrebet juridisk enhed hører således ikke offentlige myndigheder og offentligretlige organer, uanset om de i andre sammenhænge, blandt andet cvr-loven, betragtes som juridiske enheder. Offentlige myndigheder og offentligretlige organer er selvstændigt defineret. For afgrænsningen af en offentlig myndighed eller et offentligretligt organ henvises til denne bestemmelses nr. 10 og 11.

En juridisk enhed kan i relation til NemLog-in agere i rollen som tjenesteudbyder, jf. nr. 15 eller brugerorganisation, jf. nr. 16. Dette indebærer, at en juridisk enhed i rollen som tjenesteudbyder vil være karakteriseret ved at være ansvarlig for én eller flere digitale selvbetjeningsløsninger. Når en juridisk enhed er tilsluttet serviceområdet Erhvervsadministration i NemLog-in, vil den juridiske enhed betegnes som en brugerorganisation i regi af NemLog-in.

Den gældende bestemmelse i § 24, nr. 28, 1. led, i udbudsloven, lov nr. 1564 af 15. december 2015, (herefter benævnt udbudsloven), medfører, at der ved ordregiver forstås statslige, regionale og kommunale myndigheder.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 10, medfører, at begrebet offentlig myndighed defineres som statslige, regionale og kommunale myndigheder.

Definitionen af offentlige myndigheder skal forstås i overensstemmelse med udbudslovens definition af offentlige myndigheder i rollen som ordregivere, jf. § 24, nr. 28, 1. led, i udbudsloven.

Definitionen af en offentlig myndighed i den foreslåede bestemmelse er baseret på et formelt (organisatorisk) kriterium. I dele af lovforslaget suppleres definitionen med et materielt (funktionelt) kriterium, idet der her vil være fremhævet, at bestemmelsen alene omfatter offentlige myndigheder, når de udfører en myndighedsopgave. I forhold til det formelle kriterium ses der på, om den offentlige myndighed formelt set er en statslig, regional eller kommunal myndighed og således er en ordregiver, jf. udbudslovens § 24, nr. 28, 1. led. Hvor definitionen af offentlige myndigheder i lovforslagets bestemmelser om pligt suppleres med et materielt kriterium, kan en offentlig myndighed være omfattet delvist af bestemmelsen. Det indebærer, at hvis en offentlig myndighed både løser myndighedsopgaver og opgaver af privat karakter, gælder pligten alene for den offentlige myndighed, når den offentlige myndighed udfører myndighedsopgaver, som kræver sikker autentifikation.

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 3 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 ikkeindustriel eller ikkekommerciel 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 3 betingelser skal være opfyldt.

Det følger af bestemmelsen, 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. Eksempelvis 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 imødekom sådan behov ved dets oprettelse, men på et senere tidspunkt.

I henhold til Europa-Parlamentets og Rådet direktiv 2014/24/EU af 26. februar 2014 om offentlige udbud og om ophævelse af direktiv 2004/18/EF (fremover udbudsdirektivet) præambel 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 eksempelvis 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 (forsorghjem, kvindekrisecentre, væresteder m.v.), som kommunen 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 Dyrtidsfond, Naviair, de almene boligorganisationer og universiteterne.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 11, medfører, at der ved et offentligretligt organ forstås: 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 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.

Bestemmelsen skal forstås i overensstemmelse med § 24, nr. 27 i udbudsloven.

Offentligretlige organer er et udbudsretligt begreb, der omfatter almennyttige organer med nær tilknytning til den offentlige sektor. Definitionen af et offentligretligt organ er i den foreslåede lov baseret på et formelt (organisatorisk) kriterium, der indholdsmæssigt svarer til udbudslovens § 24, nr. 27. I dele af lovforslaget suppleres definitionen med et materielt (funktionelt) kriterium. Lovforslagets pligter omfatter alene offentligretlige organer, når de udfører myndighedsopgaver. Det samme gælder for offentlige myndigheder, hvorfor vurderingen af om det offentligretlige organ lever op til det materielle kriterium, er funderet i de samme hensyn, som gør sig gældende for offentlige myndigheder. For en nærmere beskrivelse henvises der til bemærkningerne til denne bestemmelses nr. 10.

I gældende ret er digitale selvbetjeningsløsninger ikke defineret. Dog skal begrebet forstås i overensstemmelse med begrebet ”onlinetjeneste”, som anvendes som udefineret begreb i eIDAS-forordningen.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 12, medfører, at digital selvbetjeningsløsning defineres som et it-system, hvor privatpersoner eller erhvervsbrugere med digitale identiteter kan tilgå digital selvbetjening efter at være blevet autentificeret.

En digital selvbetjeningsløsning udstiller digitale services, som kan tilgås af privatpersoner eller erhvervsbrugere. Med udstiller menes i denne sammenhæng en elektronisk tilrådighedsstillelse af en digital selvbetjeningsløsning, applikation eller funktion for brugeren.

En offentlig myndighed eller et offentligretligt organ kan i rollen som tjenesteudbyder, jf. den foreslåede nr. 15, have en eller flere digitale selvbetjeningsløsninger tilsluttet NemLog-in, der udstiller digitale services til offentlig anvendelse.

Såfremt der er tale om internt anvendte onlinetjenester eller it-systemer inden for et myndighedsområde, som ikke udstiller digitale services til offentlig anvendelse, er disse ikke at anse som digitale selvbetjeningsløsninger i denne lovs forstand og er derfor ikke påkrævet tilslutning til NemLog-in og MitID-løsningen. Fx vil et kommunalt sagsbehandlingssystem, som alene betjenes af erhvervsbrugere i kommunen ikke være omfattet af definitionen digital selvbetjeningsløsning, idet et sådant sagsbehandlingssystem ikke vil være åbent for offentlig anvendelse af privatpersoner eller erhvervsbrugere. Dette gælder også, hvis fx flere kommuner i fællesskab har anskaffet og anvender et sagsbehandlingssystem.

Den gældende bestemmelse i art. 3, nr. 1, i eIDAS-forordningen, medfører, at der ved elektronisk identifikation forstås det at bruge personidentifikationsdata i elektronisk form, der entydigt repræsenterer enten en fysisk eller juridisk person eller en fysisk person, der repræsenterer en juridisk person.

En digital identitet er det samme som en elektronisk identitet (eID), jf. gældende ret fra eIDAS-forordningen, og skal således forstås i overensstemmelse med definitionen i eIDAS-forordningen.

Bestemmelsen tilsigter endvidere ikke en anden definition end definitionen af en digital identitet, som findes i den gældende standard, Digitaliseringsstyrelsen har udarbejdet, og som hedder ”Referencarkitektur for brugerstyring”. Standarden har til formål at understøtte udviklingen af brugerstyring i den offentlige sektor. Begrebet i den gældende Referencearkitektur for brugerstyring er nedarvet fra e-IDAS-forordningen.

Endvidere skal definitionen forstås i overensstemmelse med den gældende NSIS-standard, hvoraf det

fremgår, at en identitet (elektronisk) udgør en digital persona repræsenteret ved et sæt af attributter, som fx kan repræsentere en fysisk person (privatidentitet), en juridisk enhed (virksomhedsidentitet), eller en fysisk person, der er associeret med en juridisk - 9 af 32 - enhed (fx erhvervsidentitet). En identitet kan rumme personidentifikationsdata men kan også være pseudonym. Det bemærkes, at den gældende definition af elektronisk identitet i NSIS-standarden er i overensstemmelse med e-IDAS-forordningens definition af elektronisk identitet.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 13, medfører, at der ved digital identitet forstås, en samling af data, der unikt identificerer en privatperson eller en erhvervsbruger.

En digital identitet udstedes af en identitetsgarant og kobles til et eller flere elektroniske identifikationsmidler eller certifikater, der over for tredjepart beviser koblingen mellem den private person og den elektroniske identitet. Udstedelse af en digital identitet kræver indsamling af personidentifikationsdata, som er et sæt af data, der gør det muligt entydigt at fastslå identiteten af en privatperson eller en erhvervsbruger. Den samling af persondata, som danner grundlag for en digital identitet indsamles ved anmodningen om udstedelse af MitID.

Som eksempel på personidentifikationsdata kan nævnes navn og personnummer. Der henvises i øvrigt til de almindelige bemærkninger i afsnit 2.3. om behandling af personoplysninger.

Den gældende bestemmelse i art. 3, nr. 2, i eIDAS-forordningen, medfører, at elektronisk identifikationsmiddel defineres som en materiel og/eller immateriel enhed, der indeholder personidentifikationsdata, og som bruges til autentifikation i forbindelse med en onlinetjeneste.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 14, 1. pkt. medfører, at elektronisk identifikationsmiddel defineres som en materiel enhed, en immateriel enhed eller en kombination af disse, der indeholder personidentifikationsdata, og som bruges til autentifikation i digitale selvbetjeningsløsninger.

Et elektronisk identifikationsmiddel benyttes til entydigt at autentificere en digital identitet. Ved anvendelse af offentlige digitale selvbetjeningsløsninger følger en lang række af beslutninger med potentielt vidtrækkende konsekvenser for den enkelte privatperson eller erhvervsbruger, hvorfor det er afgørende, at den digitale identitet fastslås korrekt. Det kræver derfor et eller flere elektroniske identifikationsmidler for, at en privatperson eller erhvervsbruger kan autentificere sig i MitID-løsningen.

Det skal bemærkes, at en erhvervsbruger i særlige tilfælde kan anvende andre typer af elektroniske identifikationsmidler end dem, som er indeholdt i MitID. Det kan fx være elektroniske identifikationsmidler udstedt af en lokal identitetsgarant.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 14, 2. pkt. medfører, at et elektronisk identifikationsmiddel består af ét eller flere elementer, der hver især er et elektronisk identifikationsmiddel.

Et elektronisk identifikationsmiddel kan være knyttet til bestemt hardware, således at en applikation til elektronisk identifikation er bundet til en materiel enhed, der fremstiller selve applikationen til elektronisk identifikation, fx en kodeviser eller en app. Et elektronisk identifikationsmiddel kan udstedes til en privatperson eller en erhvervsbruger til brug for autentifikation i digitale selvbetjeningsløsninger. Et elektronisk identifikationsmiddel, som er udstedt i MitID-løsningen, betegnes som et MitID-identifikationsmiddel.

Der findes ikke gældende ret, som definerer begrebet tjenesteudbyder i relation til lovforslagets anvendelsesområde.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 15, medfører, at tjenesteudbyder defineres som en offentlig myndighed, et offentligretligt organ eller en juridisk enhed, der er ansvarlig for én eller flere digitale selvbetjeningsløsninger.

En tjenesteudbyder er karakteriseret ved at være ansvarlig for de digitale selvbetjeningsløsninger, som tjenesteudbyderen vælger at udstille.

I NemLog-in kan de offentlige myndigheder, offentligretlige organer og juridiske enheder agere i rollen

som tjenesteudbydere eller i rollen som brugerorganisationer. I rollen som tjenesteudbyder tilbyder en offentlig myndighed, et offentligretligt organ eller en juridisk enhed adgang til og anvendelse af et eller flere serviceområder i NemLog-in i deres digitale selvbetjeningsløsninger, som minimum anvendes serviceområdet Login og autentifikation. Om brugerorganisationer se bestemmelsens nr. 16.

En tjenesteudbyder skal altid være tilsluttet en broker.

En tjenesteudbyder kan fx være en offentlig myndighed, offentligretligt organ eller en juridisk enhed, der ved en aftale med en broker kan anvende MitID-løsningen til autentifikation af en privatperson eller en erhvervsbruger, til deres digitale selvbetjeningsløsning.

I denne lov reguleres alene en sådan flerhed af tjenesteudbydere, når den indgår i og anvender den offentlige infrastruktur, og den benævnes i loven som NSIS anmeldt broker tilsluttet NemLog-in.

I den gældende ret er brugerorganisation ikke defineret.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 16, medfører, at en brugerorganisation defineres som en offentlig myndighed, et offentligretligt organ eller en juridisk enhed, der er tilsluttet og anvender serviceområdet Erhvervsadministration i NemLog-in til deres erhvervsbrugere.

I rollen som brugerorganisation er det således den enkelte offentlige myndighed, det offentligretlige organ eller den juridiske enhed, som anvender funktionerne i serviceområdet Erhvervsadministration, som er nærmere beskrevet i § 8, stk. 3. I modsætning til en tjenesteudbyder stiller en brugerorganisation således ikke digitale selvbetjeningsløsninger til rådighed for tredjeparter.

I den gældende NSIS-standard er identitetsbroker angivet som en ID-tjeneste, som formidler en autentificeret identitet til tredjeparter på baggrund af en autentifikation verificeret af brokern selv eller evt. af en anden tredjepart (brokere i flere led). En identitetsbroker foretager ikke nødvendigvis selv identitetssikring eller udstedelse af elektroniske identifikationsmidler, og kan derfor være separat fra en elektronisk identifikationsordning. En identitetsbroker er en tjeneste, som kræver tillid (optræder som en såkaldt trusted third party) fra forretningstjenester, og er derfor underlagt krav i denne standard.

For brokere der indgår i den offentlige infrastruktur, skal begrebet broker forstås i overensstemmelse med begrebet identitetsbroker, som angivet i NSIS-standard.

Den foreslåede bestemmelse i lovforslagets § 2, nr. 17, medfører, at en broker defineres som, en offentlig myndighed, et offentligretligt organ eller en juridisk enhed, der videreformidler autentifikation af digitale identiteter.

En tjenesteudbyder skal fremover tilsluttes en broker for at kunne tilbyde log-in med MitID til sine brugere. Brokermodellen er blandt andet introduceret for at øge sikkerheden i MitID og for at gøre integrationen nemmere for tjenesteudbydere. Det er en forudsætning for, at en broker kan blive koblet direkte på MitID-løsningen, at brokern er certificeret. For at blive certificeret som broker for MitID, skal en broker leve op til høje krav om fx sikkerhed, forretningsførelse, rapportering, databehandling, support og garantier. For at en broker kan interagere med den offentlige infrastruktur og formidle autentifikation af digitale identiteter til offentlige tjenester, kræves det yderligere, at brokern er NSIS anmeldt.

En broker, der ikke er certificeret, kan ikke tilsluttes MitID-løsningen direkte, men skal tilsluttes via en certificeret broker. Den ikke-certificerede broker kan således via en aftale med en certificeret broker acceptere aftalevilkår fastsat af Digitaliseringsstyrelsen for at kunne anvende MitID-løsningen og videreformidle autentifikation af digitale identiteter til en eller flere tjenesteudbydere.

NemLog-in udgør den offentlige broker for MitID-løsningen, og vil således være den broker, som anvendes i langt de fleste tilfælde for offentlige myndigheder og offentligretlige organer, jf. også den foreslåede § 11. Det vil ligeledes være muligt for private tjenesteudbydere at få adgang til dele af NemLog-in.

Til § 3

Tilrådgivningsstillingen af MitID-løsningen er ikke reguleret i anden lovgivning. Med MitID-løsningen hjemtager Digitaliseringsstyrelsen løsningen og påtager sig myndighedsansvaret for at stille løsningen til rådighed. Dette gør sig ikke gældende for NemID, hvorfor bestemmelsen udgør ny regulering.

Med den foreslåede bestemmelse i § 3, stk. 1, 1. pkt., fastslås det, at Digitaliseringsstyrelsen stiller MitID-løsningen til rådighed for offentlige myndigheder, offentligretlige organer og juridiske enheder.

Med bestemmelsen fastslås det, at Digitaliseringsstyrelsen pålægges myndighedsopgaven at stille MitID-løsningen som Danmarks nationale elektroniske identifikationsordning til rådighed for offentlige myndigheder, offentligretlige organer og juridiske enheder samt at sikre og levere udvikling, drift, vedligeholdelse og forvaltning af løsningen.

Digitaliseringsstyrelsens tilrådgivningsstilling af MitID-løsningen sker i praksis gennem realiseringen af den indgåede kontrakt om udvikling og drift af MitID og har til formål at sikre en digital infrastruktur, hvor privatpersoner og erhvervsbrugere kan blive autentificeret i offentlige myndigheders og offentligretlige organers digitale selvbetjeningsløsninger, som kræver sikker autentifikation. Ligeledes kan MitID-løsningen anvendes af juridiske enheder. Herved kan private virksomheder vælge at benytte MitID-løsningen til autentifikation i deres digitale selvbetjeningsløsninger.

Digitaliseringsstyrelsen stiller MitID-løsningen til rådighed for offentlige myndigheder og offentligretlige organer gennem NemLog-in. Når NemLog-in fungerer som fællesoffentlig broker, sikres en høj tillid til den fællesoffentlige digitale infrastruktur samt en ensartet brugerrejse på tværs af offentlige digitale selvbetjeningsløsninger.

Digitaliseringsstyrelsen stiller desuden MitID-løsningen til rådighed for juridiske enheder gennem NemLog-in eller en broker, som er certificeret af Digitaliseringsstyrelsen.

Bestemmelsen udelukker ikke, at andre aktører udvikler og udbyder elektroniske identifikationsordninger eller brokere på markedsvilkår. Bestemmelsen udelukker heller ikke, at andre EU-landes anmeldte eID-ordninger efter eIDAS-forordningen kan anvendes til at tilgå offentlige myndigheders digitale selvbetjeningsløsninger i Danmark gennem den nationale eID-gateway.

Digitaliseringsstyrelsen stiller MitID-løsningen til rådighed for offentlige myndigheder og offentligretlige organer efter de nærmere regler om tilrådgivningsstilling og anvendelse, der fremgår af § 15, stk. 2 og § 16.

Digitaliseringsstyrelsen stiller MitID-løsningen til rådighed for juridiske enheder efter § 7, § 15, stk. 1 og § 16.

Det fastslås med § 3, stk. 1, 2. pkt., at Digitaliseringsstyrelsen sikrer udvikling, drift og vedligeholdelse af løsningen.

Med bestemmelsen konkretiseres Digitaliseringsstyrelsens myndighedsopgave, til at omfatte udvikling, drift og vedligeholdelse af løsningen.

Tilrådgivningsstillingen i medfør af 1. pkt., af MitID-løsningen vil derfor være forbundet med en pligt for Digitaliseringsstyrelsen til at udvikle, drifte og vedligeholde løsningen.

Da kontrakten på NemID udløber, er det nødvendigt, at udvikle en ny løsning. Da NemID har udviklet sig til at være samfundskritisk it-infrastruktur, ønsker staten at hjemtage løsningen, således at staten ejer løsningen og påtager sig myndighedssansvaret at stille løsningen til rådighed for offentlige myndigheder, offentligretlige organer og juridiske enheder. Udviklingen af løsningen kan ske i samarbejde med andre offentlige myndigheder, offentligretlige organer eller juridiske enheder, jf. § 5, stk. 1. Opgaverne med udvikling, drift og vedligeholdelse af MitID-løsningen inkluderer etablering og løbende tilpasning af løsningen samt varetagelse af den daglige drift af løsningen. MitID-løsningen tilpasses løbende i takt med den teknologiske udvikling samt det skiftende trusselsbillede og ændrede samfundsbehov. Digitalise-

ringsstyrelsen varetager den sædvanlige kontraktstyring af leverandøren, som udpeges med hjemmel i den foreslåede § 4, stk. 2.

Det foreslås med § 3, *stk. 2*, at Digitaliseringsstyrelsen stiller MitID til rådighed for privatpersoner og erhvervsbrugere, såfremt privatpersoner og erhvervsbrugere opfylder betingelserne for udstedelse af MitID, som fastsat i medfør af § 4, stk. 2.

Med bestemmelsen får privatpersoner og erhvervsbrugere mulighed for at få udstedt MitID og kan derved tilgå digitale selvbetjeningsløsninger, der anvender MitID-løsningen til autentifikation.

Når Digitaliseringsstyrelsen stiller MitID til rådighed for privatpersoner og erhvervsbrugere, betyder det, at privatpersoner kan få stillet et MitID til rådighed, og at erhvervsbrugere kan få stillet et MitID-identifikationsmiddel til rådighed. Således kan erhvervsbrugere anvende dette MitID-identifikationsmiddel til at autentificere deres erhvervsidentitet på vegne af en virksomhed.

Lovforslaget pålægger ikke privatpersoner eller erhvervsbrugere at anvende løsningerne, men indeholder et retskrav for disse til at få udstedt MitID, hvis de opfylder betingelserne, som fastsættes i medfør af foreslåede § 4, stk. 2.

Når privatpersoner får udstedt MitID, tildeles disse en digital identitet i MitID-løsningen. Herved fungerer MitID-løsningen som identitetsgarant for privatpersoners digitale identiteter oprettet i MitID-løsningen. Erhvervsidentiteter registreres fremadrettet i NemLog-in i serviceområdet Erhvervsadministration, jf. § 8, stk. 3. NemLog-in fungerer dermed som identitetsgarant for erhvervsidentiteter.

Det forventes, at der i bekendtgørelse udstedt i medfør af den foreslåede § 4, stk. 2, vil blive fastsat regler om, at MitID til privatpersoner kan udstedes ved personligt fremmøde hos en registreringsenhed, der er udpeget af Digitaliseringsstyrelsen til at udstede MitID. Dette kan fx være borgerservicecentre, hvis de er udpeget af kommunalbestyrelsen, jf. § 5, stk. 2, eller et pengeinstitut, som har indgået en aftale om at være registreringsenhed. En registreringsenhed angiver ved indgåelse af aftale, hvilke funktioner og ydelser, som er knyttet til udstedelse og indrulling, som registreringsenheden ønsker at varetage. Erhvervsbrugere skal oprette og administrere digitale erhvervsidentiteter gennem serviceområdet Erhvervsadministration i NemLog-in, jf. § 8, stk. 3. Erhvervsbrugere kan herigennem tilknytte MitID-identifikationsmidler til de digitale erhvervsidentiteter.

Offentlige myndigheder, offentligretlige organer og juridiske enheder, som er oprettet i serviceområdet Erhvervsadministration i NemLog-in, betegnes som brugerorganisationer, jf. § 2, nr. 16.

Som en del af tilrådighedsstillelsen af MitID-løsningen kan en brugerorganisation anmode om at få udstedt MitID-identifikationsmidler dedikeret til organisationens erhvervsbrugere. Brugerorganisationen kan oprette og administrere digitale erhvervsidentiteter til enhedens erhvervsbrugere og tilknytte MitID-identifikationsmidler til disse.

Til § 4

Da MitID-løsningen er en ny løsning, er den derfor ikke lovreguleret i dag. Reglerne som fastsættes i medfør af § 4, vil delvist være en videreførelse af reglerne om udstedelse, spærring og håndtering af NemID i lov om NemID, jf. § 1, stk. 2, dog tilpasset de nye krav til sikkerhed fra NSIS-standarden.

Med den foreslåede § 4, *stk. 1, litra a*, fastslås det, at Digitaliseringsstyrelsen sikrer, at der sker identitetssikring af privatpersoner, registrering af identiteter, udstedelse, spærring og genåbning af MitID til privatpersoner efter reglerne fastsat i medfør af bestemmelsens stk. 2.

Begrebet MitID anvendes både for den nationale digitale identitet og for elektroniske identifikationsmidler, jf. den foreslåede § 2, nr. 2. Derfor vil udstedelse, suspendering, spærring og genåbning af MitID i praksis betyde, at Digitaliseringsstyrelsen sikrer udstedelse, suspendering, spærring og genåbning af nationale digitale identiteter og elektroniske identifikationsmidler.

Ved udstedelse og registrering af MitID sker der en identitetssikring og registrering af den fysiske

person, hvorefter der oprettes en digital identitet og udstedes elektroniske identifikationsmidler. For at sikre identiteten af den fysiske person, der anmoder om udstedelse af et MitID, identitetssikrer registreringsenheden den fysiske persons identitet. I praksis sker det ved, at en person legitimerer sig med gyldig legitimation fx pas, kørekort eller lignende. Den registreringsenhed, som har identitetssikret en privatperson, registrerer, hvordan identitetssikringen er sket

For at en privatperson kan gøre brug af den digitale identitet, skal denne således være i besiddelse af et elektronisk identifikationsmiddel, som er knyttet til den digitale identitet, jf. den foreslåede § 2, nr. 14. Et elektronisk identifikationsmiddel er fx kodeviser eller MitID-app. Privatpersoner, som ønsker at gøre brug af deres digitale identitet, skal således autentificere deres nationale digitale identitet ved anvendelse af det elektroniske identifikationsmiddel. En privatperson kan have flere typer af elektroniske identifikationsmidler.

Ved spærring af MitID, kan der foretages spærring af den nationale digitale identitet og af ét eller flere elektroniske identifikationsmidler. En privatperson som har fået udstedt MitID, kan således vælge at spærre enten den nationale digitale identitet eller det dertil hørende elektroniske identifikationsmiddel. Ved spærring af et elektronisk identifikationsmiddel vil det stadig være muligt at anvende den nationale digitale identitet med et nyt elektronisk identifikationsmiddel. Hvis der sker spærring af privatpersonens nationale digitale identitet, vil spærringen dog være fuldstændig.

Dette indebærer, at hverken den digitale identitet eller elektroniske identifikationsmidler knyttet til den digitale identitet efterfølgende kan anvendes. En privatperson, som har fået sin digitale identitet spærret, kan anmode om at få udstedt en ny digital identitet.

Det er ligeledes muligt for en privatperson at suspendere den digitale identitet. Ved en suspension af den digitale identitet, vil det efterfølgende være muligt at genåbne den digitale identitet, uden at gennemføre en ny registrering og udstedelse af MitID. Hvis det elektroniske identifikationsmiddel ikke er spærret, vil det være muligt for privatpersonen fortsat at anvende det elektroniske identifikationsmiddel sammen med den genåbnede digitale identitet.

Det vil derimod kun under ganske særlige omstændigheder være muligt at suspendere det elektroniske identifikationsmiddel. Dette gør sig fx gældende, hvis MitID-løsningen systemisk suspenderer MitID identiteten og det elektroniske identifikationsmiddel i en begrænset periode. Det kan fx være af sikkerhedsmæssige årsager. Efter en suspension vil både den digitale identitet og det elektroniske identifikationsmiddel kunne anvendes igen. Det forventes, at der fastsættes regler om suspension af det elektroniske identifikationsmiddel med hjemmel i den foreslåede § 4, stk. 2.

De nærmere regler om registrering, udstedelse, suspension, spærring og genåbning vil blive fastsat med hjemmel i § 4, stk. 2.

Med § 4, stk. 1, litra b, fastslås det desuden, at Digitaliseringsstyrelsen sikrer udstedelse, spærring af identifikationsmidler til erhvervsbrugere efter reglerne fastsat i medfør af stk. 2.

Bestemmelsen medfører, at erhvervsbrugere kan få udstedt et elektronisk identifikationsmiddel, som Digitaliseringsstyrelsen sikrer udstedelse, suspension, spærring og genåbning af. Regler for udstedelse, spærring og genåbning vil blive fastsat med hjemmel i den foreslåede § 4, stk. 2. Herved kan erhvervsbrugere få udstedt et elektronisk identifikationsmiddel i MitID. Erhvervsbrugere får til forskel fra privatpersoner ikke udstedt en digital identitet i MitID. En erhvervsbruger får derimod udstedt en digital identitet i NemLog-in i serviceområdet Erhvervsadministration.

Når en erhvervsbruger efter den foreslåede § 4, stk. 1, litra b, bliver oprettet med en erhvervsidentitet i serviceområdet Erhvervsadministration i NemLog-in og vil have udstedt et elektronisk MitID-identifikationsmiddel, som skal anvendes i erhvervsøjemed, foretages dette ligeledes gennem serviceområdet Erhvervsadministration i NemLog-in. Der henvises til bemærkningerne til § 8, stk. 3. Erhvervsbrugeren kan vælge at få koblet sit private MitID-identifikationsmiddel til en eller flere erhvervsidentiteter, eller

anvende et særskilt dedikeret MitID-identifikationsmiddel, som alene kan anvendes i erhvervsøjemed, og som kan tilknyttes én eller flere erhvervsidentiteter, som erhvervsbrugeren har. Koblingen mellem en erhvervsidentitet og et MitID-identifikationsmiddel udstedt til privatbrug forudsætter, at både den fysiske person, der er associeret med en offentlig myndighed, et offentligt organ eller en juridisk enhed, som accepterer, at den fysiske person anvender sit private MitID-identifikationsmiddel. Dette forhold kaldes det dobbelte frivillighedsprincip. Det dobbelte frivillighedsprincip hjemles i den foreslåede § 9, stk. 2 og stk. 3.

De nærmere betingelser for spærring, suspension og udstedelse vil blive fastsat i regler med hjemmel i § 4, stk. 2.

Det skal bemærkes, at hvis en privatperson er den eneste fult ansvarlige i en virksomhed, kan personen anvende sit private MitID (MitID privat til erhverv) uden at oprette sin juridiske enhed som brugerorganisation i Serviceområdet Erhvervsadministration i NemLog-in. Privatpersonen vil derved kunne anvende både sin digitale identitet og elektroniske identifikationsmiddel oprettet i MitID-løsningen, til personens juridiske enhed, hvis personen er den eneste tegningsberettigede for den juridiske enhed. Der henvises i øvrigt til bemærkningerne til den foreslåede § 8, stk. 3.

Formålet med identitetssikringen vil i hovedsagen være at sikre de forvaltningsretlige rammer om udstedelsesprocedurer af MitID til privatpersoner og erhvervsbrugere. Derudover er det formålet at sikre efterlevelse af NSIS-standarden.

Med det foreslåede *stk. 2* fastsættes en hjemmel til, at finansministeren fastsætter regler om forvaltningen af MitID-løsningen og MitID, herunder regler om udstedelse, suspension, spærring og genåbning af MitID og regler for indbringelse af klage over en afgørelse om udstedelse, suspension og spærring af MitID. Det forventes, at en klage over en afgørelse kan indbringes for Digitaliseringsstyrelsen efter genvurdering hos den registreringsenhed, der har truffet afgørelsen. Finansministeren vil tillige kunne fastsætte regler med krav, der stilles til privatpersoner og erhvervsbrugere ved løbende håndtering af MitID.

Det forventes, at der med hjemmel i den foreslåede bestemmelse blive fastsat nærmere regler for forvaltningen af MitID-løsningen og MitID, herunder processuelle regler om identitetssikring ved oprettelse af digitale identiteter, registrering af identiteter samt udstedelse, betingelser, der skal opfyldes for at kunne få udstedt MitID, samt hvilke vilkår, der løbende skal opfyldes for at besidde og anvende MitID, suspension, spærring, nyudstedelse og genåbning af MitID samt regler om en nedre aldersgrænse for at få udstedt et MitID.

Det er hensigten, at den nedre aldersgrænse fra indførelsen af MitID sættes til 13 år. Bestemmelsen omfatter derved selve forvaltningen af MitID, som er rettet mod privatpersoner og i et mere begrænset omfang erhvervsbrugere, idet erhvervsidentiteter håndteres i serviceområdet Erhvervsadministration i NemLog-in, jf. nærmere i den foreslåede § 8, stk. 3 og forvaltningen heraf i den foreslåede § 9.

Det er forventningen, at der med hjemmel i den foreslåede § 4, stk. 2, fastsættes regler om udstedelse af MitID. Udstedelse af MitID kræver, at den fysiske person gennemgår en identitetssikringsproces, som har til formål entydigt at identificere den pågældende fysiske person. Sagsbehandling i forbindelse med identitetssikring er en forvaltningsopgave. Dette indebærer, at også udpegede juridiske enheder, som foretager identitetssikring vil være underlagt forvaltningsregler. Der henvises til den foreslåede § 20. Formålet med identitetssikringen er at sikre, at privatpersoners identitet registreres korrekt, således at deres nationale digitale identiteter ikke kan forveksles med andres digitale identiteter. Samtidig skal det sikres, at NSIS overholdes ved registrering og udstedelse af MitID. Privatpersoner har alene et retskrav på at få udstedt MitID, hvis de opfylder betingelserne for udstedelse af MitID, som fastsat i medfør af denne foreslåede bestemmelse. Hvis fx en privatperson ikke kan dokumentere sin identitet, vil det have den konsekvens, at personen ikke kan få udstedt et MitID.

Ved udstedelse af MitID sker der en registrering af den fysiske person i MitID-løsningen. Det forventes, at der fastsættes nærmere regler om registrering i MitID med hjemmel i denne bestemmelse.

Det forventes endvidere, at der fastsættes nærmere regler om besiddelse og anvendelse af MitID, med hjemmel i den foreslåede bestemmelse. Regler om forvaltning af MitID fastsættes under inddragelse af hensyn til løsningens sikkerhed og privatpersoners og erhvervsbrugeres tillid til MitID-løsningen. I denne afvejning er det formålet at skabe en balance mellem hensynet til den enkelte privatpersons muligheder for at indgå i det digitale samfund og hensynet til den generelle tillid til MitID-løsningen. Reglerne skal være med til at sikre privatpersoner og juridiske enheder mod konkret misbrug og skal samtidig bidrage til at opretholde den samlede sikkerhed i MitID-løsningen. Der skal blandt andet fastsættes regler om hemmeligholdelse og beskyttelse af det elektroniske identifikationsmiddel, og at privatpersonen eller erhvervsbrugeren kognitivt skal have evnen til at forstå og følge reglerne, herunder beskytte det udstedte MitID og elektroniske identifikationsmiddel mod andres brug og misbrug. Der skal ligeledes fastsættes regler om, at privatpersoner og erhvervsbrugere skal tage rimelige forholdsregler for at beskytte de sikkerhedsmekanismer, der sikrer MitID mod kompromittering, ændring, tab og uautoriseret brug. Finansministeren vil tillige kunne fastsætte, hvilke konsekvenser det har, hvis en privatperson eller erhvervsbruger ikke overholder disse krav, efter MitID er udstedt til den pågældende. Det vil eksempelvis kunne fastsættes, at MitID spærres ved mistanke om misbrug eller brud på sikkerheden. Det forventes, at det bliver fastsat, at den fysiske person kan få udstedt MitID ved personligt fremmøde hos en registreringsenhed fx i et pengeinstitut eller hos en registreringsenhed i kommunernes borgerservicecentre.

Derudover forventes det, at der i lighed med i dag vil blive fastsat regler om, at udstedelse af MitID kan afslås, hvis en registreringsenhed vurderer, at en privatperson ikke er i stand til at sikre MitID mod misbrug eller videregivelse til tredjemand. Det forudsætter, at registreringsenheden som led i udstedelsesprocessen foretager et skøn af privatpersonens evner til at besidde, beskytte og sikre sit MitID. Reglerne herom fastsættes under inddragelse af hensyn til sikkerheden i løsningen og tilliden til anvendelsen af MitID.

Et afslag på udstedelse af MitID indebærer en væsentlig begrænsning i indehaverens digitale færden og udgør en forvaltningsretlig afgørelse.

Herudover vil en spærring foretaget af andre end indehaveren selv, udgøre en forvaltningsretlig afgørelse. En registreringsenhed vil fx kunne spærre et MitID, hvis der kan opstå tvivl om identiteten på den fysiske person stemmer overens med den digitale identitet. Ligeledes vil et MitID kunne suspenderes systemisk, hvis fx adgangskoden er skrevet forkert flere gange i træk. Det skal i den sammenhæng bemærkes, at både en hel eller en delvis spærring af MitID alene vil betragtes som en forvaltningsretlig afgørelse, hvis den foretages af Digitaliseringsstyrelsen eller af de offentlige myndigheder, offentlige organer eller juridiske enheder, der i medfør af den foreslåede § 5, stk. 1, er udpeget til på vegne af Digitaliseringsstyrelsen at varetage opgaver med blandt andet forvaltning af MitID samt opgaver i medfør af § 4, stk. 1.

Det forventes med den foreslåede bestemmelse i stk. 2, at finansministeren bemyndiges til at fastsætte nærmere regler for, hvornår og hvordan MitID kan spærres. Det er hensigten, at der både vil blive fastsat regler om, at en privatpersonen selv kan spærre sin digitale identitet, sit digitale identifikationsmiddel eller begge dele. Ligeledes forventes det, at en registreringsenhed kan spærre en digital identitet, et digitalt identifikationsmiddel eller begge dele. Ved en spærring af en digital identitet eller et digitalt identifikationsmiddel, er det nødvendigt at genregistrere og genudstede den digitale identitet, det digitale identifikationsmiddel eller begge dele til privatpersonen. Det forventes også, at der med hjemmel i den foreslåede bestemmelse, bliver fastsat regler om suspendering af den digitale identitet og i særlige tilfælde det elektroniske identifikationsmiddel. En suspendering vil i praksis betyde, at den digitale identitet er midlertidig spærret. Således vil det være muligt at genåbne den digitale identitet, uden at skulle foretage en ny registrering og udstedelse. En suspension kan fx foretages, hvis der er mistanke om, at MitID

er kompromitteret. Såvel en registreringsenhed som indehaveren af MitID skal kunne suspendere eller spærre MitID. En registreringsenhed er en enhed, som er udpeget af Digitaliseringsstyrelsen til at udstede og spærre MitID, fx borgerservice eller et pengeinstitut. Ligeledes kan en udpeget leverandør og forvalter, jf. § 5, stk. 1, af MitID-løsningen suspendere eller spærre en MitID-identitet, hvis det konstateres, at et MitID er kompromitteret eller det forsøges kompromitteret.

Spærring er endvidere relevant, når indehaveren ikke overholder reglerne for brug af MitID, fx hvis koder overlades til tredjemand. Spærring sker ligeledes, når det konstateres, at den fysiske person, der er indehaver af et MitID, er afgået ved døden. Bemyndigelsen skal sikre, at privatpersoner sikres de samme muligheder for fx klageadgang, uanset om det er offentlige myndigheder eller offentligretlige organer, som varetager disse opgaver, eller om opgaverne varetages af en juridisk enhed, jf. § 6, stk. 1.

Det forventes også, at der vil blive fastsat regler om erhvervsbrugere udstedelse og spærring af det elektroniske MitID-identifikationsmiddel, som disse kan få udstedt i medfør af § 4, stk. 1, litra b.

Med lovforslaget ændres der ikke på, at de forvaltningsretlige principper finder anvendelse også i den situation, hvor finansministeren udpeger en juridisk enhed til eksempelvis at varetage opgaven med at udstede MitID til privatpersoner. Hertil følger det af lovforslagets § 20, at forvaltningsretten finder anvendelse på afgørelser om forvaltning af MitID, hvilket blandt andet vil være tilfældet for afgørelser om afslag på udstedelse af MitID eller spærring af MitID.

Det forventes med den foreslåede stk. 2, at finansministeren skal fastsætte nærmere regler om adgangen til at klage over en afgørelse om afslag på udstedelse af MitID, spærring og suspension af MitID og genåbning af MitID.

Når der træffes en forvaltningsretlig afgørelse om afslag på udstedelse, spærring og suspension, skal der gives mulighed for at indgive en klage over afgørelsen, ligesom forvaltningslovens regler om afgørelsesvirksomhed skal iagttages. Det er således væsentligt, at en privatperson kan klage over et afslag på udstedelse, da et afslag kan have indgribende betydning for den persons digitale færden. Ligeledes er MitID en forudsætning for, at en privatperson kan tilgå Digital Post og anvende offentlige digitale selvbetjeningsløsninger. Privatpersoner, som ikke kan få udstedt MitID, vil ikke kunne betjene sig hos en offentlig myndighed eller et offentligretligt organ via den fællesoffentlige adgang. Det er op til den enkelte offentlige myndighed eller offentligretlige organ at beslutte, hvordan de vil understøtte en privatperson i dette tilfælde. De enkelte myndigheder vil i den sammenhæng være forpligtet til at vejlede privatpersoner efter de forvaltningsretlige regler, hvilket blandt andet indebærer, at en myndighed har pligt til at vejlede og hjælpe privatpersoner inden for de ressortområder, som de er ansvarlige for. Således har en myndighed pligt til at hjælpe en privatperson, der fx ikke kan få udstedt MitID til at agere inden for myndighedens område og give privatpersonen adgang til de oplysninger og den offentlige service, som andre privatpersoner kan tilgå ved brug af MitID.

Det forventes, at en afgørelse om afslag på udstedelse af MitID, spærring og suspension af MitID, efter genvurdering hos registreringsenheden, skal kunne indbringes for Digitaliseringsstyrelsen. Regler om dette forventes ligeledes fastsat med hjemmel i den foreslåede stk. 2.

Det bemærkes, at det er hensigten, at der udarbejdes én bekendtgørelse med regler for udstedelse og spærring af MitID samt om muligheden for at indbringe klager over afgørelser herom, således at de borgerrettede regler fastsættes samlet. Dette sker af hensyn til, at privatpersoner og erhvervsbrugere kan få et gennemsigtigt og samlet overblik over de regler, som retter sig mod dem.

De nærmere regler om tilrådighedsstilling og anvendelse af MitID-løsningen for offentlige myndigheder og offentligretlige organer fastsættes i medfør af den foreslåede § 16.

Finansministeren fastsætter ikke regler om udvikling og drift af MitID, idet disse forhold reguleres i kontrakten med den private virksomhed, offentlige myndighed eller offentligretlige organ, der kan udpeges i medfør af § 5, stk. 1.

Til § 5

MitID-løsningen er en ny løsning, og er derfor ikke lovreguleret i dag. Det forventes, at der videreføres regler fra lov om NemID med offentlige digital signatur, om udpegning af offentlige myndigheder, offentligretlige organer eller juridiske enheder til på vegne af Digitaliseringsstyrelsen at varetage opgaven med udvikling, drift, vedligeholdelse og forvaltning af MitID-løsningen.

Det fastslås med den foreslåede bestemmelse § 5, stk. 1, at Digitaliseringsstyrelsen kan udpege offentlige myndigheder, offentligretlige organer eller juridiske enheder til på vegne af Digitaliseringsstyrelsen at varetage opgaver efter § 3, stk. 1, 2. pkt., samt opgaver i medfør af § 4, stk. 1.

Enhver udpegning skal ske under overholdelse af udbudsreglerne.

Det påhviler Nets DanID A/S på vegne af Digitaliseringsstyrelsen at varetage driften af MitID-løsningen og at forestå udvikling og vedligeholdelse af løsningen i overensstemmelse med de kontraktuelle vilkår, som er fastsat i aftalen mellem Digitaliseringsstyrelsen og Nets DanID A/S.

Opgaverne inkluderer etablering og løbende tilpasning af løsningen samt varetagelse af den daglige drift i tæt samarbejde med Digitaliseringsstyrelsen og øvrige relevante aktører, herunder supportorganisationer og registreringsenheder. MitID-løsningen tilpasses løbende i takt med den teknologiske udvikling samt det skiftende trusselsbillede og ændrede samfundsbehov.

Det er hensigten med § 5, at Digitaliseringsstyrelsen kan udpege registreringsenheder, som på vegne af Digitaliseringsstyrelsen sikrer, at der sker identitetssikring af identiteter, registrering af identiteter, udstedelse, spærring og genåbning af MitID til privatpersoner, jf. opgaverne i lovforslagets § 4, stk. 1. Registreringsenhederne kan både være offentlige myndigheder, offentligretlige organer og juridiske enheder. Det er hensigten, at de enheder, som i dag varetager opgaven som registreringsenheder for udstedelse af NemID, så vidt muligt kan fortsætte med at varetage denne opgave for MitID.

Opgaven med forvaltningen af MitID-løsningen omfatter desuden supporten af løsningen. Supportopgaven kan på baggrund af bestemmelsen varetages af en offentlig myndighed, et offentligretligt organ eller en juridisk enhed. Digitaliseringsstyrelsen kan således udpege offentlige og private supportorganisationer, der har som opgave at yde support til privatpersoner og erhvervsbrugere og derved udføre slutbrugersupport for MitID-løsningen. Der kan opstå behov for, at supportorganisationen træffer afgørelser om fx spærring af MitID under behandlingen af en supporthenvendelse.

Når en supportorganisation træffer afgørelser, er den på samme måde som en registreringsenhed, underlagt regler og instrukser fastlagt i samarbejde mellem partnerskabet og den private virksomhed, som er udpeget i medfør af bestemmelsen. For at kunne agere som supportorganisation skal der være indgået en aftale om varetagelse af support.

Da MitID-løsningen er en ny løsning, er løsningen ikke lovreguleret i dag.

Der findes ikke regulering, som forpligter kommunalbestyrelsen til at varetage opgaver for NemID.

Det følger af den foreslåede bestemmelses stk. 2, at kommunalbestyrelsen på vegne af Digitaliseringsstyrelsen skal varetage opgaver i medfør af § 4, stk. 1.

Kommunerne er i dag ikke forpligtet til at håndtere udstedelse og spærring af NemID, selvom mange af de kommunale borgerservicecentre allerede i dag varetager opgaven. Med bestemmelsen forpligtes kommunerne til at varetage opgaverne med registrering af identiteter, udstedelse, spærring og genåbning af MitID til privatpersoner. Disse opgaver varetages i dag i registreringsenheder, som findes i de fleste kommuner. Registreringsenheder findes i dag primært i forbindelse med kommunale borgerservicecentre.

Kommunerne skal ved varetagelsen af opgaverne i henhold til § 4, stk. 1, sikre, at det fortsat er let og nemt tilgængeligt for privatpersoner at få hjælp til oprettelsen af MitID, fx ved at opgaverne placeres i kommunale borgerservicecentre eller lignende. Kommunalbestyrelsen skal endvidere ved varetagelsen af

opgaverne, følge de almindelige forvaltningsretlige regler, som relaterer sig til de pågældende opgaver, herunder skal privatpersoner tilbydes vejledning, jf. vejledningspligten i forvaltningslovens § 7, stk. 1.

Til § 6

MitID-løsningen er en ny løsning og der findes derfor ikke gældende ret for MitID. For NemID-løsningen findes der ikke ved lov en forpligtelse for offentlige myndigheder og offentligretlige organer til at sikre, at privatpersoner og erhvervsbrugere kan anvende NemID til at få adgang til de pågældende myndigheders digitale selvbetjeningsløsninger.

Med den foreslåede bestemmelse i § 6, stk. 1 fastslås, at når offentlige myndigheder og offentligretlige organer anvender digitale selvbetjeningsløsninger til at udføre en myndighedsopgave, skal de sikre, at privatpersoner og erhvervsbrugere med MitID gives adgang til selvbetjeningsløsningen, hvis adgangen kræver sikker autentifikation. MitID-løsningen skal i dette tilfælde anskaffes fra Digitaliseringsstyrelsen.

Formålet med § 6, stk. 1, er at sikre, at offentlige myndigheder og offentligretlige organer, når de udfører myndighedsopgaver i digitale selvbetjeningsløsninger, der kræver sikker autentifikation, stiller MitID-løsningen til rådighed for privatpersoner og erhvervsbrugere. Herved sikres en ensartet og sikker brugerrejse for privatpersoner og erhvervsbrugere på tværs af den offentlige sektor. Pligten, i medfør af den foreslåede bestemmelse, er fastsat med henblik på at sikre den offentlige orden og sikkerhed, samt hensynet til de samfundsøkonomiske overvejelser ved fælles anskaffelse af it-løsninger i staten. Se nærmere herom i de almindelige bemærkninger afsnit 2.1.2.2.

Det er den enkelte offentlige myndighed eller det offentligretlige organ, som må vurdere, om pågældende offentlige myndighed eller offentligretlige organ udfører en myndighedsopgave. I vurderingen kan medregnes opgaver, som er pålagt den offentlige myndighed eller det offentligretlige organ ved lov eller anden retsakt, opgaver hvor myndigheden eller det offentligretlige organ er ordregivende myndighed og desuden opgaver, som umiddelbart synes at ligge inden for myndigheds eller det offentligretlige organs ressort og som løses af myndigheden eller det offentligretlige organ. I vurderingen af om der udføres en myndighedsopgave suppleres det formelle kriterier for myndighedens eller det offentligretlige organs struktur med et materielt kriterium. Der henvises i øvrigt til definitionen af offentlige myndighed og offentligretligt organ. De offentlige myndigheder, som er omfattet af pligten i § 6, stk. 1, er offentlige myndigheder i henhold til denne lovs definition i § 2, nr. 10. De offentligretlige organer som er omfattet af pligten i § 6, stk. 1, er offentligretlige organer i henhold til denne lovs definition i § 2, nr. 11.

Pligten i medfør af den foreslåede bestemmelse, afhænger endvidere af, at den digitale selvbetjeningsløsning kræver sikker autentifikation. Sikker autentifikation er defineret i den foreslåede § 2, nr. 5, og omfatter NSIS sikringsniveauerne betydelig og høj. Det er tjenesteudbyderen selv, som med udgangspunkt i NSIS skal vurdere hvilket sikringsniveau selvbetjeningsløsningen skal være på. For adgang til MitID-løsningen på sikringsniveau lav henvises til den foreslåede § 6, stk. 2.

Anskaffelsen af MitID skal ske fra Digitaliseringsstyrelsen. Med den nye brokerstruktur, vil det ikke længere være muligt, at tilkoble en digital selvbetjeningsløsning direkte til MitID-løsningen. For mere om brokerstrukturen henvises til de almindelige bemærkninger afsnit 2.1.2 og afsnit 2.3. Derfor vil anskaffelsen af MitID-løsningen i praksis foregå igennem tilslutning til NemLog-in, som den fællesoffentlige broker. Herved vil alle tjenesteudbydere, som er forpligtet til at stille MitID til rådighed for privatpersoner og erhvervsbrugere, skulle tilkobles NemLog-in, for at en privatperson eller en erhvervsbruger kan anvende den pågældende digitale selvbetjeningsløsning. I nogle tilfælde vil det være relevant, at efterleve pligten til at anskaffe MitID-løsningen igennem tilslutning til en NSIS-anmeldt broker, som er tilsluttet til NemLog-in eller en lokal identitetsgarant tilsluttet NemLog-in. Der henvises i øvrigt til § 11 for pligter til anvendelse af Serviceområder i NemLog-in. Ved en tilkobling til NemLog-in skal tjenesteudbyderen kunne iagttage de aftalevilkår, som gælder for tjenesteudbydere, og som fastsættes af

Digitaliseringsstyrelsen. Offentlige myndigheder og offentligretlige organer i rollen som tjenesteudbydere skal iagttage regler fastsat i medfør af § 16.

Det bemærkes, at retten til at anvende MitID-løsningen skal ses i sammenhæng med den foreslåede § 15, stk. 3, om opkrævning af gebyr og vederlag. Det indebærer, at de offentlige myndigheder og offentligretlige organer skal betale for at anvende MitID-løsningen, uanset om de har en lovbestemt ret eller pligt til at anvende den, jf. § 15, stk. 3.

Med den foreslåede bestemmelse i § 6, stk. 2, sikres det, at når offentlige myndigheders og offentligretlige organers digitale selvbetjeningsløsninger ikke anvendes til at udføre en myndighedsopgave, eller hvis adgangen til løsningerne ikke kræver sikker autentifikation, kan de offentlige myndigheder og offentligretlige organer give privatpersoner og erhvervsbrugere adgang til løsningerne med MitID. MitID-løsningen skal i dette tilfælde anskaffes fra Digitaliseringsstyrelsen.

Bestemmelsens sigte er offentlige myndigheder og offentligretlige organer i de tilfælde, hvor de ikke er forpligtet til at anvende MitID-løsningen, jf. bestemmelsens stk. 1, kan vælge at anskaffe MitID-løsningen. Anskaffelsen vil ske fra Digitaliseringsstyrelsen. Det fremgår af vejledning til digitaliseringsklar lovgivning, at offentlige myndigheder i det omfang, det er muligt og hensigtsmæssigt, bør anvende eksisterende fællesoffentlig infrastruktur, så der sikres størst muligt genbrug og sammenhæng på tværs. Med den foreslåede bestemmelses 1. pkt. gives en ret til at offentlige myndigheder og offentligretlige organer kan give privatpersoner og erhvervsbrugere adgang til digitale selvbetjeningsløsningerne med MitID uden at gennemføre et selvstændigt udbud, såfremt løsningen anskaffes fra Digitaliseringsstyrelsen gennem NemLog-in som broker. Dette betyder at, når en offentlig myndighed ikke er omfattet af pligten i medfør af den foreslåede bestemmelse § 6, stk. 1, vil det forsat være muligt for de offentlige myndigheder og de offentligretlige organer at give adgang til deres digitale selvbetjeningsløsninger, uden at gå i udbud.

Det bemærkes, at retten til at anvende MitID-løsningen skal ses i sammenhæng med den foreslåede § 15, stk. 3, om opkrævning af gebyr og vederlag. Det indebærer, at de offentlige myndigheder og offentligretlige organer skal betale for at anvende MitID-løsningen, uanset om de har en lovbestemt ret eller pligt til at anvende den, jf. § 15, stk. 3.

Til § 7

Da MitID-løsningen er en ny løsning, findes der ikke gældende ret på området. Med MitID-løsningen hjemtager staten ejerskabet og ansvaret for løsningen. Dette gør sig ikke gældende for NemID, hvorfor lov om NemID ikke regulerer tilrådighedsstillelse af løsningen for juridiske enheder.

Med den foreslåede § 7 fastslås det, at juridiske enheder i rollen som tjenesteudbydere kan anvende MitID-løsningen.

Med den foreslåede § 7 får juridiske enheder mulighed for at anvende MitID-løsningen som tjenesteudbydere i deres digitale selvbetjeningsløsning. Det er således frivilligt for de juridiske enheder, om de vil anvende MitID-løsningen som tjenesteudbydere.

For at anvende MitID-løsningen skal den juridisk enhed iagttage aftalevilkår for tjenesteudbydere og den foreslåede bestemmelse § 15, stk. 1, om opkrævning af gebyr og vederlag for anvendelse af løsningen. Det indebærer, at juridiske enheder skal betale for at anvende MitID-løsningen.

Med den nye brokerstruktur, vil det ikke længere være muligt at tilkoble en digital selvbetjeningsløsning direkte til MitID-løsningen. Derfor vil det tillige være nødvendigt for den juridiske enhed for at tilgå MitID, at indgå aftale via en broker, som er certificeret til at være MitID-broker af Digitaliseringsstyrelsen. Juridiske enheder kan indgå aftale med NemLog-in, om at anvende denne som broker eller der kan indgås aftale med en hvilken som helst anden broker, som er certificeret af Digitaliseringsstyrelsen, til at være broker for MitID. Den juridiske enhed skal således igennem en aftale acceptere de aftalevilkår, som er fastsat af Digitaliseringsstyrelsen overfor brokern, for at kunne anvende MitID-løsningen.

Bestemmelsen indeholder ikke et retskrav.

Til § 8

Der er ikke gældende ret som regulerer tilrådighedsstillelsen af NemLog-in.

Med den foreslåede bestemmelse i § 8, *stk. 1* fastslås, at Digitaliseringsstyrelsen stiller NemLog-in til rådighed for offentlige myndigheder, offentligretlige organer og juridiske enheder.

Den foreslåede bestemmelse indebærer, at Digitaliseringsstyrelsen pålægges myndighedsopgaven at stille NemLog-in til rådighed for offentlige myndigheder, offentligretlige organer og juridiske enheder.

I NemLog-in kan de offentlige myndigheder, offentligretlige organer og juridiske enheder agere i to forskellige roller: som tjenesteudbyder eller som brugerorganisation. En tjenesteudbyder er ansvarlig for én eller flere digitale selvbetjeningsløsninger. Offentlige myndigheder, offentligretlige organer og juridiske enheder agerer i rollen som tjenesteudbydere, når de anvender serviceområderne Login og autentifikation, Digital signering og Digital repræsentation i deres selvbetjeningsløsninger. En brugerorganisation er tilsluttet og anvender serviceområdet Erhvervsadministration i NemLog-in til deres erhvervsbrugere.

Digitaliseringsstyrelsen stiller NemLog-in til rådighed for offentlige myndigheder, offentligretlige organer og juridiske enheder som tjenesteudbydere, hvorefter disse har pligt eller ret til at tilbyde fysiske personer og erhvervsbrugere anvendelse af NemLog-ins serviceområder i deres digitale selvbetjeningsløsninger, jf. bemærkningerne til bestemmelsens *stk. 2*. Offentlige myndigheder, offentligretlige organer og juridiske enheder kan i rollen som brugerorganisationer oprette og administrere erhvervsbrugere, som kan anvende digitale selvbetjeningsløsninger på vegne af organisationen.

Med den foreslåede § 8, *stk. 1, 2. pkt.*, fastslås det, at Digitaliseringsstyrelsen sikrer udvikling, drift og vedligeholdelse af NemLog-in.

I Digitaliseringsstyrelsens opgave med at sikre drift og forvaltning, indgår ligeledes en sikring af, at der sker drift og support for løsningen. Tjenesteudbydere og brugerorganisationerne, som anvender de enkelte serviceområder, har således som en del af serviceområdet mulighed for at få både teknisk support og slutbrugersupport til blandt andet tilslutning til serviceområderne. Dele af supportopgaverne er vederlagsbelagte, jf. § 15, *stk. 2*.

I gældende ret er de serviceområder, som er indeholdt i den næste generation af NemLog-in ikke reguleret. Det skal dog bemærkes, at det med NemID, som er den eksisterende løsning er muligt at signere lokalt udelukkende ved brug af NemID, idet der til det enkelte NemID er knyttet nøgler og certifikat til afgivelse af digital signatur. Ved overgangen fra NemID til MitID vil signering under anvendelse af MitID kunne ske ved brug af serviceområdet Digital signering i NemLog-in, jf. den foreslåede § 8, *stk. 2, nr. 3*, idet MitID som eID ikke indeholder de signaturgenereringsdata, der er nødvendige for at afgive signaturer. Ovenstående ændrer ikke på, at det fortsat vil være muligt at anvende private signeringsløsninger.

Det betyder, at i gældende lovgivning, hvor der i dag foreskrives anvendelse af NemID, OCES eller digital signatur eller digital signatur med et sikkerhedsniveau svarende til OCES eller højere til login og autentifikation, skal dette efter denne lovs ikrafttræden sidestilles med og være opfyldt ved anvendelse, og anvendelse af MitID på sikringsniveau betydelig eller højere eller et nationalt eID med sikringsniveau betydelig eller højere.

I tilfælde, hvor der i gældende lovgivning foreskrives, at underskrift kan afgives ved anvendelse af NemID, OCES, digital signatur eller digital signatur med et sikkerhedsniveau svarende til OCES eller højere, vil dette ikke fremadrettet være muligt alene ved autentifikation med MitID. En digital underskrift kræver i stedet anvendelse af serviceområdet Digital signering. Selve autentifikation ved afgivelsen af underskriften kan dog ske ved anvendelse af MitID, men den digitale signering vil dog ske ved anvendelsen af serviceområdet Digital signering. Selvom Digitaliseringsstyrelsen fremadrettet vil

varetage rollen som certificeringscenter for serviceområdet Digital signering, er regulering af certificeringscenteret ikke omfattet af denne lov, men følger af eIDAS-forordningen. Digitaliseringsstyrelsen har udformet, varetager og vedligeholder på vegne af den danske stat de gældende certifikatpolitikker, som stiller krav til udbydere af tillidstjenester i Danmark. Digitaliseringsstyrelsens certifikatpolitik indeholder hovedkategorierne ”OCES-certifikater” og ”kvalificerede certifikater”.

Med den foreslåede § 8, stk. 2 fastlægges det, at NemLog-in indeholder en række serviceområder til tjenesteudbydere.

Bestemmelsen indeholder en opstilling af hvilke serviceområder NemLog-in indeholder til tjenesteudbydere, og som Digitaliseringsstyrelsen leverer og stiller til rådighed for at offentlige myndigheder, offentligretlige organer og juridiske enheder kan tilslutte sig, jf. nr. 1-3.

Den foreslåede § 8, stk. 2, nr. 1, fastsætter, at NemLog-in indeholder serviceområdet login og autentifikation for tjenesteudbydere, som sikrer den service, at privatpersoner og erhvervsbrugere kan tilgå digitale selvbetjeningsløsninger.

Med bestemmelsens nr. 1 foreslås det, at Login og autentifikation udgør et serviceområde i NemLog-in. Det foreslåede serviceområde muliggør, at der med autentifikation af digitale identiteter kan logges på digitale selvbetjeningsløsninger tilsluttet NemLog-in eller anden NSIS-anmeldt broker tilsluttet NemLog-in. Offentlige myndigheder og offentligretlige organers autentifikation i den fællesoffentlige infrastruktur af digitale identiteter for privatpersoner sker i MitID-løsningen gennem NemLog-in. Erhvervsbrugere autentificeres i serviceområdet Erhvervsadministration eller gennem en lokal identitetsgarant tilsluttet Erhvervsadministration i NemLog-in, jf. lovforslagets § 8, stk. 3.

I praksis betyder det fx, at når en privatperson eller en erhvervsbruger, som har fået udstedt et elektronisk identifikationsmiddel i MitID-løsningen, logger ind på en digital selvbetjeningsløsning, som er tilsluttet NemLog-in eller en NSIS-anmeldt broker koblet til NemLog-in, sender NemLog-in en digital autentifikationsanmodning til MitID-løsningen. MitID-løsningen sender herefter et sikkert svar tilbage til NemLog-in, som indeholder autentifikationssvaret til den pågældende selvbetjeningsløsning. Der henvises til lovforslagets almindelige bemærkninger afsnit 7.3.1 vedrørende behandling af personoplysninger.

Funktionen log-in muliggør, at privatpersoner og erhvervsbrugere kan tilgå digitale selvbetjeningsløsninger efter, at de har foretaget den påkrævede autentifikation over for den selvbetjeningsløsning, som de ønsker at tilgå.

Log-in og autentifikation vil for privatpersonen og erhvervsbrugeren blive oplevet som en samlet proces.

Derudover indeholder serviceområdet funktionen Single sign-on. Funktionen Single sign-on kan alene anvendes af offentlige myndigheder og offentligretlige organer, når de udfører en myndighedsopgave, jf. den foreslåede § 11, stk. 1, nr. 1.

Med funktionen Single sign-on kan en privatperson eller en erhvervsbruger tilgå flere offentlige digitale selvbetjeningsløsninger på baggrund af et enkelt login, såfremt selvbetjeningsløsningerne er på samme NSIS-sikringsniveau. Herved kan der for privatpersoner og erhvervsbrugere etableres en bedre brugerrejse og mere effektiv anvendelse af offentlige digitale selvbetjeningsløsninger. Hvis en selvbetjeningsløsning kræver et højere NSIS-sikringsniveau end den forrige, vil det kræve, at den fysiske person eller erhvervsbrugeren foretager en ny og stærkere autentifikation for at kunne tilgå selvbetjeningsløsningen med det højere NSIS-sikringsniveau. Det betyder i praksis, at der skal foretages en ny autentifikation, med en yderligere anerkendt faktor, det kunne fx være ved anvendelse af et supplerende identifikationsmiddel.

Den foreslåede § 8, stk. 2, nr. 2, litra a, fastsætter, at NemLog-in indeholder serviceområdet Digital repræsentation til tjenesteudbydere, som sikrer Digital repræsentation af en privatperson, således at privatpersonen ved anvendelse af en digital selvbetjeningsløsning kan lade sig repræsentere digitalt af en

anden privatperson, af en erhvervsbruger eller af en juridisk enhed over for en offentlig myndighed eller et offentligretligt organ, som udbyder en digital selvbetjeningsløsning.

Med bestemmelsens foreslåede litra a, udgør Digital repræsentation et serviceområde i NemLog-in. Digital repræsentation i NemLog-in finder primært anvendelse for privatpersoner, som kan lade sig repræsentere digitalt af en tredjepart. En privatperson kan administrere og afgive digital repræsentation til en anden privatperson, en erhvervsbruger eller en juridisk enhed. En privatperson kan gennem serviceområdet Digital repræsentation i NemLog-in tildele og administrere afgivne repræsentationer.

En privatperson kan lade sig repræsentere i serviceområdet Digital repræsentation i NemLog-in, men vil ikke kunne overlade sin digitale identitet eller identifikationsmiddel i MitID til en anden.

Det er teknisk muligt for en privatperson at anmode en anden privatperson om at repræsentere sig gennem Digital repræsentation i NemLog-in.

Denne funktion muliggør, at en borger, der ikke er digital parat, alligevel har mulighed for at blive understøttet på digitale selvbetjeningsløsninger ved anvendelsen af serviceområdet Digital signering. Den udpegede repræsentant kan således påbegynde oprettelsen af repræsentationsforholdet i selve tilslutningsflowet, hvorefter repræsentationsafgiver senere kan tilslutte sig flowet analogt.

Serviceområdet Digital repræsentation udgør en digital repræsentationsløsning, som understøtter forvaltningslovens § 8, stk. 1 om repræsentation i forvaltningsretlig sammenhæng, hvor det kræves, at en part i en sag på ethvert tidspunkt af sagens behandling kan lade sig repræsentere eller bistå af andre. Digital repræsentation understøtter digital repræsentation på flere myndighedsområder og centraliserer muligheden for at afgive digitale fuldmagter i offentligt regi, hvor en privatperson ønsker at lade sig repræsentere af en tredjepart. Folketingets Ombudsmand har i FOB 2019-11 understreget, at en kommunes digitale selvbetjeningsløsning bør understøtte muligheden for partsrepræsentation, eller at kommunen som minimum bør vejlede herom. Den digitale repræsentationsløsning i serviceområdet Digital repræsentation er dermed central for at skabe sammenhæng mellem myndigheders pligt til at anvende digitale selvbetjeningsløsninger og privatpersoners retsgarantier i forhold til repræsentation, som fastsat i forvaltningsloven. Digital repræsentation er eksklusiv i den forstand, at det er den eneste digitale løsning i Danmark, hvor der kan foretages repræsentation på flere myndighedsområder. Serviceområdet Digital repræsentation gør hermed muligheden for digital repræsentation enkel, særligt hvis en privatperson ønsker repræsentation på flere myndighedsområder.

Der kan ikke efter den foreslåede bestemmelse udledes en ret til partsrepræsentation. Retten til partsrepræsentation følger alene af forvaltningslovens § 8. Privatpersoner og juridiske enheder, der ønsker partsrepræsentation, skal således fortsat påberåbe sig hjemlen i forvaltningsloven. Den foreslåede bestemmelse om serviceområdet Digital repræsentation i NemLog-in har alene til formål at give hjemmel til, at denne service indgår i NemLog-in, som Digitaliseringsstyrelsen er forpligtet til at stille til rådighed.

Serviceområdet Digital repræsentation indeholder også andre former for repræsentation end partsrepræsentation, fx understøtter serviceområdet, at værger i nogle tilfælde vil kunne anmode om at agere som digital repræsentant i overensstemmelse med værgemålet.

De nærmere myndighedsområder, der kan afgives digital repræsentation til, er defineret af myndigheden som tjenesteudbyder og er specifikt tilrettet tjenesteudbyderens digitale selvbetjeningsløsning. I den forbindelse er det en forudsætning, at en tjenesteudbyders digitale selvbetjeningsløsninger er tilsluttet NemLog-in.

En privatperson forpligtes ikke til at lade sig repræsentere digitalt og skal kunne vælge at lade sig repræsentere analogt, hvis privatpersonen ikke ønsker at anvende en digital repræsentationsløsning.

Serviceområdet har den funktion, at Digitaliseringsstyrelsen forvalter oprettelse og tilbagekaldelse af et digitalt repræsentationsforhold i de tilfælde, hvor repræsentationsforholdet oprettes på anmodning fra repræsentanten. Tjenesteudbydere, som anvender serviceområdet Digital repræsentation, overlader derfor

den praktiske håndtering af oprettelse og tilbagekaldelse af repræsentationsforholdet i serviceområdet Digital repræsentation til Digitaliseringsstyrelsen, når det er repræsentanten, der anmoder om oprettelse af repræsentationsforholdet. Når anmodningen om oprettelse af et repræsentationsforhold afgives af fuldmagtsgiveren, varetages behandlingen af anmodningen af borgerservice eller tjenesteudbydere selv. I forhold til hvilke offentlige myndigheder og offentligretlige organer, som har pligt eller ret til at stille servicen Digital repræsentation til rådighed for privatpersoner og erhvervsbrugere, henvises i øvrigt til bemærkningerne til lovforslagets kapitel 8 om anvendelse af NemLog-in.

Digital repræsentation kan alene anvendes i digitale selvbetjeningsløsninger, hvor en offentlig myndighed eller et offentligretligt organ udfører myndighedsopgaver, jf. § 11, stk. 1, nr. 2. Det er således ikke muligt at anvende serviceområdet til opgaver, som ikke er myndighedsopgaver. Serviceområdet Digital repræsentation fungerer derved som en offentlig central repræsentationsløsning til repræsentationsstyring, der kan anvendes af en privatperson eller en tegningsberettiget erhvervsbruger, som ønsker at lade sig repræsentere på ét eller flere myndighedsområder.

Den foreslåede § 8, stk. 2, nr. 2, litra b, fastsætter, at NemLog-in indeholder serviceområdet Digital repræsentation til tjenesteudbydere, som sikrer Digital repræsentation af en juridisk enhed, således at en erhvervsbruger, der selvstændigt kan repræsentere en juridisk enhed, kan repræsentere enheden ved anvendelse af en digital selvbetjeningsløsning over for en offentlig myndighed eller et offentligretligt organ, som udbyder en digital selvbetjeningsløsning.

Den foreslåede bestemmelse i litra b skal muliggøre at anvende Digital repræsentation i erhvervsøjemed for en juridisk enhed. Det er kun en virksomheds tegningsberettigede, der kan tegne en juridisk enhed fuldstændigt, som kan anvende serviceområdet, dvs. både tegningsberettigede i enkeltmandsvirksomheder og i fx anpartsvirksomheder kan anvende løsningen.

Det er en forudsætning, at den tegningsberettigede anvender MitID privat til erhverv for at anvende serviceområdet Digital repræsentation og selvstændigt kan repræsentere den juridiske enhed. Når erhvervsbrugere, som anvender MitID privat til erhverv, afgiver rettigheder til en anden erhvervsbruger benævnes det som digitale erhvervsfuldmagter i NemLog-in.

De områder, der kan afgives Digital repræsentation til, er på forhånd defineret af den offentlige tjenesteudbyder og er specifikt tilrettet den enkelte offentlige tjenesteudbyders digitale selvbetjeningsløsning. I den forbindelse er det en forudsætning, at den offentlige tjenesteudbyders digitale selvbetjeningsløsninger er tilsluttet NemLog-in samt serviceområdet Digital repræsentation. Digital repræsentation kan alene anvendes i digitale selvbetjeningsløsninger, hvor en offentlig myndighed eller et offentligretligt organ udfører myndighedsopgaver, jf. § 11, stk. 1, nr. 2. Det er således ikke muligt at anvende serviceområdet til opgaver, som ikke er myndighedsopgaver. Serviceområdet Digital repræsentation fungerer derved som en offentlig central repræsentationsløsning til repræsentationsstyring, der kan anvendes af en privatperson eller en tegningsberettiget erhvervsbruger, som ønsker at lade sig repræsentere på ét eller flere myndighedsområder.

I bestemmelsens foreslåede § 8, stk. 2, nr. 3, litra a fastsættes, at offentlige myndigheder, offentligretlige organer og juridiske enheder kan udstille digital signering af dokumenter i digitale selvbetjeningsløsninger.

Når offentlige myndigheder, offentligretlige organer og juridiske enheder anvender serviceområdet Digital signering, jf. litra a, gør de det i rollen som tjenesteudbydere, idet de herved udbyder serviceområdet Digital signering som tjeneste på deres digitale selvbetjeningsløsning.

Tjenesteudbydere kan således i serviceområdet Digital signering udstille Digital signering af dokumenter i digitale selvbetjeningsløsninger tilsluttet NemLog-in. Herved kan, kan privatpersoner og erhvervsbrugere som led i anvendelsen af den digitale selvbetjeningsløsning signere dokumenter hos tjenesteudbyderen.

Ved udstilling af Digital signering forstås, at en tjenesteudbyder i deres digitale selvbetjeningsløsninger muliggør, at en privatperson eller en erhvervsbruger kan anvende signeringsservicen. For at offentlige myndigheder, offentligretlige organer og juridiske enheder kan anvende serviceområdet Digital signering i NemLog-in, skal de tilsluttes som tjenesteudbydere, så de kan udbyde signeringsservicen til signering af indhold i deres digitale selvbetjeningsløsning.

Signeringsservicen lever op til de lovmæssige krav om Digital signering, som er fastsat i eIDAS-forordningen.

Digitaliseringsstyrelsen varetager således gennem NemLog-in serviceområdet Digital signering udstedelse af kvalificerede certifikater og kvalificerede segl på vegne af den danske stat. For at varetage denne opgave, etablerer Digitaliseringsstyrelsen et certificeringscenter gennem NemLog-in, som muliggør udstedelse af certifikater, tidsstempling og signering. Dette indebærer, at Digitaliseringsstyrelsen selvstændigt varetager rollen som certificeringscenter. Certificeringscenteret forestår ligeledes udstedelse af OCES-certifikater og kvalificerede certifikater, der kan udstedes til brugerorganisationer i serviceområdet Erhvervsadministration, jf. bemærkningerne til § 8, stk. 3.

Med bestemmelsens § 8, stk. 2, nr. 3, litra b, sikres med serviceområdet Digital signering, at privatpersoner og erhvervsbrugere kan signere digitale dokumenter og validere signerede dokumenters digitale signatur og integritet.

I serviceområdet Digital signering stilles en signeringsservice til rådighed, der giver mulighed for afgivelse af digitale signaturer på digitale dokumenter. Signeringen sker i praksis ved anvendelsen af en digital identitet og et elektronisk identifikationsmiddel til brug for autentifikation af privatpersonen eller erhvervsbrugeren over for signeringstjenesten i serviceområdet Digital signering, hvorefter signaturen kan afgives. På baggrund af den gennemførte autentifikation sikrer servicen, at det er muligt at identificere afgiveren af den digitale signatur. Den digitale signering sikrer det digitale dokumentets integritet, idet dokumentet ikke efterfølgende kan ændres, uden at dette kan konstateres i forbindelse med en verifikation af signaturen på dokumentet.

Som en del af serviceområdet Digital signering kan privatpersoner og erhvervsbrugere anvende en valideringstjeneste, der giver mulighed for at kontrollere integriteten af det digitalt signerede dokument. Valideringstjenesten kan således afgøre, om der efter afgivelsen af signaturen er foretaget ændringer i dokumentet.

For erhvervsbrugere vil kunne foretage en digital signering i serviceområdet Digital signering ved brug af en digital identitet og identifikationsmiddel udstedt til en erhvervsbruger. Det vil også være muligt at foretage digital signering i serviceområdet Digital signering ved brug af et MitID udstedt til privatbrug, men som anvendes til erhverv, forudsat at privatpersonen hæfter fuldt ud for den juridiske enheds aktiviteter. Dette er fx tilfældet i enkeltmandsvirksomheder.

Serviceområdet Digital signering giver således mulighed for at afgive en digital signatur med samme retsvirkning som en fysisk underskrift. Der henvises til eIDAS-forordningens artikel 25, der beskriver retsvirkningen af digitale signaturer. Afgivelsen af en digital signatur vil ske på baggrund af sikker autentifikation.

Digital signering sker i praksis ved, at underskriver autentificerer sig ved anvendelsen af sin digitale identitet og elektroniske identifikationsmiddel. På den baggrund sikres ægtheden og uafviseligheden af den digitale signatur, og det er derved muligt at identificere afgiveren af den digitale signatur. Signeringen sikrer ligeledes det digitale dokumentets integritet og bevisværdi, idet det ved efterfølgende verifikation af signaturen vil fremgå, om dokumentet er blevet ændret.

Digitaliseringsstyrelsen må behandle persondata i forbindelse med valideringen af en digital signatur afgivet i serviceområdet Digital signering i NemLog-in, jf. den forslåede § 14.

Når et dokument efter Digital signering skal valideres, foregår det i NemLog-in, som udstiller en

valideringstjeneste, hvorfra der kan foretages en validering. Valideringstjenesten kan tilgås af privatpersoner eller erhvervsbrugere på den måde, at et digitalt dokument overføres til validering i tjenesten. En privatperson eller en erhvervsbruger kan således anvende valideringstjenesten i NemLog-in til at validere digitalt signerede dokumenter og validere integriteten af disse dokumenter. I forbindelse med valideringen konstateres det således, om der er foretaget ændringer i det signerede dokument, efter at det er blevet signeret.

Med det foreslåede § 8, stk. 3, litra a, foreslås det, at NemLog-in indeholder serviceområdet Erhvervsadministration til brugerorganisationer, som sikrer at offentlige myndigheder, offentligretlige organer og juridiske enheder kan oprette, administrere og anvende digitale erhvervsidentiteter samt tildele og administrere elektroniske identifikationsmidler, hvis de opfylder betingelserne for identitetssikring ved oprettelse som brugerorganisation, som nærmere fastsat i medfør af § 9, stk. 4.

Erhvervsadministration udgør et serviceområde i NemLog-in, som brugerorganisationer, kan tilslutte sig, såfremt de overholder reglerne om identitetssikring ved oprettelse som brugerorganisation, som nærmere fastsat i medfør af § 9, stk. 2. En brugerorganisation udgør således en offentlig myndighed, et offentligretligt organ eller en juridisk enhed, der er tilsluttet og anvender serviceområdet Erhvervsadministration i NemLog-in til deres erhvervsbrugere.

Efter den foreslåede bestemmelse i litra a muliggør serviceområdet Erhvervsadministration, at offentlige myndigheder, offentligretlige organer og juridiske enheder i rollen som brugerorganisation i NemLog-in kan oprette, administrere og anvende digitale erhvervsidentiteter samt tilknytte og administrere elektroniske identifikationsmidler til erhvervsbrugere. Serviceområdet Erhvervsadministration kaldes også MitID Erhverv. For at serviceområdet i litra a kan anvendes, kræver det, at en offentlig myndighed eller juridisk enhed, oprettes som brugerorganisation i NemLog-in.

Det er et krav, at en brugerorganisation overholder vilkår for at blive oprettet i NemLog-in. De regler, som regulerer forholdet til offentlige myndigheder og offentligretlige organer fastsættes af finansministeren med hjemmel i § 16.

Når en erhvervsbruger skal have tildelt et elektronisk identifikationsmiddel, vil det ske ved bestilling i serviceområdet Erhvervsadministration. Der kan knyttes tre typer af identifikationsmidler til erhvervsidentiteten. De tre typer af identifikationsmidler kan være følgende: MitID udstedt til en privatperson, et dedikeret MitID udstedt til en privatperson som erhvervsbruger eller et lokalt udstedt elektronisk identifikationsmiddel. Det er erhvervsbrugeren og brugerorganisationen, som vælger identifikationsmidlet.

Det skal bemærkes, at et lokalt udstedt elektronisk identifikationsmiddel udgør et identifikationsmiddel, som er udstedt af den pågældende brugerorganisation selv. Det kan fx være et hospital, hvor lægerne anvender et lokalt identifikationsmiddel med høj autentifikation, når de skal tildele medicin, skrive patientjournal og lign. Et lokalt identifikationsmiddel vil typisk blive anvendt, hvor en brugerorganisation har brug for et identifikationsmiddel med høj autentifikation, som dog alene skal anvendes lokalt og internt hos den pågældende brugerorganisation.

Et lokalt identifikationsmiddel kan alene tilknyttes, hvis brugerorganisationen har tilsluttet en lokal identitetsgarant og er det eneste elektroniske identifikationsmiddel, som ikke er et MitID-identifikationsmiddel. For brugerorganisationer, som ikke anvender lokale identitetsgaranter, vil et elektronisk identifikationsmiddel til en erhvervsbruger være et MitID-identifikationsmiddel.

Det er ligeledes muligt i Erhvervsadministration at tilkoble dedikerede identifikationsmidler til flere erhvervsidentiteter. Desuden kan brugerorganisationen sammen med erhvervsbrugeren vælge, at erhvervsbrugeren private MitID-identifikationsmiddel kan benyttes til autentifikation af erhvervsbrugeren erhvervsidentitet. Hvis en erhvervsbruger har flere erhvervsidentiteter, kan erhvervsbrugeren fx vælge at anvende sit private MitID-identifikationsmiddel til nogle erhvervsidentiteter og et dedikeret MitID til

andre. Således kan en erhvervsbruger med flere erhvervsidentiteter vælge, hvilken digital identitet, som erhvervsbrugeren vil foretage autentifikation med på den digitale selvbetjeningsløsning.

En erhvervsbruger kan benytte sit private MitID-identifikationsmiddel i erhvervsøjemed i to situationer. For det første såfremt erhvervsbrugeren egenhændigt kan tegne virksomheden. Dette kan fx være, når en enkelt person er indehaver af en virksomhed og tegner denne alene. For det andet såfremt en erhvervsbruger i brugerorganisationen har fået tilknyttet det private identifikationsmiddel til sin erhvervsidentitet. Benyttelse af en privatpersons private MitID-identifikationsmiddel i sammenhæng med en erhvervsidentitet kræver både accept fra erhvervsbrugeren og den pågældende juridiske enhed, hvilket er benævnt ”det dobbelte frivillighedsprincip” i NemLog-in, jf. bemærkningerne til § 9, stk. 3.

Endvidere er det muligt i serviceområdet Erhvervsadministration at sammenkoble lokale erhvervsidentiteter med elektroniske identifikationsmidler til digitale erhvervsidentiteter i erhvervs løsningen i NemLog-in. For sammenkobling af lokale identiteter med elektroniske identifikationsmidler til digitale erhvervsidentiteter er det en betingelse, at den offentlige myndighed, det offentligretlige organ eller den juridiske enhed er oprettet som brugerorganisation og tilslutter en lokal identitetsgarant i forhold til NemLog-in.

Serviceområdet Erhvervsadministration omfatter endvidere en ydelse, som udstiller et erhvervs-API, hvorigennem andre brokere har mulighed for at foretage opslag og validering af en erhvervsbruger oprettet i serviceområdet Erhvervsadministration i NemLog-in. Dette giver mulighed for, at erhvervsbrugeren kan anvende sin erhvervsidentitet ved login til en digital selvbetjeningsløsning hos en tjenesteudbyder tilsluttet en anden broker end NemLog-in. Anvendelse af NemLog-in’s erhvervs-API fordrer, at den anden broker indgår aftale med NemLog-in herom.

Med det foreslåede § 8, stk. 3, *litra b*, foreslås det, at NemLog-in indeholder serviceområdet Erhvervsadministration til brugerorganisationer, som sikrer at offentlige myndigheder, offentligretlige organer og juridiske enheder kan tildele og administrere rettigheder og certifikater til erhvervsidentiteter.

Den foreslåede *litra b* indebærer blandt andet, at en brugerorganisation kan tildele rettigheder til enkelte erhvervsbrugere i organisationen eller tildele rettigheder til en erhvervsbruger i en anden brugerorganisation.

En brugerorganisation kan således anvende serviceområdet Erhvervsadministration til Digital repræsentation, hvorved brugerorganisationen kan administrere rettighedstildeling. Rettighedstildelingen foregår ved, at en brugerorganisation giver rettigheder til at lade sig repræsentere af en erhvervsbruger.

I serviceområdet Erhvervsadministration er det endvidere muligt at udstede og administrere certifikater til erhvervsbrugere, som tilknyttes erhvervsbrugeres erhvervsidentitet. Der er grundlæggende to typer certifikater i serviceområdet Erhvervsadministration, hvor den ene certifikattype kan tildeles privatpersoner, der repræsenterer juridiske enheder, og den anden certifikattype kan tildeles en juridisk enhed. Der er to variationer af disse certifikattyper, henholdsvis OCES-certifikater, som udgør offentlige certifikater til elektroniske services (OCES) og kvalificerede certifikater, som kan anvendes fx på tværs af EU. Certifikater kan eksempelvis anvendes lokalt af erhvervsbrugere til autentifikation på lokale it-systemer, eller organisationen kan udstede certifikater som anvendes til integration og kommunikation mellem systemer.

Digitaliseringsstyrelsen skal gennem NemLog-in varetage udstedelse af kvalificerede og OCES-certifikater på vegne af den danske stat. For at varetage denne opgave etablerer Digitaliseringsstyrelsen et certificeringscenter gennem NemLog-in, som muliggør udstedelse af certifikater, tidsstempling og signering, jf. serviceområderne i § 8, stk. 2. nr. 3, og stk. 3.

Til § 9

Der findes ikke gældende regler om forvaltning af NemLog-in.

Reguleringen af forvaltningen af NemLog-in vil dog i et vist omfang videreføre de regler, som

gælder for medarbejdere og administratorer i bekendtgørelse om NemID, dog tilpasset de nye krav til sikkerhed fra NSIS-standard og nye tekniske tilføjelser i serviceområdet Erhvervsadministration. I bekendtgørelsen er der således fastsat identifikationskrav for medarbejdere, som ønsker oprettelse af et NemID. Endvidere gælder der regler for, at en juridisk enhed skal udpege en administrator ved tildeling af NemID til enhedens medarbejdere.

Med den foreslåede § 9, stk. 1, 1 pkt., sikrer Digitaliseringsstyrelsen, at der sker forvaltning af NemLog-in, herunder identitetssikring af offentlige myndigheder, offentligretlige organer og juridiske enheder, når de oprettes som brugerorganisationer i serviceområdet Erhvervsadministration i NemLog-in.

Digitaliseringsstyrelsen sikrer oprettelse af offentlige myndigheder, offentligretlige organer og juridiske enheder som brugerorganisationer i serviceområdet Erhvervsadministration i NemLog-in. Når offentlige myndigheder, offentligretlige organer og juridiske enheder skal oprettes i serviceområdet Erhvervsadministration i NemLog-in jf. den foreslåede § 8, stk. 3, oprettes de som brugerorganisation. En oprettelse som brugerorganisation kræver, at der sker en identitetssikring af den offentlige myndighed, offentligretlige organ og juridiske enhed. Identitetssikringen sker efter de nærmere regler som fastsat i medfør af § 9, stk. 2.

Ved oprettelse af en brugerorganisation i serviceområdet Erhvervsadministration sker der en registrering af, hvordan denne har identificeret sig og efter identitetssikring kan den oprettes som brugerorganisation i Erhvervsadministration.

Når offentlige myndigheder, offentligretlige organer og juridiske enheder er oprettet som brugerorganisation kan de efterfølgende benytte de funktioner, som er indeholdt i serviceområdet Erhvervsadministration. Det indebærer, at den offentlige myndighed, det offentligretlige organ eller den juridiske enhed blandt andet kan tildele digitale identiteter til deres erhvervsbrugere, typisk medarbejdere, men også andre erhvervsbrugere, der har en tilknytning til den offentlige myndighed, det offentligretlige organ eller den juridiske enhed, jf. den foreslåede § 8, stk. 3. Offentlige myndigheder, offentligretlige organer og juridiske enheder har ligeledes mulighed for at udstede og spærre erhvervsidentiteter til erhvervsbrugere tilknyttet til dem.

Det er et privatretligt forhold mellem brugerorganisationen og de tilknyttede erhvervsbrugere at administrere erhvervsbrugernes rettigheder.

En erhvervsbruger skal have et elektronisk identifikationsmiddel for at anvende den digitale identitet tilknyttet erhvervsbrugeren. Et elektronisk identifikationsmiddel kan eksempelvis være udstedt som et MitID-identifikationsmiddel, jf. § 2, nr. 14. Der henvises til den foreslåede § 3, stk. 2, for en uddybning af tilrådgivningsstilling af MitID til erhvervsbrugere og til den foreslåede § 4, stk. 1, om forvaltningen og udstedelsen af MitID.

Med den foreslåede § 9, stk. 1, 2 pkt., sikrer Digitaliseringsstyrelsen, at brugerorganisationers adgang til serviceområdet Erhvervsadministration i NemLog-in samt erhvervsbrugeres digitale identiteter kan spærres og genåbnes efter reglerne fastsat i medfør af stk. 4.

Stk. 1, 2. pkt. indebærer, at Digitaliseringsstyrelsens opgave er at sikre, at brugerorganisationers adgang til Erhvervsadministration i NemLog-in samt erhvervsbrugeres digitale identiteter kan spærres og genåbnes.

De nærmere regler for identitetssikring af offentlige myndigheder, offentligretlige organer og juridiske enheder, når disse oprettes som brugerorganisationer i serviceområdet Erhvervsadministration og regler for spærring af erhvervsbrugeres digitale identiteter vil blive fastsat i regler med hjemmel i § 9, stk. 4. Se nærmere herom i bemærkningerne til stk. 4.

Med den foreslåede § 9, stk. 2, kan en privatperson, der skal registreres som erhvervsbruger i serviceområdet Erhvervsadministration, anvende sit MitID udstedt til privatbrug, til identitetssikring ved registreringen.

En erhvervsbruger kan således anvende sit MitID-identifikationsmiddel udstedt til privatbrug, til identitetssikring ved registreringen af en erhvervsidentitet. Herved sikres, at der kan ske en digital identitetssikring af privatpersonen i forbindelse med oprettelse af erhvervsidentiteten, inden denne kan agere som erhvervsbruger.

Det forudsættes, at identitetssikring ved registrering af erhvervsidentiteten alene vil ske én gang pr. erhvervsidentitet, som oprettes til erhvervsbrugeren. I nogle tilfælde vil det være muligt at identitetssikre erhvervsbrugeren på anden vis. Dette kan fx ske med et andet eID på samme eller højere sikringsniveau som MitID og hvis serviceområdet Erhvervsadministration i NemLog-in systemisk tillader det.

Identitetssikring af en erhvervsidentitet ved brug af et MitID-identifikationsmiddel udstedt til privatbrug, vil være mulig for både erhvervsbrugere i offentlige myndigheder, offentligtretlige organer og juridiske enheder. Det vil endvidere være muligt for erhvervsbrugeren at anvende brugerorganisationens udstyr, eget udstyr eller en kombination af dette til at foretage identitetssikring af erhvervsidentiteten med MitID-identifikationsmidlet udstedt til privatbrug. Dette medfører, at identitetssikring fx kan ske fra vedkommendes egen mobil, computer eller tablet.

Derudover kan en lokal identitetsgarant, som er oprettet som brugerorganisation i NemLog-in, selv foretage identitetssikring. En lokal identitetsgarant fastsætter selv, hvordan der skal foretages identitetssikring i overensstemmelse med NSIS.

Bestemmelsen styrker en fælles høj tillid og sikkerhed på tværs af den offentlige og private sektor, ved at skabe fælles grundlag for sikker elektronisk interaktion mellem privatpersoner, juridiske enheder og offentlige myndigheder og derved øge effektiviteten i de offentlige og private digitale selvbetjeningsløsninger.

Finansministeriet vurderer, at behandlingen i forbindelse med § 9, stk. 2, kan henføres under databeskyttelsesforordningens art. 6, litra e, om myndighedsudøvelse, idet behandlingen sker for, at Digitaliseringsstyrelsen kan varetage den pligt til tilrådighedsstillelse af MitID og NemLog-in, som lovforslaget pålægger Digitaliseringsstyrelsen, jf. § 3 og § 8.

Med den foreslåede § 9, stk. 3, 1. pkt., fastsættes det, at en erhvervsbruger kan få tilknyttet sit elektroniske identifikationsmiddel, som er tilknyttet privatpersonens MitID-identitet, til sin erhvervsidentitet, således at erhvervsbrugeren kan anvende førnævnte identifikationsmiddel til at autentificere en eller flere erhvervsidentiteter.

Med bestemmelsen gøres det muligt for erhvervsbrugere, at anvende deres MitID-identifikationsmiddel udstedt til privatbrug, til at autentificere en eller flere erhvervsidentiteter.

Hvor bestemmelsens stk. 2, gør det muligt at identitetssikre en erhvervsidentitet med et MitID-identifikationsmiddel udstedt til privatbrug, i forbindelse med registreringen, sikrer stk. 3, at en erhvervsbruger løbende kan anvende deres private MitID-identifikationsmiddel til login og autentifikation af en erhvervsidentitet i forbindelse med login i selvbetjeningsløsninger. Dette vil alene være muligt under iagttagelse af princippet om dobbelt frivillighed. Princippet om dobbelt frivillighed medfører, at såvel erhvervsbrugeren som brugerorganisationen skal acceptere, at erhvervsbrugeren kan og må anvende sit MitID-identifikationsmiddel udstedt til privatbrug, i sammenhæng med en erhvervsidentitet knyttet til den pågældende brugerorganisation. Det skal bemærkes, at der alene er tale om brug af det private MitID-identifikationsmiddel og ikke den private MitID-identitet. Der vil derfor være fuldstændig adskillelse mellem privatpersonens digitale identitet i MitID og personens digitale erhvervsidentitet(er). Det kan derfor ikke forekomme, at en erhvervsbruger logger ind med sin private MitID-identitet som medarbejder i en virksomhed. En erhvervsbrugers brug af sit private MitID-identifikationsmiddel er alene mulig, såfremt brugerorganisationen har oprettet en erhvervsidentitet til erhvervsbrugeren.

Herved kan erhvervsbrugeren, forudsat aftale herom mellem erhvervsbrugeren og brugerorganisationen, anvende sit private MitID-identifikationsmiddel. Det betyder også, at såfremt brugerorganisationen

ønsker at spærre erhvervsbrugerens mulighed for at agere på brugerorganisationens vegne, kan brugerorganisationen spærre erhvervsidentiteten, men ikke det private MitID-identifikationsmiddel. Dermed har brugerorganisationen fuld kontrol over erhvervsidentiteten, og erhvervsbrugeren kan stadig foretage login med sin private MitID identitet og sit private MitID-identifikationsmiddel i private sammenhænge. En erhvervsbruger, der ikke længere ønsker at benytte sit private MitID-identifikationsmiddel ved login med sin erhvervsidentitet, kan anmode om et dedikeret MitID-identifikationsmiddel, der så kun kan anvendes i erhvervsmæssig sammenhæng.

Ovenstående er ikke til hinder for, at en privatperson kan anvende sit MitID-identifikationsmiddel og identitet i erhvervsmæssig sammenhæng, forudsat at privatpersonen hæfter fuldt ud for den juridiske enheds aktiviteter. Dette er fx tilfældet i enkeltmandsvirksomheder.

Finansministeriet vurderer, at behandlingen i forbindelse med § 9, stk. 3, kan henføres under databeskyttelsesforordningens art. 6, litra e) om myndighedsudøvelse, idet behandlingen sker for, at Digitaliseringsstyrelsen kan varetage den pligt til tilrådighedsstilling af MitID og NemLog-in, som lovforslaget pålægger Digitaliseringsstyrelsen, jf. § 3 og § 8.

Med den foreslåede § 9, stk. 3, 2. pkt. fastsættes det, at tilknytningen er frivillig for erhvervsbrugeren og frivillig for brugerorganisationen, som erhvervsbrugeren er tilknyttet.

Bestemmelsens 2. pkt. indebærer, at tilknytningen af en erhvervsbrugers elektroniske identifikationsmiddel, som er tilknyttet privatpersonens MitID-identitet grundlæggende hviler på et princip om frivillighed. Det er således frivilligt for erhvervsbrugeren, om erhvervsbrugeren vil foretage en tilknytning af erhvervsbrugerens elektroniske identifikationsmiddel, som er tildelt denne i regi af privatperson. En arbejdsgiver kan således ikke påtvinge sine medarbejdere denne tilknytning.

Ligeledes er tilknytningen også frivillig for brugerorganisationen. Dette indebærer, at en arbejderstager ikke kan påtvinge sin arbejdsgiver, at der skal ske en tilknytning af arbejderstagerens MitID-identitet, som er tildelt i privat regi. Princippet om dobbelt frivillighed gælder for alle brugerorganisationer, som er oprettet i serviceområdet Erhvervsadministration, jf. § 9, stk. 1. Princippet om dobbelt frivillighed gælder således for offentlige myndigheder, offentligretlige organer og juridiske enheder og erhvervsbrugere relateret til disse, jf. § 2, nr. 8 og § 2, nr. 16. Med den foreslåede § 9, stk. 4, fastsættes det, at Finansministeren fastsætter regler om forvaltning af NemLog-in, herunder regler for identitetssikring af brugerorganisationer, spærring og genåbning af erhvervsbrugeres digitale identiteter og om adgang til at klage til Digitaliseringsstyrelsen over afgørelser truffet i medfør af disse regler.

Den foreslåede stk. 4 indeholder en hjemmel til, at finansministeren fastsætter regler om forvaltning af NemLog-in, herunder regler for identitetssikring af offentlige myndigheder, offentligretlige organer og juridiske enheder, når de oprettes som brugerorganisationer i serviceområdet Erhvervsadministration i NemLog-in, og at brugerorganisationers adgang til serviceområdet Erhvervsadministration i NemLog-in og erhvervsbrugeres digitale identiteter kan spærres og genåbnes samt om adgang til at klage til Digitaliseringsstyrelsen over afgørelser truffet i medfør af disse regler.

Finansministeren vil tillige kunne fastsætte regler med krav til løbende anvendelse af serviceområdet Erhvervsadministration i NemLog-in. Dette vil være regler, som skal sikrer, at der til enhver tid er lighed mellem brugerorganisationens fysiske identitet og digitale identitet og med det overordnede formål at værne om sikkerheden i løsningen.

Finansministeren fastsætter ikke regler om udvikling og drift af NemLog-in, idet disse forhold reguleres i kontrakten med den juridiske enhed, offentlige myndighed eller offentligretlige organ, der udpeges i medfør af den foreslåede § 10.

Der vil med hjemmel i den foreslåede bestemmelse blive fastsat nærmere regler for forvaltningen af NemLog-in, herunder processuelle regler om identitetssikring af digitale identiteter, registrering af

identiteter samt regler for oprettelse og spærring af brugerorganisationer i serviceområdet Erhvervsadministration.

Reglerne om oprettelse for serviceområdet Erhvervsadministration vil indeholde betingelser for identitetssikring af offentlige myndigheder, offentligretlige organer og juridiske enheder og identitetssikring af de erhvervsbrugere i offentlige myndigheder, offentligretlige organer og juridiske enheder, som er bemyndiget til at oprette den offentlige myndighed, offentligretlige organ eller juridiske enhed som brugerorganisation i serviceområdet Erhvervsadministration. Derudover vil reglerne indeholde de betingelser, der løbende skal opfyldes for at være brugerorganisation i serviceområdet Erhvervsadministration og regler for udpegelse af administratorer for den offentlige myndighed, det offentlige organ eller den juridiske enhed.

Regler om forvaltning af NemLog-in fastsættes af hensyn til løsningens- og erhvervsbrugernes sikkerhed, samt brugerorganisationers tillid til løsningen. Reglerne skal være med til at sikre erhvervsbrugere og brugerorganisationer mod konkret misbrug og skal samtidig bidrage til at opretholde den samlede sikkerhed i løsningen. Der kan blandt andet fastsættes regler om, at brugerorganisationer og erhvervsbrugere skal tage rimelige forholdsregler for at beskytte de sikkerhedsmekanismer, der sikrer mod kompromittering, ændring, tab og uautoriseret brug af erhvervsbrugerens digitale identitet. Finansministeren vil tillige kunne fastsætte, hvilke konsekvenser det har, hvis en brugerorganisation eller erhvervsbruger ikke overholder disse krav. Det vil eksempelvis kunne fastsættes, at digitale identiteter og adgang til Erhvervsadministration spærres ved mistanke om misbrug eller brud på sikkerheden.

Tildelingen af en erhvervsidentitet og rettighedsstyring påhviler brugerorganisationen og er således et privatretligt anliggende mellem erhvervsbrugeren og den offentlige myndighed, det offentligretlige organ eller juridiske enhed, der har oprettet brugerorganisationen.

Sagsbehandling i forbindelse med identitetssikring og spærring er en forvaltningsopgave. Dette indebærer, at også udpegede juridiske enheder, som foretager identitetssikring vil være underlagt forvaltningsregler, der henvises til den foreslåede § 20. Identitetssikringen skal sikre, at erhvervsbrugerens erhvervsidentitet korrekt afspejler den fysiske persons identitet og skal ske under overholdelse af den gældende NSIS-standard. En juridisk enhed, der er oprettet som brugerorganisation i Erhvervsadministration, beslutter selv hvilke medarbejdere, der skal oprettes som erhvervsbrugere.

Bemyndigelsen har desuden til formål at sikre, at når der træffes en forvaltningsretlig afgørelse om spærring af en brugerorganisation eller en erhvervsbruger, skal der gives mulighed for at indbringe en klage over afgørelsen. Det bemærkes, at spærring alene betragtes som en forvaltningsretlig afgørelse, hvis spærringen foretages af

Digitaliseringsstyrelsen eller af de offentlige myndigheder, offentligretlige organer eller juridiske enheder, som i medfør af den foreslåede § 10 er udpeget til at på vegne af Digitaliseringsstyrelsen at varetage opgaver med blandt andet forvaltningen af NemLog-in samt opgaver i medfør af § 9, stk. 1. Det er således væsentligt, at en erhvervsbruger eller en brugerorganisation kan klage over en sådan spærring, da denne kan have indgribende betydning for brugerorganisationen eller erhvervsbrugerens digitale færden. Ligeledes er den digitale identitet en forudsætning, for at offentlige myndigheder, offentligretlige organer og juridiske enheder kan tilgå og anvende offentlige digitale selvbetjeningsløsninger. Offentlige myndigheder, offentligretlige organer og juridiske enheder, som ikke kan blive oprettet i Erhvervsadministration i NemLog-in vil i stedet skulle betjene sig hos en myndighed uden at være digital. Det vil være op til den enkelte myndighed at beslutte, hvordan de vil understøtte en ikke-digital offentlig myndighed, offentligretligt organ eller juridisk enhed. De enkelte myndigheder vil i den sammenhæng være forpligtet til at vejlede efter de forvaltningsretlige regler, hvilket blandt andet indebærer, at en myndighed har pligt til at vejlede og hjælpe den erhvervsdrivende inden for de ressortområder, som de er ansvarlige for. Således har en myndighed pligt til at hjælpe en offentlig myndighed, offentligretligt organ eller juridisk enhed, der fx ikke kan tilgå myndighedens digitale selvbetjeningsløsninger til at agere inden for

myndighedens område og give adgang til de oplysninger og den offentlige service, som andre ellers kan tilgå ved brug af den digitale selvbetjeningsløsning.

De nærmere regler om tilrådighedsstillelse, tilslutning og anvendelse af NemLog-in for offentlige myndigheder og offentligretlige organer fastsættes i medfør af den foreslåede § 16.

Til § 10

Der findes ikke gældende regler om forvaltning af NemLog-in og retstilstanden på området er derfor ny.

Den foreslåede § 10 medfører, at Digitaliseringsstyrelsen kan udpege offentlige myndigheder, offentligretlige organer eller juridiske enheder til på vegne af Digitaliseringsstyrelsen at varetage opgaver i medfør af § 8, stk. 1, 2. pkt., samt opgaver i medfør af § 9, stk. 1.

I medfør af den foreslåede bestemmelse kan Digitaliseringsstyrelsen udpege offentlige myndigheder, offentligretlige organer eller juridiske enheder til at varetage opgaven med udvikling, drift, vedligeholdelse og forvaltning af NemLog-in samt til at varetage opgaver i medfør af lovforslagets § 9, stk. 1.

I Digitaliseringsstyrelsens opgave med at sikre drift og forvaltning indgår ligeledes en sikring af, at der sker drift og forvaltning af både en teknisk support og en slutbrugersupport for NemLog-in. Digitaliseringsstyrelsen kan ifølge bestemmelsen udpege supportenheder. Slutbrugersupporten kan enten placeres hos en offentlig myndighed eller hos en juridisk enhed. Enhver udpegelse efter § 10 skal ske under overholdelse af udbudsreglerne.

Hvis Digitaliseringsstyrelsen vil udpege en juridisk enhed som it-leverandør af NemLog-in, skal dette ske efter afholdelse af udbud. Digitaliseringsstyrelsen har i 2018 indgået kontrakt med henholdsvis NNIT A/S og Nets DanID A/S.

Digitaliseringsstyrelsen har således indgået kontrakt med NNIT om drift på baggrund af afholdelse af EU-udbud, jf. udbudsbekendtgørelse nr. 2017/S 213442780. Det påhviler dermed NNIT A/S at varetage drift af NemLog-in i overensstemmelse med de kontraktuelle vilkår, som er fastsat i aftalen mellem Digitaliseringsstyrelsen og NNIT A/S. Opgaven med at varetage den daglige drift af NemLog-in sker i tæt samarbejde med Digitaliseringsstyrelsen og øvrige relevante aktører, herunder forvaltnings- og supportorganisationer.

Digitaliseringsstyrelsen har endvidere indgået kontrakt med Nets DanID A/S om at udvikle, vedligeholde, udøve teknisk support og forvaltning på baggrund af afholdelse af EU-udbud, jf. udbudsbekendtgørelse nr. 2018/S 030-065286. Opgaverne inkluderer blandt andet etablering og løbende tilpasning af løsningen. NemLog-in tilpasses løbende i takt med den teknologiske udvikling samt det skiftende trusselsbillede og ændrede samfundsbehov.

Endelig indeholder § 10 en bemyndigelse til, at Digitaliseringsstyrelsen kan udpege offentlige myndigheder, offentligretlige organer eller juridiske enheder til at varetage opgaver i medfør af lovforslagets § 9, stk. 1. Opgaverne i medfør af § 9, stk. 1, omfatter identitetssikring af juridiske enheder, når de oprettes som brugerorganisationer i serviceområdet Erhvervsadministration i NemLog-in. Identitetssikringen skal ske efter de regler, som fastsættes i medfør af § 9, stk. 2. For nærmere beskrivelse af reglerne for identitetssikring henvises til bemærkninger til den foreslåede § 9, stk. 2.

Til § 11

NemLog-in er ikke lovreguleret i dag. Området er derimod reguleret kontraktuelt mellem Digitaliseringsstyrelsen og den private virksomhed NNIT A/S. I dag varetages opgaven med drift af NemLog-in af NNIT A/S.

Det fremgår af tekstanmærkning nr. 124, stk. 1 ad 07.12.02 til § 7 på finansloven fra 2020, at ministeren for offentlig innovation, nu finansministeren, bemyndiges til at indføre de myndigheder mv., der fremgår af bilag 1a, 1b og bilag 1c i bekendtgørelse nr. 1078 af 3. oktober 2014 om offentlige afsendere i Offentlig

Digital Post og desuden domstolene, KL, Danske Regioner, Metroselskabet I/S, Udviklingselskabet By Havn I/S, Odense Letbane P/S og Aarhus Letbane I/S som parter i Digitaliseringsstyrelsens aftale med leverandøren af NemLog-in. Derudover fremgår det af tekstanmærkning nr. 124, stk. 2, at de offentlige myndigheder, selvejende institutioner mv. kan vælge at gøre brug af aftalen.

For en nærmere beskrivelse af NemLog-in henvises til de almindelige bemærkninger afsnit 2.2.

Den foreslåede § 11, stk. 1, nr. 1 medfører, at offentlige myndigheder og offentligretlige organer, som anvender en digital selvbetjeningsløsning til at udføre en myndighedsopgave, i rollen som tjenesteudbydere skal anvende serviceområdet Login og autentifikation, jf. § 8, stk. 2, nr. 1, hvis adgangen til den digitale selvbetjeningsløsning kræver sikker autentifikation.

Bestemmelsen forpligter offentlige myndigheder og offentligretlige organer til som tjenesteudbydere at anvende serviceområdet Login og autentifikation.

Med den foreslåede stk. 1, nr. 1, skal offentlige myndigheder og offentligretlige organer, som anvender en digital selvbetjeningsløsning til at udføre en myndighedsopgave anvende Login og autentifikation, jf. § 8, stk. 2, nr. 1, hvis adgangen til den digitale selvbetjeningsløsning kræver sikker autentifikation. Det er alene, når den offentlige myndighed eller det offentligretlige organ agerer i rollen som tjenesteudbyder, at pligten indtræder. Det indebærer, at it-løsninger, som alene fungerer som intranet og øvrige interne sagsbehandlingssystemer, som ikke er offentligt tilgængelige for borgere mv., ikke vil være omfattet af pligten. Ligeledes kan offentlige myndigheder og offentligretlige organer fortsat anvende andre former for autentifikation, hvis deres digitale selvbetjeningsløsninger ikke vedrører myndighedsopgaver eller ikke kræver sikker autentifikation.

Når offentlige myndigheder og offentligretlige organer forpligtes til at anvende serviceområdet Login og autentifikation i rollen som tjenesteudbydere, sikres det, at privatpersoner og erhvervsbrugere oplever genkendelighed og tillid i deres møde med offentlige digitale selvbetjeningsløsninger.

Privatpersoner og erhvervsbrugere vil opleve, at autentifikation og login foregår på den samme måde, når de skal tilgå en offentlig digital selvbetjeningsløsning. Der findes på markedet for Login- og autentifikationservices ikke andre løsninger, som går på tværs af den offentlige sektor. Således tilbydes serviceområdet Login og autentifikation som en eksklusiv løsning til sikker autentifikation ved adgangen til de offentlige digitale selvbetjeningsløsninger.

Visse væsentlige funktioner i serviceområdet Login og autentifikation i NemLog-in er alene tilgængelige for den offentlige sektor. En af de væsentlige funktioner er funktionen Single sign-on, som sikrer en ubrudt og sammenhængende brugerrejse på tværs af de offentlige løsninger, således at en privatperson eller en erhvervsbruger alene afkræves et enkelt login ved adgangen til de tilsluttede offentlige selvbetjeningsløsninger. Det giver privatpersoner og erhvervsbrugere en ensartet, sikker og enkel brugerrejse ved anvendelse af de offentlige digitale selvbetjeningsløsninger. Der henvises til bemærkningerne til § 8, stk. 2, nr. 1.

Det er væsentligt, at privatpersoner og erhvervsbrugere fortsat kan betjene sig digitalt og sikkert i den offentlige sektor. Det understøttes ved, at NemLog-in anvendes på tværs af hele den offentlige sektor, når offentlige myndigheder og offentligretlige organer indtager rollen som tjenesteudbydere.

NemLog-in har en central rolle i den nationale digitale infrastruktur, idet NemLog-in sammen med MitID skaber en nem og sikker mulighed for privatpersoner og erhvervsbrugere til selv at varetage opgaver i de offentlige digitale selvbetjeningsløsninger, hvor der tidligere krævedes fysisk fremmøde fx hos kommunen. For at sikre, at dette kan ske, skal offentlige myndigheder og offentligretlige organer, som anvender en digital selvbetjeningsløsning til at udføre en myndighedsopgave, anvende serviceområdet Login og autentifikation.

I de tilfælde, hvor offentlige myndigheder og offentligretlige organer forpligtes til at anvende serviceområderne i NemLog-in, jf. § 11, sker det med henblik på at sikre den offentlige orden og sikkerhed, samt

hensynet til de samfundsøkonomiske overvejelser om fælles anskaffelse af it-løsninger i staten, jf. afsnit 2.3 i de almindelige bemærkninger.

Bestemmelsen medfører, at offentlige myndigheder og offentligretlige organer, når de udfører en myndighedsopgave med behov for repræsentation i digitale selvbetjeningsløsninger, forpligtes til at stille serviceområdet Digital repræsentation til rådighed. Digital repræsentation kræver altid sikker autentifikation, jf. bemærkningerne til den foreslåede § 8, stk. 2, nr. 2.

Når serviceområdet Digital repræsentation anvendes af offentlige myndigheder og offentligretlige organer, bliver det muligt for en privatperson og en erhvervsbruger at anvende digital repræsentation i digitale selvbetjeningsløsninger på tværs af myndighedsområder i én samlet offentlig digital løsning.

Med den foreslåede stk. 2, nr. 2 understøttes muligheden for at digitalisere partsrepræsentation i medfør af forvaltningslovens § 8 i offentligt regi. Derudover kan Digital repræsentation i nogle tilfælde anvendes af privatpersoner, som repræsenteres ved værgemål eller på anden måde repræsenteres i offentligt regi.

Pligten gælder, når offentlige myndigheder og offentligretlige organer i deres digitale selvbetjeningsløsninger tilbyder, at en privatperson eller en erhvervsbruger kan lade sig repræsentere eller bistå af andre. I henhold til lovens § 8, stk. 2, nr. 2, er det alene tegningsberettigede erhvervsbrugere, som kan tegne en juridisk enhed fuldstændigt, som kan anvende serviceområdet, dvs. både tegningsberettigede i enkeltmandsvirksomheder og i fx anpartsvirksomheder kan anvende løsningen. Det er en forudsætning, at den tegningsberettigede anvender MitID privat til erhverv for at anvende serviceområdet Digital repræsentation. Når erhvervsbrugere, som anvender MitID privat til erhverv, afgiver rettigheder til en anden erhvervsbruger benævnes det som digitale erhvervsfuldmagter i NemLog-in. Pligten gælder alene for offentlige myndigheder og offentligretlige organer i rollen som tjenesteudbydere.

Pligten har ydermere til formål at stille repræsentationsløsningen til rådighed for at sikre en ensartet brugerrejse på tværs af den offentlige sektor ved anvendelsen af repræsentationsløsninger. Det giver mulighed for, at privatpersoner og erhvervsbrugere nemt kan lade sig repræsentere digitalt i den offentlig sektor ved alene at skulle anvende én samlet løsning for repræsentation som alternativ til anvendelse af flere løsninger, som ligeledes kan variere efter myndighedsområder.

Offentlige myndigheder og offentligretlige organer skal stille Digital repræsentation til rådighed, hvis det er muligt at foretage repræsentation i deres digitale selvbetjeningsløsninger, fx med henblik på den forvaltningsretlige repræsentationsadgang, som er fastsat i forvaltningslovens § 8, stk. 1.

Hvis funktionaliteten i serviceområdet Digital repræsentation ikke tilstrækkeligt understøtter behovet for repræsentation hos en offentlig myndighed eller et offentligretligt organ, kan disse vælge at tilbyde en sekundær løsning til den del af repræsentationen, som serviceområdet Digital repræsentation ikke understøtter. En sekundær løsning skal således alene fungere som et supplement til serviceområdet Digital repræsentation. Dette indebærer, at en myndighed eller et offentligretligt organ som minimum skal tilbyde adgang til serviceområdet Digital repræsentation, såfremt der udføres en myndighedsopgave og er behov for repræsentation i digitale selvbetjeningsløsninger. Serviceområdet Digital repræsentation kan derfor betragtes som en basisløsning for offentlig Digital repræsentation. Digital repræsentation kan kun anvendes af offentlige myndigheder og offentligretlige organer.

Hvis Digital repræsentation ikke hensigtsmæssigt kan sameksistere med en sekundær løsning og dermed ikke kan imødekomme nødvendige forretningsmæssige- og tekniske krav for et givent myndighedsområde, kan den offentlige myndighed eller det offentligretlige organ anvende egen infrastruktur.

I takt med videreudvikling af Digital repræsentation til teknisk bredere understøttelse af forskellige komplekse forretningsmæssige behov, skal offentlige myndigheder og offentligretlige organer genoverveje muligheden for anvendelsen af Digital repræsentation ved udskiftning af egen infrastruktur.

Bestemmelsens foreslåede § 11, stk. 2, nr. 1, medfører, at offentlige myndigheder og offentligretlige organer i rollen som tjenesteudbydere kan anvende serviceområdet Login og autentifikation, jf. § 8, stk. 2,

nr. 1, hvis adgangen til den digitale selvbetjeningsløsning ikke kræver sikker autentifikation eller hvis der ikke udføres en myndighedsopgave.

Med bestemmelsen skabes der en ret i loven for offentlige myndigheder og offentligretlige organer i rollen som tjenesteudbydere, til at anvende serviceområdet Login og autentifikation.

Bestemmelsen giver således offentlige myndigheder og offentligretlige organer en ret til som tjenesteudbydere at anvende serviceområdet Login og autentifikation, jf. § 8, stk. 2 nr. 1, hvis adgangen til den digitale selvbetjeningsløsning ikke kræver sikker autentifikation, eller hvis der ikke udføres en myndighedsopgave, jf. bemærkningerne til den foreslåede § 2, nr. 10 og 11. Det indebærer, at offentlige myndigheder og offentligretlige organer kan vælge at tilbyde privatpersoner eller erhvervsbrugere adgang til deres digitale selvbetjeningsløsninger med serviceområdet Login og autentifikation. Den lovskabte ret indebærer, at offentlige myndigheder og offentligretlige organer får en mulighed for at anvende serviceområdet Login og autentifikation i medfør af loven.

Det er den enkelte offentlige myndighed eller det offentligretlige organ, som må vurdere, om pågældende offentlige myndighed eller offentligretlige organ udfører en myndighedsopgave. I vurderingen kan medregnes opgaver, som er pålagt den offentlige myndighed eller det offentligretlige organ ved lov eller anden retsakt, opgaver hvor myndigheden eller det offentligretlige organ er ordregivende myndighed og desuden opgaver, som umiddelbart synes at ligge inden for myndigheds eller det offentligretlige organs ressort og som løses af myndigheden eller det offentligretlige organ. I vurderingen af om der udføres en myndighedsopgave suppleres det formelle kriterier for myndighedens eller det offentligretlige organs struktur med et materielt kriterium. Der henvises i øvrigt til definitionen af offentlige myndighed og offentligretligt organ. De offentlige myndigheder, som er omfattet af pligten i § 11, stk. 2, nr. 1, er offentlige myndigheder i henhold til denne lovs definition i § 2, nr. 10. De offentligretlige organer, som er omfattet af pligten i § 11, stk. 2, nr. 1, er offentligretlige organer i henhold til denne lovs definition i § 2, nr. 11.

Bestemmelsens foreslåede § 11, stk. 2, nr. 2, medfører, at offentlige myndigheder og offentligretlige organer i rollen som tjenesteudbydere kan anvende serviceområdet Digital signering, jf. § 8, stk. 2, nr. 3. Det foreslås med nr. 2, at offentlige myndigheder og offentligretlige organer i rollen som tjenesteudbydere kan anvende serviceområdet Digital signering, jf. § 8, stk. 2 nr. 3. Digital signering kan alene ske på baggrund af autentifikation, der opfylder NSIS-standardens definition af sikringsniveau betydelig og høj og tillige opfylder kravene i eIDAS-forordningens artikel 24, stk. 1.

Offentlige myndigheder og offentligretlige organer kan således vælge at anvende serviceområdet Digital signering i NemLog-in, hvis de har en digital selvbetjeningsløsning, hvor der udstilles digitalt signerede dokumenter, eller hvor det er muligt for privatpersoner og erhvervsbrugere at foretage digital signering. Ved udstilling af digital signering muliggør en tjenesteudbyder i deres digitale selvbetjeningsløsninger, at en privatperson eller en erhvervsbruger kan anvende serviceområdet Digital signering i NemLog-in. For at offentlige myndigheder og offentligretlige organer kan anvende serviceområdet Digital signering i NemLog-in, skal de tilsluttes serviceområdet Digital signering i NemLog-in som tjenesteudbydere, så de kan udbyde muligheden for signering af indhold i deres digitale selvbetjeningsløsning.

Når offentlige myndigheder og offentligretlige organer gives en ret til at anvende serviceområdet Digital signering, understøttes de i at tilbyde privatpersoner og erhvervsbrugere en sagsbehandling og procedure, som fuldt ud kan digitaliseres. Med offentlige myndigheders og offentligretlige organers anvendelse af serviceområdet Digital signering, vil privatpersoner og erhvervsbrugere genkende signeringstjenesten på tværs af den offentlige sektor.

Signaturer afgivet i serviceområdet valideres ensartet i serviceområdets valideringstjeneste uanset hvilken offentlig myndighed eller offentligretligt organ, der som tjenesteudbyder har anvendt servicen. Ved valideringen kontrolleres bl.a. det digitale dokumentets integritet og det konstateres i denne forbindelse

om dokumentet er ændret efter at signaturen er afgivet. For behandling af persondata i forbindelse med valideringen i serviceområdet Digital signering i NemLog-in, henvises til denne lovs foreslåede § 14.

Bestemmelsens foreslåede § 11, stk. 3, medfører, at offentlige myndigheder og offentligretlige organer i rollen som brugerorganisationer kan anvende serviceområdet Erhvervsadministration, jf. § 8, stk. 3.

Med den foreslåede stk. 3 skabes der en ret i loven til for offentlige myndigheder og offentligretlige organer i rollen som brugerorganisation at benytte serviceområdet Erhvervsadministration i NemLog-in, jf. § 8, stk. 3. Serviceområdet Erhvervsadministration giver offentlige myndigheder og offentligretlige organer mulighed for at oprette, administrere og anvende digitale erhvervsidentiteter samt tildele og administrere elektroniske identifikationsmidler.

Endelig kan offentlige myndigheder og offentligretlige organer med serviceområdet Erhvervsadministration vælge at tildele og administrere rettigheder og certifikater til erhvervsidentiteter oprettet i serviceområdet.

Det er hensigten med retten til at anvende serviceområdet Erhvervsadministration, at offentlige myndigheder og offentligretlige organer tilbydes et redskab til at digitalisere styringen af digitale erhvervsidentiteter. Endvidere kan offentlige myndigheder og offentligretlige organer med retten til at anvende serviceområdet Erhvervsadministration vælge at anvende en løsning, som fungerer på tværs af den offentlige sektor. Løsningen vil derved udgøre et effektivt arbejdsredskab, som blandt andet understøtter samarbejdet på tværs af den offentlige sektor.

Offentlige myndigheder og offentligretlige organer kan i rollen som brugerorganisation i serviceområdet Erhvervsadministration yderligere vælge at oprette sig som lokal identitetsgarant i NemLog-in.

Den foreslåede § 11, stk. 4, 1. led, medfører, at offentlige myndigheder og offentligretlige organer i de i stk. 1 anførte tilfælde skal anskaffe serviceområderne fra Digitaliseringsstyrelsen.

Med bestemmelsen fastsættes det, at de nævnte serviceområder skal anskaffes fra Digitaliseringsstyrelsen. Betingelserne for anskaffelsen fremgår af § 16 og § 15, stk. 3. Der henvises til bemærkningerne til § 16 og § 15, stk. 3.

Bestemmelsen har til formål at understrege, hvornår de offentlige myndigheder og offentligretlige organer har en pligt til at anskaffe sig serviceområderne i NemLog-in. For en nærmere beskrivelse af de enkelte serviceområder i NemLog-in henvises til bemærkningerne til § 8, stk. 2 og 3.

I de tilfælde, hvor offentlige myndigheder og offentligretlige organer forpligtes til at anvende serviceområderne i NemLog-in, jf. § 11, sker det med henblik på at sikre den offentlige orden og sikkerhed, samt hensynet til de samfundsøkonomiske overvejelser om fælles anskaffelse af it-løsninger i staten, jf. afsnit 2.3 i de almindelige bemærkninger.

Det skal bemærkes, at der er et væsentligt hensyn til, at der sikres en høj grad af tillid og sikkerhed på tværs af de offentlige digitale selvbetjeningsløsninger. Det afgørende for, at de offentlige myndigheder og offentligretlige organer forpligtes til at anvende serviceområderne er, om de anvender en digital selvbetjeningsløsning til at udføre en myndighedsopgave. Omvendt vil der ikke gælde en pligt til at anvende de nævnte serviceområder, såfremt en myndighed eller et offentligretligt organ ikke udfører en myndighedsopgave på en digital selvbetjeningsløsning. Det er op til den enkelte myndighed og det offentligretlige organ at vurdere, hvorvidt de materielt set udfører en myndighedsopgave, der henvises til bemærkningerne i den foreslåede § 2, nr. 10 og nr. 11. For en definition af en digital selvbetjeningsløsning henvises der endvidere til den foreslåede § 2, nr. 12.

Den foreslåede § 11, stk. 4, 2. led, medfører, at offentlige myndigheder og offentligretlige organer i de i stk. 2 og 3 anførte tilfælde kan anskaffe serviceområderne fra Digitaliseringsstyrelsen.

Med bestemmelsens 2. led fastsættes det, hvilke serviceområder, som kan anskaffes fra Digitaliseringsstyrelsen. Betingelserne for anskaffelsen fremgår af § 16 og § 15, stk. 3. Der henvises til bemærkningerne til § 16 og § 15, stk. 3.

Bestemmelsen har til formål at understrege, hvornår de offentlige myndigheder og offentligretlige organer har en ret til at anskaffe sig serviceområderne i NemLog-in. For en nærmere beskrivelse af de enkelte serviceområder i NemLog-in henvises til bemærkningerne til § 8, stk. 2 og 3.

Til § 12

Der findes ikke gældende ret, som regulerer aftaleforhold eller vilkår for anvendelsen af serviceområderne i NemLog-in.

Den foreslåede § 12 medfører, at juridiske enheder kan indgå aftale med Digitaliseringsstyrelsen om anvendelse af serviceområderne nævnt i § 8, stk. 2, nr. 1 og nr. 3, samt stk. 3.

Med den foreslåede § 12 får juridiske enheder mulighed for at anvende serviceområder i § 8, stk. 2, nr. 1 samt stk. 3, efter aftale med Digitaliseringsstyrelsen.

For at anvende serviceområderne i § 8, stk. 2, nr. 1 samt stk. 3 kræves det, at den juridiske enhed indgår aftale herom med Digitaliseringsstyrelsen. Den juridiske enhed skal således acceptere de aftalevilkår, som er fastsat ensidigt af Digitaliseringsstyrelsen for at kunne anvende de nævnte serviceområder i NemLog-in. Digitaliseringsstyrelsen har udarbejdet en række standardvilkår for juridiske enheder, som ønsker at anvende serviceområderne Login og autentifikation og Digital signering. Når den juridiske enhed vil være tjenesteudbyder til enten serviceområdet Login og autentifikation eller Digital signering kræves det således, at tjenesteudbyderen accepterer de nævnte vilkår. Vilkårene vil bl.a. sætte rammerne for anvendelsen af serviceområderne, misligholdelse, håndtering af sikkerhedsbrud mv.

Tilsvarende fastsætter Digitaliseringsstyrelsen vilkår for de juridiske enheder, der ønsker at anvende serviceområdet Erhvervsadministrationen som brugerorganisationer.

Det skal understreges, at retten til at anvende NemLog-in skal læses i sammenhæng med den foreslåede § 15 om opkrævning af gebyr og vederlag. Det er frivilligt for de juridiske enheder, om de vil anvende serviceområderne Login og autentifikation, Digital signering og Erhvervsadministration. Det er således en forudsætning for en juridisk enheds anvendelse af serviceområderne i NemLog-in, at de accepterer de aftalevilkår, som er fastsat af Digitaliseringsstyrelsen. Det skal understreges, at vilkårene vil fastsættes efter principperne om saglig forvaltning og ligebehandling af erhvervsaktørerne.

Til § 13

Der findes ikke gældende ret, som regulerer behandlingen af personoplysninger og videregivelse af risikodata for MitID-løsningen og NemLog-in. Bestemmelsen er dog fastsat ud fra iagttagelsen af gældende regler i databeskyttelsesforordningen (2016/679) og databeskyttelsesloven, lov nr. 502 af 23. maj 2018.

Den foreslåede § 13, stk. 1, medfører, at ved en privatpersons anvendelse af MitID eller en erhvervsbrugers anvendelse af det elektroniske identifikationsmiddel i MitID til login og autentifikation kan Digitaliseringsstyrelsen videregive autentifikationssvar, herunder risikodata vedrørende den konkrete og enkelte transaktion, til en broker, der er tilsluttet MitID-løsningen eller NemLog-in.

Med den foreslåede bestemmelse indføres hjemmel til, at Digitaliseringsstyrelsen kan videregive autentifikationssvar, herunder risikodata til en offentlig myndighed, et offentligretligt organ eller en juridisk enhed i rollen som broker i forbindelse med det enkelte login og autentifikation forbundet hermed. Autentifikationssvaret indeholder oplysninger om privatpersonen eller erhvervsbrugeren, der logger ind samt indsamlede risikodata, jf. de almindelige bemærkninger, afsnit 2.3.2.1. Hensynet til at opretholde tilliden til anvendelsen af MitID samt hensynet til at følge med den teknologiske udvikling gør, at der kan opstå behov for at ændre eller tilføje andre risikodata, der kan indsamles og videregives til risikovurdering af den enkelte transaktion, der gennemføres med MitID.

Om vurdering af behovet for en særskilt hjemmel henvises til de almindelige bemærkninger, afsnit 3.

Den hjemmel, der indføres til videregivelse af personoplysninger fra Digitaliseringsstyrelsen, indebærer,

at en broker kan modtage og behandle autentifikations svar, herunder risikodata til vurdering af risikoen ved hver enkelt konkrete transaktion. Formålet med videregivelse af risikodata er, at give brokeren en yderligere mulighed for at vurdere og afgøre om det modtagne svar af sikkerhedsmæssige årsager skal umuliggøre login på den pågældende tjeneste.

Ved modtagelsen af data bliver brokeren dataansvarlig herfor og skal i så henseende efterleve databeskyttelsesreglerne, herunder opfylde sin oplysningspligt over for de registrerede. I det omfang brokeren behandler modtagne autentifikations svar og de deri indeholdte data til andet formål, vil det kræve, at brokeren har en selvstændig behandlingshjemmel hertil. Brokerens behandling af autentifikations svar indebærer, at brokeren danner et autentifikations svar, der kan beriges med andre af brokerens egne data. Andre data, som brokeren kan berige autentifikations svaret med kan fx være rettigheder til at anvende et it-system. En sådan berigelse er derfor nødvendig for, at en bruger kan anvende en digital selvbetjeningsløsning, og et autentifikations svar der ikke bliver beriget vil derfor fratage privatpersonen eller erhvervsbrugere, at interagere med den digitale selvbetjeningsløsning. Et eksempel på dette kunne være en erhvervsbruger, som af sin brugerorganisation har fået tilknyttet rettigheder til at kunne læse Digital Post for brugerorganisationen. Endvidere kan risikodata være undtaget i det autentifikations svar, der formidles til en tjenesteudbyder, idet det er en forudsætning for en tjenesteudbyders modtagelse af risikodata, at tjenesteudbyderen har en særskilt hjemmel til at modtage disse.

En broker indgår en brokeraftale med Nets DanID A/S på vegne af partnerskabet mellem FR1 og Digitaliseringsstyrelsen. Aftalen indeholder en række af partnerskabet fastsatte vilkår for at blive og vedblive med at være broker. I relation til modtagelse af autentifikations svar vil brokeren blive gjort opmærksom på, at brokeren alene kan anvende autentifikations svar og de deri indeholdte data som anført i den foreslåede bestemmelse, og at enhver behandling herudover kræver, at brokeren har en selvstændig hjemmel hertil.

Den foreslåede § 13, stk. 2, medfører, at en broker kan foretage automatiske afgørelser om log-in på baggrund af risikodata videregivet efter stk. 1.

Med den foreslåede bestemmelse indføres i overensstemmelse med databeskyttelsesforordningen art. 22, stk. 2, b, hjemmel til, at en broker kan foretage automatiske afgørelser om, hvorvidt log-in i konkrete tilfælde skal tillades, afvises eller om der kan være behov for at iværksætte yderligere foranstaltninger for at sikre, at det er den rigtige privatperson og erhvervsbruger med et MitID-identifikationsmiddel, som ønsker log-in. De automatiske afgørelser i denne bestemmelse er ikke afgørelser i forvaltningslovens forstand, og det er op til den enkelte broker at beslutte, om der kan tillades log-in. Det er ligeledes op til den enkelte broker at beslutte, om denne vil anvende og agere på baggrund af de risikodata, som er videregivet efter stk. 1.

Brokeren foretager ikke vurderinger eller træffer afgørelser om de aktiviteter eller handlinger som privatpersonen eller erhvervsbrugeren med et MitID-identifikationsmiddel, ønsker at tilgå ved log-in på baggrund af anmodningen om autentifikation med det elektroniske identifikationsmiddel i MitID. Afgørelsernes formål er at sikre, om privatpersonen eller erhvervsbrugeren som indehaver af et MitID-identifikationsmiddel er identisk med den digitale identitet, som der logges ind med.

Den foreslåede § 13, stk. 3, medfører, at en broker, der i medfør af stk. 1 har modtaget autentifikations svar, kan videregive det modtagne og behandlede autentifikations svar til en tjenesteudbyder, der gennem pågældende broker, modtager autentifikationer fra MitID-løsningen.

Med den foreslåede bestemmelse kan brokere videregive det modtagne og af brokeren behandlede autentifikations svar, jf. stk.1 og bemærkningerne hertil, til en tjenesteudbyder, der har indgået en aftale med den pågældende broker om at modtage autentifikations svar. Brokerens behandling af autentifikations svar indebærer, at brokeren danner et autentifikations svar, som kan beriges med andre af brokerens egne data. De data, som autentifikations svaret kan beriges med, kan fx være e-mailadresse og fødselsdato, der anvendes til at identificere brugeren over for tjenesteudbyderens digitale selvbetjeningsløsning.

Det er en forudsætning for, at MitID-løsningen kan fungere efter sit formål, at autentifikationssvaret videregives til den tjeneste, hvor brugeren ønsker at logge ind. Tjenesteudbyderen bliver i så henseende dataansvarlig for data indeholdt i autentifikationssvaret og skal i så henseende efterleve databeskyttelsesreglerne, herunder opfylde sin oplysningspligt over for de registrerede. I det omfang tjenesteudbyderen behandler modtagne autentifikationssvar og de deri indeholdte data til andet formål, vil det kræve, at tjenesteudbyderen har en selvstændig behandlingshjemmel hertil.

Den foreslåede § 13, stk. 4, medfører, at der ved en erhvervsbrugers anvendelse af et elektronisk identifikationsmiddel fra en lokal identitetsgarant tilsluttet NemLog-in kan Digitaliseringsstyrelsen videregive autentifikationssvar vedrørende den konkrete og enkelte transaktion til en broker, der er tilsluttet NemLog-in.

Med den foreslåede bestemmelse kan Digitaliseringsstyrelsen videregive autentifikationssvar til en offentlig myndighed, et offentligt organ eller en juridisk enhed, i rollen som broker. Videregivelsen sker i forbindelse med det enkelte login og autentifikation og foretages under anvendelse af et identifikationsmiddel fra en lokal identitetsgarant, der er tilsluttet NemLog-in.

Tilslutningen til NemLog-in giver den lokale identitetsgarant mulighed for at knytte lokale identifikationsmidler til erhvervsidentiteterne i NemLog-in. En virksomhed vil således kunne tilknytte lokale identifikationsmidler til virksomhedens ansatte. Derved kan et lokalt identifikationsmiddel anvendes til autentifikation internt hos den lokale identitetsgarant fx internt i en virksomhed og til autentifikation over for tjenesteudbydere tilsluttet en broker i NemLog-in.

Autentifikationssvaret indeholder oplysninger om erhvervsbrugeren, der logger ind, jf. de almindelige bemærkninger, afsnit 2.2.2.

Tilslutning af brokere til NemLog-in med henblik på at kunne modtage autentifikation på baggrund af et identifikationsmiddel fra en lokal identitetsgarant sker ved indgåelse af særskilt aftale.

Den foreslåede § 13, stk. 5, medfører, at en broker, der i medfør af stk. 4 har modtaget autentifikationssvar, kan videregive det modtagne og behandle autentifikationssvar til en tjenesteudbyder, der gennem en broker, modtager autentifikationer fra NemLog-in.

I medfør af den foreslåede bestemmelse kan en broker, videregive autentifikationssvar til en tjenesteudbyder, der har indgået en aftale med den pågældende broker, om at modtage autentifikationssvar.

Det er en forudsætning for, at NemLog-in-løsningen kan fungere efter sit formål og muliggøre anvendelsen af identifikationsmidler fra lokale identitetsgaranter, at autentifikationssvaret videregives til den tjeneste, hvor erhvervsbrugeren ønsker at logge ind. Tjenesteudbyderen bliver i denne henseende dataansvarlig for data indeholdt i autentifikationssvaret og skal i så henseende efterleve databeskyttelsesreglerne, herunder opfylde sin oplysningspligt over for de registrerede. I det omfang tjenesteudbyderen behandler modtagne autentifikationssvar og de deri indeholdte data til andet formål, vil det kræve, at tjenesteudbyderen har en selvstændig behandlingshjemmel hertil.

Til § 14

Der findes ikke gældende ret, som regulerer behandlingen af personoplysninger og videregivelse af risikodata for MitID-løsningen og NemLog-in. Bestemmelsen er dog fastsat ud fra iagttagelsen af gældende regler i databeskyttelsesforordningen og databeskyttelsesloven.

Den foreslåede § 14, medfører, at Digitaliseringsstyrelsen kortvarigt og i et sikret teknisk miljø kan behandle følsomme personoplysninger, i forbindelse med validering af digitale signaturer i valideringstjenesten i serviceområdet Digital signering.

Med den foreslåede bestemmelse indføres hjemmel til, at Digitaliseringsstyrelsen i medfør af databeskyttelsesforordningens art. 9, stk. 2, litra g, kan behandle personoplysninger omfattet af databeskyttelses-

forordningen artikel 9, stk. 1, i forbindelse med validering af en digital signatur i Digitaliseringsstyrelsens valideringstjeneste under serviceområdet Digital signering.

Baggrunden for bestemmelsen er, at valideringstjenesten i serviceområdet Digital signering i overensstemmelse med dens formål kan behandle de data, som er nødvendige for at kunne foretage valideringen. Der kan således potentielt behandles alle former for data, herunder følsomme personoplysninger omfattet af persondataforordningens artikel 9, stk. 1. Den behandling, der sker i valideringstjenesten er udelukkende maskinel. Den maskinelle behandling består i dannelse af en checksum, der senere kan sammenlignes med en på et senere tidspunkt dannet checksum. På den måde sikres, at der ikke sket ændringer af data, hvorved det underskrevne dokumentets bevisværdi sikres og senere kan sandsynliggøres.

Det er Finansministeriets vurdering, at den maskinelle behandling kan rummes inden for bestemmelsen i databeskyttelsesforordningens art 9, stk. 2, litra g, der bestemmer, at personoplysninger omfattet af art. 9, stk. 1 lovligt kan behandles, såfremt behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser, og i øvrigt står i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger i form af en kortvarig behandling i et sikret miljø, til beskyttelse af den registreredes grundlæggende rettigheder og interesser. Den kortvarige behandling vil alene ske i det moment, hvor selve valideringen foregår. Det skal bemærkes, at de data, som kortvarigt behandles i et sikret miljø i forbindelse med valideringen, vil blive slettet efter valideringen er foretaget. Som resultat af valideringen vil der således alene være en checksum, som beretter om dokumentets validitet.

Efter Finansministeriets vurdering udgør det en væsentlig samfundsinteresse, at de digitale infrastrukturløsninger er effektive og kan opfylde de behov, der er i den analoge verden. En analog underskrift og parafering af dokumenter til sikring af, at der ikke sker uønskede eller utilsigtede ændringer er således et eksempel på et behov, der findes i den analoge verden. Signering og efterfølgende validering i valideringstjenesten opfylder på digital vis dette behov. Det er endvidere Finansministeriets vurdering, at behandlingen står i rimeligt forhold til det mål, der forfølges samt respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.

Digitaliseringsstyrelsens valideringstjeneste har karakter af en kvalificeret valideringstjeneste for kvalificerede elektroniske signaturer udstedt i medfør af eIDAS-forordningen.

Valideringstjenesten er offentligt tilgængelig og kan validere digitale signaturer afgivet i NemLog-in i serviceområde Digital signering samt digitale signaturer, der opfylder standarder fastlagt af EU-Kommissionen i henhold til eIDAS-forordningens artikel 27, stk. 5, og artikel 37, stk. 5. Tjenesten understøtter offentlige myndigheder og offentligretlige organers modtagelse af kvalificerede elektroniske signaturer og kvalificerede elektroniske segl fra en anden medlemsstat som led i gensidig anerkendelse heraf på tværs af medlemsstaterne.

Digitaliseringsstyrelsen kan give mulighed for, at tjenesten kan validere andre digitale signaturer, hvis det vurderes relevant for at understøtte markedet for digitale signeringsløsninger.

I forbindelse med verifikation foretages en kortvarig automatisk behandling i et sikret miljø af de data, der er underskrevet. Behandlingen sker med henblik på at kontrollere integriteten af de pågældende data ved at sammenligne disse i klartekst med den checksum eller hash-værdi, der blev genereret på underskriftstidspunktet, og som er koblet til den digitale signatur.

Til § 15

Der findes ikke gældende ret, som regulerer opkrævning af gebyr og vederlag for tilslutning til og anvendelse af MitID-løsningen og NemLog-in.

Den foreslåede § 15, stk. 1, medfører, at Digitaliseringsstyrelsen indgår aftale med juridiske enheder om vederlag for tilslutning til og anvendelse af MitID-løsningen og NemLog-in.

Det foreslås med bestemmelsens stk. 1, at Digitaliseringsstyrelsen kan indgå aftale med juridiske enheder om tilslutning til og anvendelse af MitID-løsningen og NemLog-in og om vederlaget herfor. Bestemmelsen regulerer forholdet mellem Digitaliseringsstyrelsen som leverandør og juridiske enheder i egenskab af tjenesteudbydere, brugerorganisationer og brokere.

Det foreslås, at forholdet er rent kontraktbaseret, da Digitaliseringsstyrelsen på trods af pligten til at stille MitID-løsningen og NemLog-in til rådighed for juridiske enheder agerer på et (delvist) kommercielt marked. Vederlaget, der opkræves fra juridiske enheder, skal dække Digitaliseringsstyrelsen omkostninger, en forholdsmæssig andel af omkostningerne til udvikling af løsningerne svarende til de juridiske enheders anvendelse af løsningerne, være ikke-diskriminerende og skal sikre, at der ikke sker konkurrencefordrejning.

Den foreslåede § 15, stk. 2, medfører, at offentlige myndigheder og offentligretlige organer betaler for MitID-løsningen og NemLog-in gennem fællesoffentlig finansiering eller ved betaling af vederlag fastsat af finansministeren.

Formålet med den foreslåede bestemmelse er at bemyndige finansministeren til at fastsætte regler om opkrævning af gebyr for anskaffelse og anvendelse af MitID, MitID-løsningen og NemLog-in for offentlige myndigheder og offentligretlige organer.

Det foreslås med bestemmelsen, at når offentlige myndigheder og offentligretlige organer benytter MitID-løsningen og NemLog-in, betaler de gennem fællesoffentlig finansiering eller ved betaling af vederlag fastsat af finansministeren for særlige områder af løsningerne.

Digitaliseringsstyrelsen er for så vidt angår MitID-løsningen og NemLog-in en teknisk tjeneste for den offentlige forvaltning i Danmark, og 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 MitID-løsningen og NemLog-in på de vilkår, der i § 16 er fastsat af finansministeren, og til den betaling, der i henhold til bemyndigelsen i § 15, stk. 2, er fastlagt af finansministeren. Digitaliseringsstyrelsen kan således ikke forhandle om vederlaget.

Det er aftalen mellem de offentlige parter, der regulerer, hvilke offentlig myndigheder og offentligretligt organer, som er en del af den fællesoffentlige finansiering.

Såfremt en offentlig myndighed eller et offentligretligt organ ikke er omfattet af den fællesoffentlige finansiering skal betalingen for MitID-løsningen og NemLog-in i stedet ske efter de vederlag, som er fastsat af finansministeren. Regler herom forventes fastsat i en bekendtgørelse om vilkår for offentlige myndigheder og offentligretlige organer i deres rolle som enten tjenesteudbyder eller brugerorganisation, jf. den foreslåede stk. 2.

Den foreslåede § 15, stk. 3, medfører, at finansministeren kan fastsætte regler om opkrævning af gebyr hos privatpersoner for registrering og udstedelse af MitID.

Formålet med den foreslåede bestemmelse er at bemyndige finansministeren til at fastsætte regler om opkrævning af gebyr hos privatpersoner.

Bestemmelsen vil ikke kunne anvendes til at fastsætte regler om gebyr for selve registreringen af et MitID. Det er i den forbindelse hensigten, at MitID-app'en kan anvendes som elektronisk identifikationsmiddel uden brugerbetaling.

Det er herudover hensigten, at der alene skal fastsættes regler om privatpersoners betaling af gebyr for fysiske elektroniske identifikationsmidler ud over et nærmere fastsat antal, der udleveres gebyrfrit. Fra idriftsættelse af MitID-løsningen er det hensigten at fastsætte regler om, at en privatperson gebyrfrit kan

få op til tre fysiske elektroniske identifikationsmidler, hvorefter der skal betales gebyr for yderligere identifikationsmidler.

Endelig er det hensigten, at en privatperson skal have vederlagsfri adgang til elektroniske identifikationsmidler. Antallet på tre fysiske elektroniske identifikationsmidler er valgt ud fra et princip om, at privatpersonen bør udvise behørig påpasselighed med håndtering og brug af de tildelte identifikationsmidler og derfor ikke vil have behov for yderligere identifikationsmidler for at kunne betjene sig med MitID.

En privatperson kan alene have et aktivt fysisk elektronisk identifikationsmiddel ad gangen. Det bemærkes dog, at det kan bestemmes, at der skal opkræves vederlag for særlige MitID identifikationsmidler til brug for understøttelse af sikringsniveau "høj". Dette sikringsniveau vil kun sjældent være påkrævet for en privatperson, men kan være krævet ved tilgang til og anvendelse af udenlandske selvbetjeningsløsninger. Gebyret er fastsat i kontrakten med leverandøren af MitID, vil være fast for det enkelte fysiske elektroniske identifikationsmiddel og vil være omkostningsbestemt.

Til § 16

Der findes ikke gældende ret, som regulerer tilrådighedsstillelsen og anvendelsen for offentlige myndigheder og offentligretlige organer.

Den foreslåede § 16, medfører, at finansministeren fastsætter regler om tilrådighedsstillelse for offentlige myndigheder og offentligretlige organer, jf. de foreslåede bestemmelser i §§ 3 og 8, og om offentlige myndigheder og offentligretlige organers tilslutning til og anvendelse af MitID-løsningen og NemLog-in.

Det forventes, at der fastsættes regler om de vilkår, som skal gælde for offentlige myndigheders og offentligretlige organers tilslutning og anvendelse af MitID-løsningen og NemLog-in. Det forventes at være regler, der fastlægger den ydelse, som de offentlige myndigheder og offentligretlige organer modtager. Derudover forventes det, at der bliver fastsat regler for håndtering af sikkerhedshændelser, mulighed for at modtage support m.v.

Det forventes, at der bliver fastsat særskilte vilkår om anvendelsen og tilslutning til MitID-løsningen. I forhold til NemLog-in forventes det, at der bliver fastsat vilkår til offentlige brugerorganisationer og et til offentlige tjenesteudbydere.

Digitaliseringsstyrelsen er systemejer af både MitID-løsningen og NemLog-in, og Digitaliseringsstyrelsen er, jf. § 3 og § 8, forpligtet til at stille løsningerne til rådighed for offentlige myndigheder og offentligretlige organer. Finansministeren fastsætter regler om, hvordan Digitaliseringsstyrelsen skal stille løsningerne til rådighed, herunder hvilke ydelser der mere specifikt skal tilbydes, kvalitetskrav og support.

Begge løsninger er store og komplekse digitale løsninger, der kræver regler for, hvordan de enkelte dele skal tilsluttes og anvendes af de offentlige myndigheder og offentligretlige organer, som aftager løsningerne, herunder regler om håndtering af certifikater.

Finansministeren fastsætter regler for offentlige myndigheder og offentligretlige organers tilslutning til og anvendelse af MitID-løsningen og NemLog-in. Betingelserne for juridiske enheder aftales kontraktuelt.

Til § 17

Der findes ikke gældende ret, som regulerer påbud i relation til MitID-løsningen eller NemLog-in.

Den foreslåede § 17, medfører, at Digitaliseringsstyrelsen kan meddele offentlige myndigheder og offentligretlige organer påbud om at opfylde forpligtelser i henhold til § 6, stk. 1, og § 11, stk. 1.

Digitaliseringsstyrelsen kan således meddele påbud om, at den offentlige myndighed eller det offentligretlige organ skal sikre, at privatpersoner og erhvervsbrugere gennem NemLog-in kan anvende MitID til

at få adgang til den offentlige myndigheds eller det offentligretlige organs digitale selvbetjeningsløsninger, hvis løsningerne kræver sikker autentifikation, jf. § 6, stk. 1.

Digitaliseringsstyrelsen kan derudover meddele påbud om, at den offentlige myndighed eller det offentligretlige organ skal sikre, at privatpersoner og erhvervsbrugere kan anvende serviceområderne Login og autentifikation samt Digital repræsentation i NemLog-in, når den offentlige myndigheds eller det offentligretlige organs digitale selvbetjeningsløsninger kræver det, jf. § 11, stk. 1.

Bestemmelsen giver Digitaliseringsstyrelsen mulighed for at udstede påbud i det tilfælde, at en offentlig myndighed eller et offentligretlig organ ikke overholder de forpligtelser, som er fastsat i loven.

Påbuddet udstedes skriftligt af Digitaliseringsstyrelsen. Digitaliseringsstyrelsen vil i forbindelse med påbud kunne angive en tidsfrist for, hvornår det pågældende forhold skal være bragt i orden. Det vurderes dog, at det ikke er hensigtsmæssigt at fastsætte en fast tidsfrist for, hvornår de offentlige myndigheder og offentligretlige organer skal opfylde de givne forpligtelser.

Derudover vil Digitaliseringsstyrelsen kunne følge op på et påbud, hvis dette vurderes nødvendigt.

Til § 18

I gældende ret er der i de nationale standarder for eID-ordninger fastsat krav til det tilsyn, som skal udføres for eID-ordninger. Den foreslåede bestemmelse sikrer overholdelse af de tilsynsforpligtelser, som er fastsat i de nationale standarder for eID-ordninger.

Endvidere er der i den gældende eIDAS-forordning fastsat krav til tilsyn for eID-ordninger. MitID-løsningen skal anmeldes til EU-Kommissionen som den nationale eID-ordning i Danmark. Det er i den forbindelse en forudsætning, at der føres tilsyn med løsningen, når MitID anvendes til grænseoverskridende transaktioner, jf. eIDAS-forordningens artikel 9, litra b.

Digitaliseringsstyrelsens tilsyn med MitID-løsningen dækker således både behovet efter denne lov samt kravene i medfør af eIDAS-forordningen.

Serviceområdet Digital signering i NemLog-in er en service, der er omfattet af eIDAS-forordningens kapitel III om tillidstjenester. Det følger af forordningens artikel 17, at hver medlemsstat udpeger et tilsynsorgan, samt hvilke opgaver tilsynsorganet varetager. Med lov nr. 617 af 8. juni 2016, om supplerende bestemmelser til forordning om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked blev Digitaliseringsstyrelsen udpeget til det nationale tilsynsorgan i Danmark. Tilsynet med serviceområdet Digital signering er således ikke omfattet af denne lovs foreslåede § 18, stk. 1.

Den foreslåede § 18, stk. 1, medfører, at Digitaliseringsstyrelsen fører tilsyn med drift, vedligeholdelse og forvaltning af MitID-løsningen og NemLog-in, herunder at løsningerne overholder nationale standarder for eID-ordninger.

Digitaliseringsstyrelsen bliver systemejer og tilsynsførende for MitID-løsningen og NemLog-in. Det er således formålet med den foreslåede stk. 1, at fastslå, at det er en myndighedsopgave at følge op på revisionserklæringer, audit og anden form for kontroldokumentation, som der afgives for løsningerne, herunder også tilsyn baseret på standarder, som skal udføres for løsningerne.

Digitaliseringsstyrelsens tilsyn, omfatter blandt andet, at der føres tilsyn med revisionsrapporter, audit og anden form for kontroldokumentation, der dokumenterer overholdelse af krav i denne lov eller regler udstedt i medfør af loven. Endvidere kan Digitaliseringsstyrelsen efter forudgående vurdering initiere at en uvildig sagkyndig, foretager revision og audit af offentlige myndigheder, offentligretlige organer eller juridiske enheder, jf. lovforslagets § 5 og § 10. Nærmere regler herom vil blive fastsat med hjemmel i den foreslåede stk. 2.

I Digitaliseringsstyrelsen er der ledelsesmæssig og organisatorisk adskillelse, således at tilsyn og

forvaltningen af de to løsninger bliver udført uafhængigt forskellige steder i styrelsen med forskellig ledelsesmæssig reference.

Den foreslåede § 18, stk. 2 medfører, at finansministeren kan fastsætte nærmere regler om Digitaliseringsstyrelsens tilsyn efter stk. 1, herunder om Digitaliseringsstyrelsens samarbejde med andre tilsynsmyndigheder efter aftale med vedkommende minister.

Med den foreslåede bestemmelse bemyndiges finansministeren til at fastsætte nærmere regler om udøvelsen og indholdet af tilsynet herunder samarbejdet med andre tilsynsmyndigheder og efter aftale med vedkommende minister.

Det forventes, at der fastsættes regler, som uddyber tilsynsforpligtelsen, der pålægges Digitaliseringsstyrelsen. Således sikres der gennemsigtighed omkring tilsynsforpligtelsen. Det forventes, at der i reglerne fastsættes at Digitaliseringsstyrelsens tilsyn blandt andet omfatter, at der føres tilsyn med revisionsrapporter, audit og anden form for kontroldokumentation, der dokumenterer overholdelse af krav i denne lov eller regler udstedt i medfør af loven. Endvidere forventes det, at der fastsættes regler om, at Digitaliseringsstyrelsen efter forudgående vurdering kan initiere, at en uvildig sagkyndig foretager revision og audit af offentlige myndigheder, offentligretlige organer eller juridiske enheder, jf. lovforslagets § 5 og § 10.

Til § 19

I gældende ret pålægges der tavshedspligt for en række subjekter omfattet af lovens bestemmelse, jf. straffeloven lovbekendtgørelse nr. 1650 af 17. november 2020 i §§ 152-152 f.

Med den foreslåede § 19, bestemmes det, at offentlige myndigheders medarbejdere og enhver, der i øvrigt udøver bistand til offentlige myndigheder, er under ansvar efter straffelovens §§ 152-152 f forpligtet til at iagttage tavshed over for uvedkommende med hensyn til oplysninger om den tekniske og sikkerhedsmæssige indretning samt processer for opretholdelse, vedligeholdelse og drift af sikkerhed i MitID-løsningen og NemLog-in.

Bestemmelsen indfører en særlig tavshedspligt, der medfører, at offentlige myndigheders medarbejdere iagttager tavshed over for uvedkommende med hensyn til oplysninger m.v. om MitID's og NemLog-in's systemers tekniske- og sikkerhedsmæssige indretning samt processer for opretholdelse, vedligeholdelse og drift af sikkerheden i systemerne.

Det skal bemærkes, at de subjekter, som er omfattet af straffelovens §§ 152-152 f udvides med den foreslåede bestemmelse. Bestemmelsen regulerer således tavshedspligten for offentlige myndigheders medarbejdere, samt enhver, der i øvrigt gennem bistand til eksempelvis gennemførelse af tilsyn og kontroller, eller til videreudvikling af systemerne, måtte få kendskab til MitID's og NemLog-in's systemernes tekniske- og sikkerhedsmæssige indretning samt processer for opretholdelse, vedligeholdelse og drift af sikkerheden i systemerne.

Bestemmelsen pålægger medarbejdere, der fører tilsyn og medarbejdere, der i øvrigt har adgang til oplysninger om den tekniske- og sikkerhedsmæssige indretning, tavshedspligt om disse. Bestemmelsen omfatter også den, der har virket i offentlig tjeneste eller hverv. Dette skyldes, at oplysningerne kan indikere svagheder i både systemer, systeminstallationer samt de sikkerhedsmæssige processer, som kan betyde, at tilsynet vil kræve forbedring af systemer, ændrede sikkerhedsmæssige processer eller lignende. Det er derfor afgørende, at disse oplysninger kan indberettes i fortrolighed til Digitaliseringsstyrelsen, da kendskab til og indsigt i systemers og processers eventuelle svagheder vil øge risikoen for angreb og kompromittering af sikkerheden. Angreb på systemer af så central karakter som fx MitID eller NemLog-in kan have vidtrækkende konsekvenser for borgere og erhvervsdrivende samt hele den offentlige sektor. Denne type angreb vil mindske tilliden til digitale tjenester og kan dermed begrænse den offentlige digitalisering og begrænse mulige gevinster heraf.

Der vurderes samtidig ikke at være hensyn, der tilsiger, at borgere, offentligretlige organer eller juridiske enheder skal være bekendt med de mere specifikke tekniske indretninger og sikkerhedsmæssige procedurer, som er med til at skabe sikkerheden i systemerne.

Bestemmelsen er ikke til hinder for, at offentlige myndigheder kan videregive oplysninger m.v. til andre offentlige myndigheder i det omfang, dette er nødvendigt for at disse kan udføre de opgaver, som de er pålagt.

Til § 20

I den gældende lov om NemID med offentlig digital signatur til fysiske personer og til medarbejdere i juridiske enheder af 8. maj 2018, er det fastsat i § 3, at forvaltningsloven finder anvendelse på afgørelser, som træffes af den private virksomhed, der er udpeget i medfør af lovens § 1, stk. 1, og af registreringsenheder, jf. lovens § 2.

Den foreslåede bestemmelse har til hensigt at videreføre den bestemmelse, som gælder for NemID-løsningen over i MitID-løsningen, da de samme betingelserne vil gøre sig gældende for de juridiske enheder, som udpeges efter den foreslåede § 4, stk. 2 og § 5, stk. 1.

Med den foreslåede § 20, stk. 1, bestemmes det, at forvaltningsloven finder anvendelse på afgørelser om udstedelse, spærring og genåbning af MitID, jf. § 4, stk. 2, som træffes af juridiske enheder, der er udpeget i medfør af § 5, stk. 1.

Bestemmelsen indebærer, at såfremt Digitaliseringsstyrelsen gør brug af muligheden for at udpege juridiske enheder, jf. § 5, stk. 1, til at varetage forvaltningsopgaver på vegne af Digitaliseringsstyrelsen, jf. § 4, stk. 2, skal de juridiske enheder, som træffer afgørelser om udstedelse, spærring og genåbning af MitID, overholde de samme regler, som Digitaliseringsstyrelsen er underlagt som offentlig myndighed. Det sikrer privatpersoners og erhvervsbrugeres retssikkerhed i den proces, som finder sted, når de modtager afgørelse om udstedelse, spærring og genåbning af MitID. Bestemmelsen er navnlig relevant, hvis en juridisk enhed, fx et pengeinstitut skal foretage registrering og udstedelse af MitID. Da en juridisk enhed normal ikke har pligt til at overholde forvaltningslovens regler, når de træffer en afgørelse, er det nødvendigt, at bestemmelsen præciserer, at forvaltningsloven vil finde anvendelse i de tilfælde, hvor en juridisk enhed udpeges til at træffe afgørelse om udstedelse, spærring og genåbning af MitID.

Det medfører blandt andet, at hvor der træffes afgørelser om udstedelse, spærring og genåbning af MitID, som opfylder afgørelsesbegrebet efter reglerne i forvaltningslovens kapitel 6 (§§ 22-24) skal forvaltningslovens regler herom overholdes. Derudover skal en afgørelse, der giver afslag ledsages af en klagevejledning, reglerne om partshøring iagttages, ligesom at privatpersoner og erhvervsbrugere skal tilbydes vejledning. Endelig skal det bemærkes, at der vil kunne forlanges aktindsigt efter forvaltningslovens regler. En afgørelse om at spærre et MitID træffes for at sikre mod misbrug. Spærring kan derfor foretages uden forudgående kontakt til den fysiske person eller erhvervsbrugeren.

De juridiske enheder vil således ved anmodning fra en fysisk person om at få udstedt MitID blandt andet skulle vejlede om reglerne for at få udstedt MitID og særligt reglerne for løbende at kunne anvende MitID, herunder om konsekvenserne ved ikke at overholde disse, jf. forvaltningslovens § 7.

Vejledningen kan i de konkrete tilfælde tillige omfatte, hvilke muligheder borgeren har for at blive betjent af den offentlige forvaltning uden et MitID, samt hvilke muligheder borgeren henholdsvis erhvervsbrugeren har for på ny at anmode om at få udstedt MitID.

Der henvises til bemærkningerne til lovforslagets § 5, stk. 1, hvad angår hensynet til, at Digitaliseringsstyrelsen får mulighed for at udpege juridiske enheder til på vegne af Digitaliseringsstyrelsen, at varetage opgaver om forvaltning af MitID-løsningen, herunder udstedelse, spærring og genåbning af MitID.

Den foreslåede § 20, stk. 2, medfører, at forvaltningsloven finder anvendelse på afgørelser om identitetssikring af juridiske enheder, spærring af brugerorganisationers adgang til Erhvervsadministration i

NemLog-in, samt spærring af digitale identiteter, jf. § 9, stk. 2, som træffes af juridiske enheder, der er udpeget i medfør af § 10.

Med bestemmelsen foreslås det, at forvaltningsloven og almindelige forvaltningsretlige principper finder anvendelse på afgørelser om identitetssikring af juridiske enheder, spærring af brugerorganisationers adgang til serviceområdet Erhvervsadministration i NemLog-in samt spærring af digitale identiteter efter regler fastsat i medfør af § 9, stk. 2, og som træffes af juridiske enheder, der kan udpeges i medfør af § 10.

Såfremt Digitaliseringsstyrelsen gør brug af muligheden for at udpege juridiske enheder til på vegne af Digitaliseringsstyrelsen at varetage opgaver om forvaltning af NemLog-in, skal de juridiske enheder overholde de samme regler, som Digitaliseringsstyrelsen er underlagt som offentlig myndighed. Det sikrer erhvervsbrugernes og de juridiske enheders retssikkerhed i den proces, som finder sted, når de modtager afgørelse om identitetssikring af juridiske enheder, spærring af brugerorganisationers adgang til serviceområdet Erhvervsadministration i NemLog-in samt spærring og genåbning af digitale identiteter.

Det medfører blandt andet, at afgørelser, som opfylder afgørelsesbegrebet efter forvaltningslovens § 19, skal ledsages af en begrundelse og en klagevejledning, at reglerne om partshøring skal iagttages, og at erhvervsbrugere og juridiske enheder skal vejledes tilstrækkeligt om deres rettigheder mv. En afgørelse om at spærre en erhvervsbruger eller en juridisk enhed i serviceområdet Erhvervsadministration i NemLog-in kan træffes for at sikre mod misbrug. Spærring kan derfor foretages uden forudgående kontakt til erhvervsbrugeren eller den juridiske enhed.

Til § 21

I gældende ret bestemmer eIDAS-forordningen i art. 10, nr. 1, at en medlemsstat, der anmelder en eID-løsning til EU-Kommissionen, er erstatningsansvarlig for skader, der forsætligt eller uagtsomt påføres privatpersoner, offentlig myndigheder, offentligretlige organer eller juridiske enheder, som følge af manglende overholdelse af forpligtelserne i henhold til art. 7, litra d og f i forbindelse med en grænseoverskridende transaktion.

Efter eIDAS-forordningens art. 7, litra d, skal den anmeldende stat sikre, at de personidentifikationsdata, der entydigt repræsenterer den pågældende skadelidte i overensstemmelse med de tekniske specifikationer mv., er knyttet til den rigtige fysiske eller juridiske person. Efter forordningens art. 7 e skal den part, der udsteder det elektroniske identifikationsmiddel sikre, at de elektroniske identifikationsmidler, som kan anvendes grænseoverskridende, og som knyttes til skadelidte, er i overensstemmelse med de tekniske specifikationer, standarder og procedurer for det relevante sikringsniveau.

eIDAS-forordningens erstatningsbestemmelser regulerer erstatning i en grænseoverskridende kontekst. Erstatningsansvaret dækker fejl i registrering og indrullering, uafhængigt af om MitID bruges i en grænseoverskridende eller national kontekst.

Der findes dog ikke i gældende ret regler om erstatningsansvar i relation til MitID-løsningen eller NemLog-in.

Den foreslåede § 21, medfører, at Digitaliseringsstyrelsen er erstatningsansvarlig over for privatpersoner, offentlig myndigheder, offentligretlige organer eller juridiske enheder, som følge af fejl i forbindelse med registrering, udstedelse og håndtering af MitID, anvendelse og autentifikation af en privatperson eller en erhvervsbruger, medmindre at Digitaliseringsstyrelsen kan godtgøre, at Digitaliseringsstyrelsen ikke har handlet forsætligt eller uagtsomt.

Bestemmelsen fastslår, at Digitaliseringsstyrelsen er erstatningsansvarlig over for privatpersoner, offentlige myndigheder, offentligretlige organer eller juridiske enheder, som følge af fejl i forbindelse med registrering, udstedelse og forvaltning af MitID. Der er tale om et ansvar med omvendt bevisbyrde, hvilket medfører, at Digitaliseringsstyrelsen alene er ansvarsfri, i det omfang Digitaliseringsstyrelsen kan godtgøre, at den ikke har handlet forsætligt eller uagtsomt. Herudover vil dansk rets almindelige

erstatningsregler være gældende. Skadelidte skal således dokumentere et økonomisk tab, ligesom der skal være årsagssammenhæng og adækvans mellem den lidte skade og den ansvarspådragende handling eller undladelse.

Den fastsatte bestemmelse berører ikke, at der ved den indgåede kontrakt med Nets DanID A/S om udvikling m.v. af MitID-løsningen er fastsat, at leverandøren i et vist omfang, herunder med sædvanlig beløbsmæssig begrænsning, bærer det i den foreslåede bestemmelse nævnte erstatningsansvar. Det er herunder fastsat, at leverandøren i et vist omfang hæfter for fejl i registrering m.v. af en elektronisk identitet som følge af fejlregistrering m.v. foretaget af de registreringsenheder, som jf. den foreslåede § 6 stk. 1 og 2 varetager registreringer. Leverandøren er ansvarlig for og fører kontrol med, at registreringsenhederne overholder de fastlagte instrukser.

Den omstændighed, at MitID ikke er tilgængelig, eller at autentifikationer fejler på grund af nedetid hos formidleren af autentifikationen eller hos den pågældende selvbetjeningsløsning, er ikke ansvarspådragende for Digitaliseringsstyrelsen og heller ikke videreført i kontrakten med leverandøren af MitID-løsningen.

Håndtering af manglende tilgængelighed af MitID-løsningen, MitID eller den selvbetjeningsløsning, der forsøges adgang til, påhviler den enkelte selvbetjeningsløsning En offentlig- eller en privat selvbetjeningsløsning må håndtere eventuel manglende adgang. Eksempler på hvorledes dette konkret er håndteret for så vidt angår offentlige digitale selvbetjeningsløsninger kan findes i bemærkningerne til § 10 i lov om Digital Post fra offentlige afsendere, samt i bemærkningerne til § 10 b, nr. 2, i lov om Nemrefusion.

Det bemærkes, at den foreslåede bestemmelse skal afgrænses i forhold til det erstatningsansvar, som påhviler en tjenesteudbyder. Dette indebærer, at Digitaliseringsstyrelsen ikke er erstatningssvarlig for manglende adgang til en selvbetjeningsløsning, som skyldes driftsforstyrrelser i MitID-løsningen. Her vil Digitaliseringsstyrelsen på anmodning kunne bistå tjenesteudbyderen med nærmere oplysninger om hændelsesforløb for eksempel varighed af nedetid. Det bemærkes, at der er høje krav til MitID-løsningens tilgængelighed, idet det er helt centralt for det digitale Danmark, at løsningen er tilgængelig.

Til § 22

I gældende ret reguleres delegation af beføjelser i relation til denne lov ikke.

Den foreslåede § 22, medfører at, finansministeren kan efter aftale med vedkommende minister bemyndige en anden statslig myndighed til at udøve de beføjelser, der i denne lov er tillagt Digitaliseringsstyrelsen.

Bestemmelsen fastslår, at finansministeren kan bemyndige en anden statslig myndighed til at udøve de beføjelser, der i denne lov er tillagt Digitaliseringsstyrelsen, efter aftale med vedkommende minister.

Ved en fremtidig ressortomlægning vil finansministeren således kunne delegere de kompetencer og opgaver, som Digitaliseringsstyrelsen har i medfør af denne lov, til en anden statslig myndighed efter aftale med en anden minister. Herved sikres en effektiv og smidig opgavevaretagelse ved en eventuel kommende ressortomlægning. Det er således muligt, at delegation kun vedrører dele af beføjelserne efter denne lov, fx beføjelsen til at udpege en juridisk enhed i medfør af den foreslåede § 5, stk. 1, til at forvalte løsningerne omfattet af loven eller til at føre tilsyn, jf. den foreslåede § 18.

Med bestemmelsen følger også, at de kompetencer og opgaver, som finansministeren i loven bemyndiges til at varetage ved udstedelse af bekendtgørelser, herunder om klageadgang, kan delegeres til anden myndighed efter aftale mellem finansministeren og anden minister.

Til § 23

I gældende ret fremgår hjemlen til det nuværende partnerskab mellem Digitaliseringsstyrelsen og FR I,

af tekstanmærkning nr. 120 ad 07.12.02 til § 7 på finansloven fra 2020 og er en videreførelse fra tidligere finansår.

Med den foreslåede § 23, kan Digitaliseringsstyrelsen samarbejde med offentlige myndigheder, offentligtretlige organer og juridiske enheder om at tilvejebringe fremtidige elektroniske identifikationsordninger svarende til MitID-løsningen eller andre løsninger, der måtte træde i stedet herfor.

Den foreslåede bestemmelse skaber hjemmel for Digitaliseringsstyrelsen til at indgå et fremtidigt samarbejde om tilvejebringelse af MitID-løsningen eller en anden elektronisk identifikationsordning (eID-løsning), der måtte træde i stedet herfor. Hjemlen indføres for at sikre kontinuitet og mulighed for et fortsat fremtidigt samarbejde mellem den offentlige og private sektor om udviklingen af den nationale eID-løsning.

Et fremtidigt samarbejde i medfør af den foreslåede § 23 kan eksempelvis etableres som det nuværende partnerskab om MitID-løsningen, som blev indgået med FR I af 16. september 2015 A/S på baggrund af en udbudslignende proces, som Digitaliseringsstyrelsen gennemførte i 2015/16. Det bemærkes, at bestemmelsen i den foreslåede § 23 ikke vedrører det nuværende partnerskab mellem Digitaliseringsstyrelsen og FR I.

Både MitID-løsningen og NemLog-in er tilvejebragt gennem EU-udbud, som nærmere beskrevet i de almindelige bemærkninger afsnit 2.1.2. og 2.2.2. Det er også hensigten, at fremtidige løsninger vil skulle tilvejebringes gennem EU-udbud.

Til § 24

I gældende ret reguleres NemID i lov om NemID. Med idriftsættelsen af MitID-løsningen vil NemID-løsningen stadig være i drift indtil migreringen til MitID-løsningen er fuldstændig gennemført. I den periode vil der være behov for begge regelsæt. Der findes dog på nuværende tidspunkt ikke regler, som muliggør ophævelsen af NemID-løsningen, når NemID-løsningen tages ud af drift.

Der findes ikke i gældende ret regler om ikrafttrædelsen af regler om MitID-løsningen og NemLog-in.

Den foreslåede § 24, *stk. 1*, medfører, at finansministeren fastsætter tidspunktet for lovens ikrafttræden, og kan bestemme, at forskellige dele af loven træder i kraft på forskellige tidspunkter.

Bestemmelsen indebærer, at ikrafttræden af loven følger udviklingerne af løsningerne. Med den foreslåede bestemmelse muliggøres det, at lovgrundlaget kan træde i kraft, så snart løsningerne er klar til anvendelse og der sikres således et retsgrundlag for anvendelsen af løsningerne.

Når ikrafttrædelsen sker ved nærmere fastsættelse i bekendtgørelse, sikre det, at eventuelle justeringer i tidsplanerne for de to løsninger ikke skal medføre en lovændring.

Til § 25

I gældende ret reguleres NemID i lov om NemID. For afgørelser om udstedelse og klage over NemID finder de gældende regler i lovgrundlaget for denne løsning anvendelse indtil den fysiske person og medarbejderen i den juridiske enhed får udstedt et MitID. Med idriftsættelsen af MitID-løsningen vil NemID-løsningen stadig være i drift indtil migreringen til MitID-løsningen er fuldstændig gennemført. I den periode vil der være behov for begge regelsæt. Der findes dog på nuværende tidspunkt ikke regler, som muliggør ophævelsen af NemID-løsningen, når NemID-løsningen tages ud af drift.

Den foreslåede § 25, *stk. 1*, medfører at finansministeren kan fastsætte regler om ophævelse af lov nr. 439 af 8. maj 2018, om udstedelse af NemID med offentlig digital signatur til fysiske personer og til medarbejdere i juridiske enheder.

Med den foreslåede bestemmelse har finansministeren mulighed for at ophæve Lov om NemID, når dette bliver nødvendigt. Tidspunktet for ophævelsen afhænger af, hvornår migreringen til MitID kan afsluttes. Efter endt migrering vil alle privatpersoner og erhvervsbrugere kunne betjene sig med MitID

eller på anden vis, som erstatter behovet for autentifikation med NemID. Derudover vil serviceområdet Digital signering i NemLog-in kunne anvendes som ny signaturtjeneste, hvorfor behovet for den digital signatur i NemID ophører. Det forventes, at migreringen er fuldført i medio 2023, men datoen for fuld migreringen afhænger af løsningernes fulde tilgængelighed og kan derfor ikke fastsættes allerede ved lovens fremsættelse. Når finansministeren således har mulighed for at ophæve lov om NemID ved ikrafttrædelse af regler herom, understøttes det, at migreringen kan finde sted og gennemføres fuldstændigt med begge regelsæt. Herved sikres borgernes retsstilling gennem hele migreringsperioden.

Med den foreslåede bestemmelse sikres det, at den drift og forvaltning af NemID-løsningen som er nødvendig i migreringsperioden forsat har lovhjemmel. Dette indebærer bl.a., at der forsat vil være lovhjemmel til at få udstedt NemID i migreringsperioden, ligesom de regler, som knytter sig til forvaltningen af NemID, herunder om udstedelse og spærring stadig kan påberåbes af borgere og medarbejdere i virksomheder. Endelig sikres det, at der forsat kan indbringes klager over afgørelser om NemID til Digitaliseringsstyrelsen. Det forventes, at der i bekendtgørelsen om NemID indføres overgangsregler, som har til formål at nedlukke udstedelsen af NemID, således at borgere og medarbejdere i stedet skal have udstedt MitID, såfremt MitID, som elektronisk identifikation, kan erstatte de behov, som borgeren eller medarbejderens havde ved anvendelsen af NemID.

Til § 26

I gældende ret reguleres NemID-løsning i lov om NemID, hvor der er fastsat hjemmel til, at loven ved kongelig anordning kan sættes helt eller delvist i kraft for Grønland med de ændringer, som de grønlandske forhold tilsiger, jf. § 7. Med hjemmel i § 7 i lov om NemID med offentlig digital signatur til fysiske personer og til medarbejdere i juridiske enheder er der således fastsat anordning nr. 1484 af 12. november 2018 om ikrafttræden for Grønland af lov om udstedelse af NemID med offentlig digital signatur til fysiske personer og til medarbejdere i juridiske enheder.

Der er ikke i NemID-løsningen mulighed for at sætte reglerne om NemID i kraft for Færøerne. Dog har der været udtrykt ønske fra Færøerne om, at en sådan hjemmel for MitID-løsningen vil være aktuel.

Den foreslåede § 26, medfører, at loven ikke gælder 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 grønlandske forhold tilsiger.

For Grønland er der tale om et sagsområde, der ikke er overtaget. I gældende ret reguleres NemID-løsning i lov om NemID, hvor der er fastsat hjemmel til, at loven ved kongelig anordning kan sættes helt eller delvist i kraft for Grønland med de ændringer, som de grønlandske forhold tilsiger, jf. § 7. Med hjemmel i § 7 i lov om NemID med offentlig digital signatur til fysiske personer og til medarbejdere i juridiske enheder er der således fastsat anordning nr. 1484 af 12. november 2018 om ikrafttræden for Grønland af lov om udstedelse af NemID med offentlig digital signatur til fysiske personer og til medarbejdere i juridiske enheder.

Det foreslås, at loven skal kunne sættes i kraft for Grønland med henblik på at grønlandske kommuner skal kunne udstede MitID til borgere på samme måde som de grønlandske kommuner i dag udsteder NemID. Loven vil helt eller delvist kunne sættes i kraft for Grønland.

For Færøerne vedrører lovforslaget et sagsområde, som er overtaget af de færøske myndigheder. Der er imidlertid et ønske fra de færøske myndigheder om, at det skal være muligt at udstede MitID.

Der er med virkning fra den 1. januar 2021 tilvejebragt hjemmel til, at færinger ved henvendelse til Rigsombudsmanden på Færøerne kan få tildelt et dansk administrativt personnummer. Rigsombudsmanden kan endvidere udstede NemID til borgere med dansk personnummer.

Med loven skabes der hjemmel til, at reglerne om MitID kan sættes i kraft for Færøerne med henblik på,

at Rigsombudsmanden på Færøerne kan udstede MitID til borgere med dansk personnummer, når NemID udfases på Færøerne og erstattes af MitID.

Loven vil helt eller delvist kunne sættes i kraft for Færøerne.