

Afsnit I Generelle bestemmelser

Kapitel 1 *Lovens anvendelsesområde*

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

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

Kapitel 2 *Definitioner*

§ 2. I denne lov forstås ved:

- 1) **MitID-løsningen:** Den danske nationale elektroniske identifikationsordning, som vil blive anmeldt i henhold til eIDAS-forordningen.
- 2) **MitID:** Den nationale digitale identitet af en privatperson og tilhørende elektroniske identifikationsmidler, som kan tilknyttes privatpersoners og erhvervsbrugeres digitale identiteter.
- 3) **Autentifikation:** En proces som genkender og verificerer en digital identitet gennem anvendelse af et elektronisk identifikationsmiddel.
- 4) **Sikringsniveau:** Der sondres mellem tre forskellige sikringsniveauer for autentifikation, henholdsvis niveau lav, betydelig og høj.
- 5) **Sikker autentifikation:** Autentifikation på niveau 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:** En fysisk person, der udelukkende agerer på vegne af sig selv uden forbindelse til en juridisk enhed, og som ikke er en erhvervsbruger.
- 8) **Erhvervsbruger:** En fysisk person, der er associeret med en offentlige 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:** Ved juridisk enhed forstås en juridisk enhed med et cvr-nummer, der hverken er en offentlig myndighed, jf. nr. 10) eller et offentligretligt organ, jf. nr. 11).
- 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. 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.

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, vedligeholdelse og forvaltning af løsningen.

Stk. 2. Digitaliseringsstyrelsen stiller MitID til rådighed for privatpersoner og erhvervsbrugere, såfremt privatpersoner og erhvervsbrugere opfylder reglerne om udstedelse af MitID, som fastsat i medfør af § 4, stk. 2.

Kapitel 4

Forvaltning af MitID-løsningen og MitID

§ 4. Digitaliseringsstyrelsen sikrer:

- a) At der sker identitetssikring af privatpersoner, registrering af identiteter, udstedelse, spærring og genåbning af MitID til privatpersoner efter reglerne fastsat i medfør af stk. 2.
- b) At der sker udstedelse, spærring 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 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 med udvikling, drift, vedligeholdelse og forvaltning af MitID-løsningen samt opgaver i medfør af § 4, stk. 1.

Stk. 2. Kommunale borgerservicecentre skal varetage opgaver i henhold til § 4 stk. 1.

Kapitel 5

Anvendelse af MitID-løsningen og MitID

§ 6. Når offentlige myndigheder og offentligretlige organer anvender en digital selvbetjeningsløsning til at udføre en myndighedsopgave, skal de sikre, at privatpersoner og erhvervsbrugere kan anvende MitID til at få 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, vedligeholdelse og forvaltning af NemLog-in.

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

- 1) Login og autentifikation, som sikrer, at privatpersoner og erhvervsbrugere kan tilgå digitale selvbetjeningsløsninger.
- 2) Digital repræsentation, som sikrer:
 - a) At en privatperson 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) At en erhvervsbruger, der selvstændigt kan repræsentere en juridisk enhed, kan lade den juridiske enhed repræsentere digitalt af en erhvervsbruger fra en anden juridisk enhed over for en offentlig myndighed eller et offentligretligt organ, som udbyder en digital selvbetjeningsløsning.
- 3) Digital signering, som sikrer:
 - 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:

- a) At offentlige myndigheder, offentligretlige organer og juridiske enheder kan oprette, administrere og anvende digitale erhvervsidentiteter samt tildele og administrere elektroniske identifikationsmidler, såfremt de overholder reglerne om identitetssikring ved oprettelse som brugerorganisation, som nærmere fastsat i medfør af § 9, stk. 2.
- 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 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 Erhvervsadministrationen i NemLog-in samt erhvervsbrugeres digitale identiteter kan spærres og genåbnes efter reglerne fastsat i medfør af stk. 2.

Stk. 2. 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 med udvikling, drift, vedligeholdelse og forvaltning af NemLog-in 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 Login og autentifikation, Digital signering og Erhvervsadministration, jf. § 8, stk. 2, nr. 1 og nr. 3 samt stk. 3.

Afsnit IV

Dataansvar og 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 og risikodata vedrørende den konkrete og enkelte transaktion til en offentlig myndighed, et offentligretligt organ eller en juridisk enhed i rollen som broker, der er tilsluttet MitID-løsningen eller NemLog-in.

Stk. 2. En offentlig myndighed, et offentligretligt organ eller en juridisk enhed i rollen som broker kan foretage automatiske afgørelser om log-in på baggrund af risikodata videregivet efter stk.1.

Stk. 3. En offentlig myndighed, et offentligretligt organ eller en juridisk enhed i rollen som broker, der i medfør af stk. 1, har modtaget autentifikationssvar, kan videregive dette til en tjenesteudbyder, der gennem pågældende offentlige myndighed, offentligretlige organ eller juridiske enhed, i rollen som broker, modtager autentifikationer fra MitID-løsningen.

Stk. 4. Ved en erhvervsbrugers anvendelse af et elektroniske identifikationsmiddel fra en lokal identitetsgarant tilsluttet NemLog-in, kan Digitaliseringsstyrelsen videregive autentifikationssvar vedrørende den konkrete og enkelte transaktion til en offentlig myndighed, et offentligretligt organ eller en juridisk enhed i rollen som broker, der er tilsluttet NemLog-in.

Stk. 5. En offentlig myndighed, et offentligretligt organ eller en juridisk enhed i rollen som broker, der i medfør af stk. 4, har modtaget autentifikationssvar, kan videregive dette til en tjenesteudbyder, der gennem pågældende offentlige myndighed, offentligretlige organ eller juridiske enhed, i rollen som broker, modtager autentifikationer fra NemLog-in.

§ 14. Digitaliseringsstyrelsen kan behandle persondata, jf. databeskyttelsesforordningens artikel 9, stk. 1, i forbindelse med valideringen af digitale signaturer i valideringstjenesten i serviceområdet Digital signering.

Afsnit V

Øvrige bestemmelser

Kapitel 11

Opkrævning af gebyr og vederlag

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

Stk. 2. Digitaliseringsstyrelsen indgår aftale med juridiske enheder om vederlag for tilslutning til og anvendelse af MitID-løsningen og NemLog-in.

Stk. 3. Offentlige myndigheder og offentligretlige organer betaler for MitID-løsningen og NemLog-in gennem fællesoffentlig finansiering eller ved betaling af vederlag fastsat af finansministeren.

Kapitel 12

Regler om tilrådighedsstillelse og anvendelse for offentlige myndigheder og offentligretlige organer

§ 16. Finansministeren fastsætter regler om tilrådighedsstillelsen 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 13

Påbud

§ 17. Digitaliseringsstyrelsen kan meddele offentlige myndigheder og offentligretlige organer påbud med henblik på at opfylde forpligtelser i henhold til § 6, stk. 1, og § 12, stk. 1.

Stk. 2. Finansministeren kan fastsætte nærmere regler om meddelelse af påbud.

Kapitel 12

Tilsyn

§ 18. Digitaliseringsstyrelsen påser overholdelse af regler fastsat i medfør af § 4, stk. 2 og § 9, stk. 2.

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 13

Tavshedspligt

§ 19. Myndigheder og myndighedernes medarbejdere, der udøver tilsyn i medfør af § 18, er under ansvar efter straffelovens §§ 152-152 f forpligtet til at iagttage ubetinget 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 14

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 15

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, med mindre, at Digitaliseringsstyrelsen kan godtgøre, at Digitaliseringsstyrelsen ikke har handlet forsætligt eller uagtsomt.

Kapitel 16

Delegation

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

Kapitel 17

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.

Ikrafttræden

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

Stk. 2. [I lov om xxx foretages følgende ændring: xxx]

Færøerne og Grønland

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

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1.	Lovforslagets formål og baggrund	10
2.	Lovforslagets hovedindhold	12
2.1.	Gældende ret.....	12
2.1.1.	NemID	12
2.1.2.	NemLog-in.....	13
2.2.	Finansministeriets overvejelser.....	14
2.2.1.	MitID-løsningen og MitID	14
2.2.2.	NemLog-in.....	17
2.2.3.	Centrale tekniske ændringer	19
2.3.	Den foreslåede ordning.....	20
3.	Økonomiske og implementeringskonsekvenser for det offentlige	25
4.	Økonomiske og administrative konsekvenser for erhvervslivet m.v.....	26
5.	Administrative konsekvenser for borgere.....	32
6.	Klima- og miljømæssige konsekvenser.....	33
7.	Forholdet til EU-retten.....	33
7.1.	eIDAS-forordningen.....	33
7.1.1.	Den Nationale Standard for identiteters sikringsniveauer	34
7.2.	Reglerne om fri bevægelighed og udbudsretten.....	35
7.3.	Databeskyttelsesforordningen	35
7.3.1.	Databeskyttelsesretlige overvejelser	36
7.3.1.1.	Behandling af personoplysninger i MitID	36
7.3.1.2.	Behandling af personoplysninger i NemLog-in.....	39
8.	Hørte myndigheder og organisationer m.v.....	41
9.	Sammenfattende skema	42

1. Lovforslagets formål og baggrund

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 indgår 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 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. 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. Se nærmere herom bemærkningerne til § 8, stk. 2, litra b, nr. 3.

MitID bliver den danske nationale eID-løsning og vil leve op til kravene i 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). Om lovforslagets forhold til eIDAS-forordningen henvises til afsnit 7.1.

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 en ny erhvervsidentitetsløsning, som erstatning for NemID til erhverv 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 (NSIS). Standarden er i overensstemmelse med krav fra eIDAS-forordningen og definerer en national ramme for tillid til digitale identiteter.

Formålet med lovforslaget er at fremtidssikre organiseringen af den myndighedsopgave, som udvikling og tilrådighedsstillelse af disse centrale løsninger i den kritiske offentlige digitale infrastruktur udgør. Med en samlet statslig kontrol med MitID-løsningen og NemLog-in, vil disse centrale løsninger løbende og effektivt kunne opdateres i takt med den teknologiske udvikling samt et skiftende digitalt trusselsbillede. Med lovforslaget foreslås det, at Digitaliseringsstyrelsen pålægges denne myndighedsopgave. Placeringen af denne opgave hos Digitaliseringsstyrelsen ligger inden for medlemsstaternes ret til at organisere deres forvaltning.

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, og 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 hovedindhold

2.1. Gældende ret

2.1.1. NemID

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. 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 den bemyndigelse fastsætter bekendtgørelse nr. 899 af 21. juni 2018 om udstedelse og spærring af NemID med offentlig digital signatur 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. Den daværende IT- og Telestyrelse, nu Digitaliseringsstyrelsen, har udarbejdede fire OCES-certifikatpolitikker for henholdsvis person-, medarbejder-, virksomheds- og funktionscertifikater. 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 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 lov nr. 528 af 11. juni 2012 om Digital Post fra offentlige afsendere, 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 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.dk 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. Forordningen er nærmere beskrevet i afsnit 7.1.

2.1.2. NemLog-in

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.

Af finansloven fra 2018 (§07.12.02) fremgår af tekstanmærkning nr. 124, stk. 1, 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, Udviklingsselskabet 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 tekstanmærkningernes nr. 124, stk. 2, at de offentlige myndigheder, selvejende institutioner mv. kan vælge at gøre brug af aftalen.

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. 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 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. Finansministeriets overvejelser

2.2.1. MitID-løsningen og MitID

Kontrakten med Nets 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 FRI af 16. september 2015, et selskab under bankernes interesseorganisation Finans 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 nationalt 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, fornyes ligeledes med MitID.

Herudover vil MitID-løsningen fremadrettet alene udgøre en autentifikationsløsning, hvor NemID-løsningen ud over autentifikation blandt andet 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 Signatur til den digitale underskrift baseret på autentifikation med MitID.

Med introduktionen af de nye løsninger bliver det muligt at fortsætte udviklingen i retning af en mere fleksibel og modulær arkitektur i den fællesoffentlige infrastruktur for digitale identiteter. Derudover er løsningerne baseret på løst koblede identiteter og identifikationsmidler, som særligt for erhvervsbrugere vil opleves som mere fleksible.

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 verificeret af brokeren 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-kernen direkte, tilgår løsningen gennem en broker. NemLog-in vil fungere som den fællesoffentlige broker for MitID og vil således være MitID-identitetsbroker.

Ud over MitID-identitetsbrokere vil der kunne være andre identitetsbrokere 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 betroet til at udstede lokale elektroniske identiteter, der er associeret med en eller flere brugerorganisationer oprettet i serviceområdet erhvervsadministration i NemLog-in.

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 kernen samt autentifikationsprocessen af slutbrugeren.

Finansministeren har med organiseringen af tilrådighedsstillelsen af den kritiske fællesoffentlige digitale infrastruktur blandt andet lagt vægt på, at det i Danmark i overensstemmelse med eIDAS-forordningen er valgt, at der kun skal være én national eID-løsning. Endvidere har sikkerheden, herunder forsyningssikkerheden i disse digitale løsninger, hvoraf MitID-løsningen og NemLog-in udgør kernen, haft betydning i overvejelserne om organiseringen af tilrådighedsstillelsen 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 de samme grunde er det en myndighedsopgave 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, når de udfører myndighedsopgaver, og det kræver sikker autentifikation.

Ovenstående udelukker ikke, at offentlige myndigheder og offentligretlige organer kan vælge at anvende lokale identitetsgaranter og lokale identifikationsmidler på deres digitale selvbetjeningsløsninger. 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. Når der på sigt er opstået et brokemarked, vil offentlige myndigheder og offentligretlige organer således kunne 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. Desuden vil offentlige myndigheder og offentligretlige organer kunne vælge at anvende lokale identifikationsmidler.

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.

2.2.2. *NemLog-in*

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 NemLog-in. 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. 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 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, hvis de følger de regler om tilslutning, som følger af loven. 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. MitID-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.

2.2.3. *Centrale tekniske ændringer*

Finansministeriets overvejelser har ført til, at der med lovforslaget introduceres en række tekniske ændringer.

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.

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 privat brug 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 simple 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.

2.3. *Den foreslåede ordning*

Med introduktion af MitID-løsningen og NemLog-in er det fra offentlig side hensigten at fortsætte udviklingen i retning af en mere fleksibel og modular 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 og NemLog-in 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 og landsdækkende udbredelse af velfærdsteknologi 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 privatpersonernes og juridiske enheders forventninger om effektiv og sammenhængende offentlig service. Sikre digitale identiteter og dertil relaterede services er en forudsætning for den digitale offentlige forvaltning, derfor pålægges Digitaliseringsstyrelsen med loven som myndighedsopgave at stille MitID-løsningen og 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. Relationen 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 tilrådgivelsesstillelsen af ovenstående løsninger sker centralt som led i en myndighedsopgave, sikres grundlaget for en fællesoffentlig it-infrastruktur. Tilrådgivelsesstillelsen 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.

Ordningen kan i oversigtsform illustreres som følger:

MitID-løsningen:

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

NemLog-in for tjenesteudbydere:

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 offentligretlige organer
Erhvervsadministration	Høj eller betydelig (sikker autentifikation)	Ret

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 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 identifikationsmiddel, 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, når myndighederne forpligtes til at anvende de samme it-infrastrukturløsninger.

Pligten til at anvende løsningen 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 MitID-løsningen og NemLog-in. Når offentlige myndigheder og offentligretlige organer har en ret til at anskaffe disse dele af MitID-løsningen og 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 offentligretligt 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 anvendelsen, 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 organer 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 tjenesteudbyder. 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, lov nr. 1564 af 15. december 2015 (udbudsloven), til at levere MitID-løsningen og NemLog-in 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 udbudsdirektivet. Der henvises i øvrigt til afsnit 2.2.1 og 2.2.2 ovenfor om de udbud, som Digitaliseringsstyrelsen gennemførte på vegne af hele den offentlige forvaltning ved løsningernes anskaffelse.

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

3. *Økonomiske 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 NemLog-in. Omkostningerne til udvikling af MitID-løsningen sker i samarbejde med banksektoren, gennem partnerskabet FRI af 16. september 2015, som er et selskab under bankernes interesseorganisation Finans Danmark. Af udviklingsomkostningerne finansieres 50 procent af banksektoren. Driften for MitID-løsningen finansieres af de transaktioner, der foretages gennem anvendelsen 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 657,2 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. Omstillingsomkostningerne 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 understøttes samtidigt 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 private personer 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 elektroniske identifikationsmidler. Ud over de tre elektroniske identifikationsmidler er det tiltænkt, at MitID-appen kan anvendes som elektronisk identifikationsmiddel uden brugerbetaling.

Med lovforslaget fastslås det, at privatpersoner og erhvervsbrugere kan klage til Digitaliseringsstyrelsen. Digitaliseringsstyrelsen vil med lovforslaget fortsat skulle behandle klager og træffe afgørelse, hvis privatpersoner klager over, at deres MitID er blevet helt eller delvist spærret eller over et afslag på udstedelse af MitID. Ligeledes fastsættes en hjemmel til at etablere en klageadgang for serviceområdet Erhvervsadministration i NemLog-in. Klageadgangen gælder for myndigheder og virksomheder som brugerorganisationer, der fx ikke kan blive oprettet i 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. Hovedparten 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 private personer 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. Med ændringerne for erhvervsbrugerne kan der muligvis i implementeringsperioden komme flere klager på grund af den omstilling, som erhvervsbrugerne skal gennemgå. På sigt forventes det, at klageantallet reduceres til niveauet i dag, idet erhvervsbrugerne 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 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.

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

Lovforslaget har væsentlige økonomiske og administrative konsekvenser for erhvervslivet.

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. De administrative konsekvenser er beskrevet og, i det omfang det har været muligt, estimeret nedenfor.

Det vurderes, at der er betydelige administrative konsekvenser forbundet med, at juridiske enheder fremadrettet vil kunne få tildelt og administrere deres digitale identiteter 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 estimerterne 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:

En samlet tilslutning og administration

Med videreudviklingen af NemLog-in vil det blive lettere for en juridisk enhed at tilslutte sig Erhvervsadministration som brugerorganisation og efterfølgende administrere brugerorganisationens 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 detailspecifisere ønsket funktionalitet i tilslutningsforløbet. I begge tilfælde vil en brugerorganisation efterfølgende kunne ændre opsætningen, hvis den juridiske enheds forhold og behov ændrer sig.

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 NemLog-in-serviceområdet Erhvervsadministration, 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 til at være ca. 10 minutter pr. oprettelse for den normale effektive 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 normale 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.

Fleksibel anvendelse af identifikationsmidler

I det nye serviceområde Erhvervsadministration har brugerorganisationer og deres erhvervsbrugere mulighed for at tilknytte og anvende forskellige typer identifikationsmidler i sammenhæng med oprettede erhvervsidentiteter. Det bliver muligt at anvende 1) MitID identifikationsmidler udstedt til den private person, såfremt den juridiske enhed og den private person 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 brugere tilknyttet en lokal identitetsgarant. Samlet set giver dette en langt større

fleksibilitet og administrativ lettelse for erhvervsbrugere parallelt med, 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 mobilløsningen. 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 mobil loginløsning, 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 signaturer. 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 signaturer 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 den nye mobile loginløsning til mellem 4 og 59 mio. kr.

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 medarbejderne vil derefter skulle bruge 5-15 min. på at opsætte deres nye loginmiddel. Omstillingsomkostningerne hertil forventes at udgøre ca. 97 – 195 mio. kr.

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

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 ikke-diskriminerende og skal sikre, at der ikke sker konkurrencefordrejning. Gebyrerne vil blive fastsat på bekendtgørelsesniveau. Se nærmere herom i lovforslagets specielle bemærkninger til § 15.

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.

1. Muliggør anvendelse af nye forretningsmodeller

Det er Digitaliseringsstyrelsens vurdering, at lovforslaget bidrager til, at nye forretningsmodeller kan realiseres. Både MitID og NemLog-in løsningerne opdateres, hvorved private og offentlige aktørers adgang til den digitale infrastruktur forbedres og sikres.

eIDAS-forordningen

Det forventes, at serviceområdet Digital signering i NemLog-in vil opnå status som en kvalificeret tjeneste 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 Digital signering opnår status som kvalificeret tillidstjeneste betyder, at virksomheder såvel som privatpersoner ved anvendelse af Digital signering opnår en ensartet retstilstand på tværs af EU, hvilket forbedrer mulighederne for elektronisk forretningsførelse og elektronisk handel i EU.

Broker-model

Et andet aspekt, der muliggør nye forretningsmodeller, er MitID-brockermodellen. MitID-brockermodellen giver frem over mulighed for, at private 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 juridiske 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 brokerens ydelser og omstillingsomkostninger i forbindelse med overgangen til MitID. Der eksisterer ikke i dag et marked af

brokere, men der gives med dette tiltag mulighed for, at et sådant marked vil kunne opstå. Juridiske enheder vil i henhold til lovforslaget således kunne indgå aftale med en broker som har indgået aftale med og er certificeret af Digitaliseringsstyrelsen om anvendelse af MitID-løsningen.

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.

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, at en juridisk enhed kan anvende egne lokale identiteter og identifikationsmidler i sammenhæng 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, og autentifikation til lokale it-systemer.

Det forventes, at relativt få juridiske enheder vil etablere sig som lokale identitetsgaranter, idet det kræver stor teknisk kapacitet og investering. Der vil formentlig være tale om meget store og avancerede private virksomheder.

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

2. Mere enkel og formålsbestemt

Lovforslaget har et klart fokus på at stille løsninger til rådighed for offentlige myndigheder og private. 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 tilrådgighedsstillelsen reguleres efter hver sin bestemmelse og kapitel. Kapitlerne for hver løsning, henholdsvis MitID og NemLog-in, indledes med en bestemmelse om tilrådgighedsstillelsen af løsningerne, og i de specielle bemærkningerne er indeholdt nærmere beskrivelser af den nærmere regulering af løsningerne. Herudover er tilrådgighedsstillelsen af NemLog-in inddelt i de serviceområder, som NemLog-in indeholder.

3. Teknologineutral

Private 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.

4. Helhedstænkende

Digitaliseringsstyrelsen vurderer, at lovforslaget ligger i tråd med andre relevante reguleringsområder og ikke hæmmer anvendelsen af nye teknologier og forretningsområder. Som eksempel herpå har styrelsen indgået et partnerskab med bankernes interesseorganisation Finans Danmark om udvikling af det nye MitID.

5. Sikrer brugervenlig digitalisering

Log-in og autentifikation via MitID og NemLog-in udgør ikke i sig selv en løsning, der udmønter erhvervsrettet regulering, men er en grundlæggende forudsætning for digitalisering. Serviceområder i NemLog-in såsom digital repræsentation har i højere grad karakter af løsninger, der varetager og muliggør erhvervsrettede funktioner. Serviceområdet Digital repræsentation understøtter partsrepræsentation, som det er fastsat i forvaltningslovens § 8 for blandt andet enkeltmandsvirksomheder, mens det med serviceområdet Erhvervsadministration vil være muligt at tilknytte og administrere rettigheder til en brugers identitet, 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 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.

5. *Administrative konsekvenser for borgere*

Med en omstilling fra NemID til MitID vil der være en omstilling til en ny ID-løsning, som ikke længere indeholder det analoge identifikationsmiddel, nøglekortet. Med udfasningen 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 identifikationsmidlet som mobilapplikation, vil dog fortsat kunne vælge fysiske 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 samtidig 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 skal fastslås, at privatpersoner kan klage til Digitaliseringsstyrelsen over afslag på at få udstedt MitID mv.

6. *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.

7. *Forholdet til EU-retten*

Lovforslaget indeholder ikke bestemmelser, der gennemfører ny eller ændret EU-regulering.

7.1. *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 elektroniske identifikationsmidler (eID), som i henhold til eIDAS-forordningen er anmeldt til Kommissionen på sikringsniveau betydelig eller høj, i deres offentlige digitale selvbetjeningsløsninger.

Idet NemLog-in indeholder tillidstjenester til brug for elektroniske transaktioner, særligt i forbindelse med elektronisk signering og tidsstempling, og MitID vil blive anmeldt som den danske nationale elektroniske identifikationsløsning i henhold til eIDAS-forordningen, er løsningerne underlagt bestemmelser i eIDAS. 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 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. 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).

7.1.1. Den Nationale Standard for identiteters sikringsniveauer

Den Nationale Standard for identiteters sikringsniveauer (NSIS-standard), 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-standard er 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-standard er tilpasset nationale forhold og er mere detaljeret end den gennemførelsesretsakt (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-standard er at skabe rammerne for tillid til digitale identiteter samt identitetstjenester nationalt. NSIS-standard definerer krav til styrken af en autentifikationsproces, den underliggende identitetssikring og det anvendte elektroniske identifikationsmiddel, udtrykt som et samlet sikringsniveau. NSIS-standard 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-standard implementerer de tre 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-standard 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.

7.2. Reglerne 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 afsnit 2.3, 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 private personer 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 EUF-traktaten.

7.3. Databeskyttelsesforordningen

MitID og NemLog-in vil behandle personoplysninger om det meste af den danske befolkning samt for en del udenlandske statsborgere, der har behov for adgang til danske offentlige digitale tjenester. Personoplysningerne, der indgår i systemet, er nødvendige for, at fysiske personer kan autentificere sig i offentlige digitale selvbetjeningsløsninger, så offentlige myndigheder baseret herpå kan udføre deres myndighedsopgaver og tilbyde borgerne service. Mængden og karakteren af personoplysningerne, der behandles i systemerne, kan derfor medføre en risiko for statens sikkerhed, hvis de placeres uden for Danmark.

Databeskyttelseslovens § 3, stk. 9 angår vurderingen af, hvornår it-systemer af samfundskritisk natur skal opbevares i Danmark, og derfor ikke må opbevares i udlandet. Formålet er at sikre, at visse it-systemer opbevares på servere i Danmark af hensyn til statens sikkerhed. Ved at placere de omfattede systemer i Danmark sikres det, at de danske myndigheder er kompetente til at håndhæve regler, der gælder for it-systemerne og de data, der behandles i dem. Vurderingen af hvorvidt et givent it-system er omfattet af lokationsreglen foretages af Justitsministeren efter forhandling med vedkommende minister.

Vurderingen indeholder en række momenter, herunder omfanget og karakteren af de opbevarede personoplysninger, konsekvenserne ved it-systemets utilgængelighed, konsekvenserne ved kompromittering af systemets personoplysninger, og hvor længe det vil tage at overflytte systemet til en ny leverandør.

Justitsministeren har vurderet, at MitID og NemLog-in er omfattet af databeskyttelseslovens § 3, stk. 9, hvorfor disse it-systemer skal føres i Danmark.

7.3.1. Databeskyttelsesretlige overvejelser

I MitID og NemLog-in behandles personoplysninger. Særligt for behandling af personoplysninger i forbindelse med videregivelse af risikodata og autentifikationsdata henvises til den foreslåede § 13. Desuden henvises til § 14 for behandling af data i forbindelse med validering af digitale signaturer i valideringstjenesten i NemLog-in.

Digitaliseringsstyrelsen er dataansvarlig for de personoplysninger, der behandles i MitID-løsningen og NemLog-in. Dette er en følge af, at Digitaliseringsstyrelsen i medfør af de foreslåede bestemmelser i § 3 og § 8 pålægges at stille de to infrastrukturløsninger til rådighed. Digitaliseringsstyrelsen får således ansvaret for at sikre, at løsningerne lever op til de sikkerhedskrav, der i databeskyttelseslovgivningen stilles til behandling af personoplysninger samt de øvrige forpligtelser, der efter databeskyttelsesreglerne påhviler den dataansvarlige.

7.3.1.1. Behandling af personoplysninger i MitID

For at kunne sikre, at en fysisk persons identitet registreres og valideres korrekt, er det nødvendigt at behandle personoplysninger om vedkommende. Digitaliseringsstyrelsen foretager identitetssikring af de fysiske personer, der bliver registreret i MitID-løsningen.

For så vidt angår MitID-løsningen sker anskaffelse af løsningen sammen med de danske pengeinstitutter, jf. de almindelige bemærkninger afsnit 2.2.1. Henset til, at løsningen er den danske nationale eID-løsning, der skal anmeldes til Kommissionen samt, at der med loven pålægges Digitaliseringsstyrelsen et

myndighedsansvar for løsningen, påhviler dataansvaret 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 fysisk person ønsker at få udstedt et MitID, indsamler og registrerer registreringsenhederne personoplysninger om den fysiske person. Denne indsamling sker på vegne af Digitaliseringsstyrelsen som dataansvarlig. Registreringsenheder indgår en aftale om varetagelsen af registreringsopgaven 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.

En 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 overholdelse 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. Behandling af personoplysninger, der indsamles af brokern og videregives til MitID-løsningen er særskilt reguleret i en underdatabehandleraftale.

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 om den fysiske person. Som led i sikkerheden for, at det er den rigtige fysiske person, der anvender sit MitID, indsamles desuden risikodata i MitID-løsningen. I nogle tilfælde er det af tekniske årsager brokern, der indsamler risikodata og autentifikationsdata på vegne af MitID-løsningen. I denne sammenhæng er brokern databehandler for Digitaliseringsstyrelsen.

For så vidt angår MitID-løsningen sker der behandling af personoplysninger i forbindelse med migrering fra NemID til MitID, 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.

Oplysninger om e-mailadresse og mobilnummer er ikke nødvendige for, at MitID kan udstedes, dog er mobil-nummer en forudsætning for at kunne anvende MitID App. E-mailadresse og mobilnummer er også en forudsætning for, at MitID-

løsningen hurtigt kan udsende advisering til den pågældende, 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. Personens postkasse i Digital Post kan ligeledes blive anvendt til visse typer af notifikationer.

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 MitID for at hindre misbrug.

Overgangen fra NemID til MitID kan i nogle tilfælde basere sig på den fysiske persons login med NemID. Det vil i disse tilfælde betyde, at en person, der logger ind i sin netbank med NemID, vil blive ledt igennem et flow, der fører til, at personen på baggrund af en validering med NemID bliver registreret i MitID-løsningen og får det dertil hørende MitID, som den fysiske person herefter kan anvende som identifikationsmiddel. For at sikre at disse personer på den mest smidige måde bliver oprettet korrekt i MitID-løsningen og med det nødvendige sikringsniveau, anvendes NemID-løsningen til at validere identiteten på den pågældende fysiske person.

Der indgår ikke indsamling 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 lagres ikke i MitID-løsningen. 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, jf. nedenfor. I det omfang imødegåelse af en sikkerhedsrisiko kan ske gennem indsamling af biometriske data, vil finansministeren efter forhandling med justitsministeren – og inden for databeskyttelsesforordningens rammer - kunne fastsætte regler herom med hjemmel i databeskyttelseslovens § 7, stk. 5. Det fremgår af bemærkningerne til databeskyttelsesloven, at bemyndigelsesbestemmelsen i § 7, stk. 5, er tiltænkt anvendt i situationer, hvor det kan være vanskeligt på forhånd fuldstændigt at forudse behovet for at kunne behandle personoplysninger omfattet af

forordningens 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 af hensyn til løsningens sikkerhed at indhente biometriske data både ved udstedelse af MitID og ved en brugers løbende anvendelse heraf.

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. Disse 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 hos en tjeneste. Formålet er at give broderen, der modtager risikodata, mulighed for at vurdere og afgøre om risikodataene af sikkerhedsmæssige årsager skal umuliggøre login på den pågældende tjeneste. En fysisk person kan på anmodning til den dataansvarlige få oplyst hvilke risikodata, der indsamles. Hensynet til sikkerheden i MitID-løsningen kan tilsige, at nye typer risikodata skal indsamles.

Videregivelsen af autentifikationsdata og risikodata er reguleret i denne lovs foreslåede § 13. Der henvises til de specielle bemærkninger hertil.

7.3.1.2. Behandling af personoplysninger i NemLog-in

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

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

Med udgangspunkt i specifikke serviceområder leverer NemLog-in en række services til fysiske personer 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 cpr-nummer og identifikationsnummer på den elektroniske identitet (UUID). Hvis MitID anvendes sker behandling af slutbrugerens MitID-nummer samt risikodata relateret til autentifikationssvaret. Der henvises til beskrivelse af brokeres behandling af risikodata i de almindelige bemærkninger til denne lov afsnit 7.3.1.1 ovenfor om MitID-løsningens behandling af personoplysninger samt den foreslåede § 13 og de specielle bemærkninger hertil. Det bemærkes, at NemLog-in i medfør af den foreslåede § 8, har en selvstændig behandlingshjemmel, der rækker videre end den foreslåede § 13.

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 omfattende 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, cpr-nummer, e-mailadresse, telefonnummer, virksomhedsnavn og tilknyttede rettigheder. Rettigheder omfatter både de interne systemrettigheder i erhvervsadministrationen, 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, om 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 fysisk person eller erhvervsbruger, der har fået udstedt et bestemt certifikat. Oplysningerne omfatter blandt andet navn, e-mail, cpr-nummer, og hvis certifikatet udstedes til en erhvervsbruger, oplysninger om hvilken juridisk enhed, offentlig myndighed eller offentligt retligt organ, som erhvervsbrugeren er associeret med.

Ved en fysisk person 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. Behandlingen 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, cpr-nummer 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. Det registreres ikke, hvad baggrunden for fuldmagten er.

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 som udgangspunkt indsamling af biometriske data. Dog vil hensynet til løsningens høje sikkerhed kunne medføre, at indsamling af biometriske data på et senere tidspunkt bliver relevant for at imødegå sikkerhedsmæssige trusler. Der henvises til beskrivelsen af biometriske oplysninger ovenfor i de almindelige bemærkninger om personoplysninger i MitID i afsnit 7.3.1.1.

I forbindelse med overgangen fra den eksisterende erhvervsløsning og tilknyttede tjenester hos Nets DanID til den NemLog-in løsning, som lovforslaget vedrører, sker der behandling af erhvervsbrugeres personoplysninger, herunder ved indhentning af oplysninger fra Nets DanID. Dette omfatter navn, mailadresse, stilling, virksomhedsnavn og tilknyttede rettigheder, jf. nærmere ovenfor under beskrivelse af Erhvervsadministration. 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.

8. *Hørte myndigheder og organisationer m.v.*

Udkast til lovforslaget har i perioden fra den xx. xxxx 2020 til den xx. xxxx 2020 været sendt i offentlig høring hos nedenstående myndigheder og organisationer mv.:

	Positive konsekvenser/mindre udgifter	Negative konsekvenser/merudgifter
Økonomiske konsekvenser for stat, kommuner og regioner	Der er ikke foretaget en særskilt analyse af de offentlige positive økonomiske konsekvenser af MitID og NemLog-in, da løsningerne udgør en videreførelse af den offentlige digitale infrastruktur, og ikke en omstilling fra analog sagsbehandling til primært digital selvbetjening. Der vil derfor ikke være mærkbare mindreudgifter ved overgangen fra NemID til MitID og fra det nuværende NemLog-in til næste generation NemLog-in.	De samlede projektkomkostninger til udbud og udvikling af de kommende løsninger forventes at udgøre 657,2 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.
Implementeringskonsekvenser for stat, kommuner og regioner	Ingen.	Omstillingsomkostningerne til de kommende løsninger anslås at udgøre i størrelsesordenen af 50-130 mio. kr. Det er aftalt ved økonomiforhandlingerne med kommuner og regioner, at omstillingsomkostninger, herunder både tekniske, organisatoriske og andre omstillingsomkostninger, afholdes decentralt. Omstillingsomkostningerne dækker blandt andet tilpasning af lokale it-løsninger, kompetenceudvikling af medarbejdere samt intern omstilling og udarbejdelse af nye processer. Det forventes, at antallet af klager kan stige kortvarigt i implementeringsperioden for de nye løsninger, idet private personer og erhvervsbrugere skal skifte til de nye infrastrukturløsninger. Det vurderes at disse konsekvenser vil blive reduceret efter fuld migrering, så offentlige myndigheder fremadrettet ikke får øgede administrative opgaver.
Økonomiske konsekvenser for erhvervslivet	Ingen.	Lovforslaget forventes at medføre økonomiske konsekvenser for erhvervslivet i form af gebyrer for anvendelse af serviceområderne i NemLog-in og

		<p>autentifikationstransaktioner i MitID-løsningen. Gebyrer, der opkræves fra juridiske enheder, skal dække Digitaliseringsstyrelsens omkostninger, være ikke-diskriminerende og skal sikre, at der ikke sker konkurrencefordrejning. Gebyrerne vil blive fastsat på bekendtgørelsesniveau. Se nærmere herom i lovforslagets specielle bemærkninger til § 15.</p>
Administrative konsekvenser for erhvervslivet	<p>Lovforslaget forventes årligt at medføre administrative lettelser for erhvervslivet på ca. 238 mio. kr. årligt. De årlige besparelser skyldes blandt andet nedsat tidsforbrug ved login og autentificering, en samlet tilslutning og administration samt lettere og mere fleksibel administration af erhvervsidentiteter og rettigheder i NemLog-in serviceområdet Erhvervsadministration.</p>	<p>Lovforslaget vurderes foreløbigt at medføre administrative omstillingskonsekvenser for erhvervslivet for mellem 186 og 339 mio. kr. i engangsomkostninger.</p> <p>Omstillingsomkostningerne udgøres primært af tidsforbrug ved selve migreringen til de nye løsninger samt den tid, det vil tage erhvervsbrugere at opsætte de nye løsninger samt lære dem at kende.</p>
Administrative konsekvenser for borgerne	<p>I den nye løsning reduceres risikoen for snyd med de fysiske og kopierbare nøglekort, hvilket samtidig forventes at kunne nedbringe klager. Lovforslaget indeholder et hjemmelsgrundlag, som sikrer mulighed for at fastsætte klare regler for privatpersoners retsstilling, og hvori det skal fastslås, at privatpersoner kan klage til Digitaliseringsstyrelsen over afslag på at få udstedt MitID mv. Det er hensigten, at der fastsættes regler om, at Digitaliseringsstyrelsens afgørelser kan indbringes for anden administrativ myndighed, hvilket kan anses som en forbedring for borgens administrative muligheder i forhold til NemID-løsningen.</p>	<p>Omstillingen fra NemID til MitID vil være en omstilling til en ny ID-løsning, som ikke længere indeholder det analoge identifikationsmiddel nøglekortet. Med udfasningen af det analoge identifikationsmiddel, nøglekortet, følger der en tilvænning til en ny løsning, som af nogle privatpersoner vil opleves som mere digital. Privatpersoner, som ikke har adgang til identifikationsmidlet som mobilapplikation, vil dog forsat kunne vælge fysiske identifikationsmidler som alternativ til nøglekortet til at få vist koder. Der vil dog 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.</p>
Klima- og miljømæssige konsekvenser	<p>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</p>	<p>Ingen</p>

	transport, hvilket leder til et mindre miljømæssigt aftryk og lavere udledning af drivhusgasser.	
Forholdet til EU-retten	<p>Lovforslaget indeholder ikke bestemmelser, der gennemfører ny eller ændret EU-regulering.</p> <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-standard. Dette lovforslag regulerer kun aspekter, der ikke allerede er berørt i eIDAS-forordningen og NSIS-standard.</p> <p>Lovforslaget lever op til kravene i databeskyttelsesforordningen.</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 EUF-traktaten.</p>	
Er i strid med de fem 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

Formålet med den foreslåede § 1 er at fastlægge lovens anvendelsesområde.

Det foreslås med bestemmelsens *stk. 1*, at loven finder anvendelse på de to infrastrukturløsninger MitID-løsningen og NemLog-in. Disse stilles til rådighed af Digitaliseringsstyrelsen, som det fremgår af de foreslåede bestemmelser i § 3, stk. 1, og § 8, stk. 1.

MitID-løsningen og NemLog-in er tæt forbundne, da det i forbindelse med udførelsen af myndighedsopgaver er en forudsætning for anvendelsen af MitID i offentlige digitale selvbetjeningsløsninger, der kræver sikker autentifikation, at autentifikationen går igennem NemLog-in som den fællesoffentlige broker. Når en privatperson eller en erhvervsbruger skal autentificere deres digitale identitet i en offentlig digital selvbetjeningsløsning, skal de kunne anvende deres MitID-identifikationsmiddel eller et identifikationsmiddel fra en lokal identitetsgarant tilsluttet NemLog-in. De to infrastrukturløsninger skaber således tilsammen rammen for, at privatpersoner og erhvervsbrugere har en sikker, nem og ensartet adgang til offentlige digitale selvbetjeningsløsninger. De to løsninger reguleres særskilt i lovens foreslåede afsnit II (MitID-løsningen) og III (NemLog-in).

MitID-løsningen og NemLog-in muliggør, at privatpersoner og erhvervsbrugere får adgang til autentifikation ved brug af digitale identiteter og dertilhørende elektroniske identifikationsmidler. De digitale identiteter og elektroniske identifikationsmidler, som udstedes i medfør af MitID-løsningen og NemLog-in, kan anvendes af privatpersoner og erhvervsbrugere i deres møde med offentlige digitale selvbetjeningsløsninger. Løsningerne er således centrale forudsætninger for et velfungerende, moderne og digitalt samfund, hvor myndigheder anvender selvbetjeningsløsninger til offentlig sagsbehandling.

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 elektroniske identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked. Se nærmere herom i afsnit 7.1 i den almindelige bemærkning.

Med den foreslåede *nr. 1* fastslås det, at MitID-løsningen er 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.

Privatpersoner kan anvende deres MitID (digital identitet og et eller flere elektroniske identifikationsmidler) i digitale selvbetjeningsløsninger, som kræver autentifikation af digitale identiteter. Ligeledes kan erhvervsbrugere anvende deres private MitID identifikationsmiddel eller dedikerede MitID-identifikationsmidler til erhvervsbrug i sammenhæng med deres digitale erhvervsidentitet. Der henvises til definitionerne af MitID-løsningen og MitID i den foreslåede § 2, nr. 1 og nr. 2, herunder om forskellen på MitID-løsningen og MitID.

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. Se nærmere herom bemærkningerne til § 8, stk. 2, litra b, nr. 3.

Med den foreslåede *nr. 2* fastslås det, at NemLog-in er 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. Der henvises i øvrigt til definitionen af NemLog-in i den foreslåede § 2, nr. 6.

Tilrådgivelsesstillelsen og anvendelsen af de i loven regulerede løsninger skal ses i sammenhæng med § 15 om opkrævning af vederlag og gebyrer for anvendelse af løsningerne og § 16 om regler om tilrådgivelsesstillelse og anvendelse af løsningerne for offentlige myndigheder og offentligretlige organer.

Til § 2

Med den foreslåede bestemmelse defineres de væsentlige begreber, som anvendes i loven. En del af disse definitioner er med til at afgrænse anvendelsesområdet for loven. Fx er definitionen af ”offentlig myndighed” og ”offentligretligt organ” afgørende for, om en enhed i visse situationer er forpligtet til at anvende MitID-løsningen og NemLog-in. Andre definitioner er tekniske begreber, der er nødvendige for at beskrive løsningerne.

Definitionerne i denne bestemmelse er for en dels vedkommende hel eller delvis videreførelse af definitioner fra andre retskilder. Af væsentlige retskilder er blandt andet definitionerne fra eIDAS-forordningen og udbudsloven, lov nr. 1564 af 15. december 2015 (udbudsloven). Herudover anvendes også begreber fra Vejledning til National Standard for Identiteters Sikringsniveauer (NSIS).

Med bestemmelsens *nr. 1* foreslås det, at MitID-løsningen defineres som den danske nationale elektroniske identifikationsordning, som 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.

Kerneopgaven ved forvaltningen af MitID-løsningen er varetagelse af livscyklus for MitID. I en livscyklus for MitID indgår som det første en registreringsproces, hvor en ansøger skal gøres bekendt med betingelserne for anvendelsen af det udstedte MitID, herunder de sikkerhedsforanstaltninger, der har at gøre med anvendelsen af MitID. Ansøgere skal acceptere betingelserne for at opnå MitID og udtrykkeligt tilkendegive at have læst dem. Ved ansøgningen indsamles de data, der er relevante for godtgørelse og kontrol af ansøgers identitet. Dernæst følger udstedelsen af MitID. Her udleveres og knyttes MitID til en privatperson. Når en privatperson ansøger om udstedelse af MitID, beder privatpersonen om at få tildelt en national digital identitet i MitID-løsningen. Den fastlagte proces skal sikre, at MitID udleveres til den tilsigtede ansøger. Herefter kan ansøger anvende MitID til at autentificere sig. Livscyklus for MitID dækker således over registrering, udstedelse, aktivering, anvendelse, udløb og spærring.

I løbet af en livscyklus for MitID kan der indtræffe hændelser, hvor anvendelse af MitID midlertidigt skal kunne suspenderes og/eller spærres permanent. Spærring vil ske, hvis der er mistanke om kompromittering af MitID, eller at indehaveren ikke længere har kontrol over sit MitID. Det kan fx være, hvis der bliver videregivet elektroniske identifikationsmidler til en tredjemand.

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.

MitID-løsningen afløser den hidtidige NemID-løsning, dog ikke for så vidt angår erhvervsløsningen NemID for erhverv, som i stedet afløses af erhvervsløsningen i NemLog-in, 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.

Ved overgangen fra NemID til MitID er der sket en række ændringer i den fællesoffentlige digitale infrastruktur. 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 Signatur til den digitale underskrift baseret på autentifikation med MitID.

Med bestemmelsens *nr. 2* foreslås det, at MitID anvendes som betegnelse for den nationale digitale identitet af en privatperson og tilhørende elektroniske identifikationsmidler, som kan tilknyttes privatpersoner og erhvervsbrugeres digitale identiteter. Loven regulerer ikke andre typer af elektronisk ID end MitID.

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 elektroniske identifikationsmidler, der alene eller i kombination anvendes i forbindelse med autentifikation. MitID-løsningen fungerer således som identitetsgarant for privatpersoners digitale identitet.

En digital identitet er defineret særskilt i denne bestemmelses foreslåede nr. 13. Elektroniske identifikationsmidler er defineret særskilt i denne bestemmelses foreslåede nr. 14.

Med bestemmelsens *nr. 3* foreslås det, at autentifikation defineres som en digital proces, som genkender og verificerer en digital identitet gennem anvendelse af et elektronisk identifikationsmiddel, der er koblet til identiteten. Definitionen er afstemt med definitionen af autentifikation i NSIS. Se nærmere om NSIS i afsnit 7.1.1 i de almindelige bemærkninger.

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 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.

Med bestemmelsens *nr. 4* foreslås en sontring mellem de forskellige sikringsniveauer, som anvendes for sikring af digitale identiteter. Kravene til sikringsniveauerne udspringer af NSIS-standardens og eIDAS-forordningen og er nærmere reguleret i disse. I NSIS-standardens 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 eIDAS-forordningen er det op til de enkelte medlemsstater at stille 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.

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.

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.

Med bestemmelsens *nr. 5* foreslås det, at sikker autentifikation defineres som 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.

Med bestemmelsens *nr. 6* foreslås det, at NemLog-in defineres 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.

I praksis er NemLog-in den fællesoffentlige broker for MitID og identitetsgarant for digitale erhvervsidentiteter i Danmark. NemLog-in indeholder en række serviceområder: Login og autentifikation, Digital repræsentation, Digital signering og Erhvervsadministration. Serviceområderne er nærmere beskrevet i § 8, stk. 2 og stk. 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.

Med bestemmelsens *nr. 7* foreslås det, at begrebet privatperson defineres som en fysisk person, der udelukkende agerer på vegne af sig selv, uden forbindelse til en juridisk enhed. Privatpersoner udgør i hovedreglen borgere, men er dog ikke begrænset af begrebet 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.

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 tredjemand.

Med bestemmelsens *nr. 8* foreslås det, at erhvervsbrugere defineres som fysiske personer, der er associeret med en offentlig myndighed, et offentligretligt organ eller en juridisk enhed, som er oprettet med én eller flere erhvervsidentiteter i NemLog-in. Begrebet ”associeret med” skal forstås i overensstemmelse med NSIS og eIDAS, 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.

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, i erhvervsøjemed. En erhvervsbrugers elektroniske identifikationsmiddel kan således oprettes i MitID som et dedikeret MitID, jf. princippet om dobbelt frivillighed, som nærmere beskrevet 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 den fysiske person, er erhvervsbrugers digitale identitet tilknyttet til denne i medfør af erhvervsbrugers associering med en offentlig myndighed, et offentligt organ eller en juridisk enhed.

Med bestemmelsens *nr. 9* foreslås det, at begrebet juridisk enhed defineres som en juridisk enhed med et cvr-nummer, jf. lovbekendtgørelse nr. 1052 af 16. oktober 2019 om Det Centrale Virksomhedsregister, der ikke enten er en offentlig myndighed, jf. nr. 10 eller et offentligt organ, jf. nr. 11.

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

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

Med bestemmelsens *nr. 10* foreslås det, at begrebet offentlig myndighed defineres som statslige, regionale og kommunale myndigheder.

Definitionen af offentlige myndigheder svarer indholdsmæssigt til de statslige, regionale og kommunale myndigheder, som er ordregivere, jf. udbudsloven § 24, nr. 28.

Definitionen af en offentlig myndighed i den foreslåede lov 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. 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.

Det bemærkes, at danske offentlige myndigheder, der udbyder digitale selvbetjeningsløsninger med grænseoverskridende interesse, er forpligtet til at kunne foretage grænseoverskridende autentifikation af brugere, der er i besiddelse af anmeldte eID, jf. eIDAS-forordningens artikel 6. Dette lovkrav har offentlige myndigheder i EU/EØS-regionen mulighed for at imødekomme igennem tilslutning af deres selvbetjeningsløsninger til den nationale eID-gateway, der drives af Digitaliseringsstyrelsen.

En offentlig myndighed kan i NemLog-in agere i rollen som tjenesteudbyder eller brugerorganisation. En offentlig myndighed i rollen som tjenesteudbyder er karakteriseret ved at være ansvarlig for en eller flere digitale selvbetjeningsløsninger. Når en offentlig myndighed er tilsluttet serviceområdet Erhvervsadministration i NemLog-in, betegnes den offentlige myndighed som en brugerorganisation i regi af NemLog-in.

Med bestemmelsens *nr. 11* foreslås det, at begrebet offentligretlige organer defineres som organer,

- a) der er oprettet specielt med henblik på at imødekomme almenhedens behov, dog ikke behov af industriel eller kommerciel karakter,
- b) der er juridiske personer, og
- c) som for mere end 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.

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.

Det bemærkes, at offentligretlige organer, der udbyder digitale selvbetjeningsløsninger med grænseoverskridende interesse, er forpligtet til at kunne foretage grænseoverskridende autentifikation af brugere, der er i besiddelse af anmeldte eID, jf. eIDAS-forordningens artikel 6. Dette lovkrav har offentlige myndigheder i EU/EØS-regionen mulighed for at imødekomme igennem tilslutning af deres selvbetjeningsløsninger til den nationale eID-gateway, der drives af Digitaliseringsstyrelsen.

Et offentligretligt organ kan i NemLog-in agere i rollen som tjenesteudbyder eller brugerorganisation. Et offentligretligt organ i rollen som tjenesteudbyder er karakteriseret ved at være ansvarlig for en eller flere digitale selvbetjeningsløsninger. Når et offentligretligt organ er tilsluttet serviceområdet Erhvervsadministration i NemLog-in, betegnes det offentligretlige organ som en brugerorganisation i regi af NemLog-in.

Med bestemmelsens *nr. 12* foreslås det, at en digital selvbetjeningsløsning defineres som et it-system, som kan tilgås af privatpersoner eller erhvervsbrugere med digitale identiteter 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 have en eller flere digitale selvbetjeningsløsninger tilsluttet NemLog-in. Disse digitale selvbetjeningsløsninger betegnes i denne lov som offentlige digitale selvbetjeningsløsninger. En offentlig digital selvbetjeningsløsning vil som udgangspunkt anvende serviceområdet Login og autentifikation i NemLog-in, jf. bemærkningerne til den foreslåede § 11, stk. 1, nr. 1.

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 medarbejdere i kommunen ikke være omfattet af definitionen digital selvbetjeningsløsning, idet et sådant sagsbehandlingssystem ikke vil være åbent for offentlig anvendelse af privatpersoner, fx borgere eller erhvervsbrugere. Dette gælder også, hvis fx flere kommuner i fællesskab har anskaffet og anvender et sagsbehandlingssystem.

Med bestemmelsens *nr. 13* foreslås det, at begrebet digital identitet defineres som en samling af data, der unikt identificerer en privatperson eller en erhvervsbruger. En digital identitet er det samme som en elektronisk identitet (eID), jf. e-IDAS og NSIS, og skal således forstås i overensstemmelse med definitionen i NSIS. Bestemmelsen tilsigter ikke en anden definition end definitionen af en digital identitet, som findes i Referencearkitektur for brugerstyring, som er en standard

udarbejdet i Digitaliseringsstyrelsen, som skal understøtte udviklingen af brugerstyring i den offentlige sektor.

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. I MitID-løsningen indsamles personidentifikationsdata ved anmodningen om udstedelse af MitID. Som eksempel på personidentifikationsdata kan nævnes navn og cpr-nummer. Der henvises i øvrigt til de almindelige bemærkninger i afsnit 7.3.1 om behandling af personoplysninger.

Med bestemmelsens *nr. 14* foreslås det, at begrebet elektronisk identifikationsmiddel defineres som en materiel enhed, en immateriel enhed eller en kombination af disse. 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. 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.

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 eller gennem en anden NSIS-anmeldt broker tilsluttet NemLog-in.

Ved anvendelse af flere elektroniske identifikationsmidler ved autentifikation opnås der højere sikkerhed for, at den pågældende privatperson eller erhvervsbruger har kontrol over den pågældende digitale identitet, og at denne stemmer overens med den fysiske identitet. 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.

Med bestemmelsens *nr. 15* foreslås det, at begrebet tjenesteudbyder forstås som en offentlig myndighed, et offentligretlig organ eller en juridisk enhed, der er ansvarlig for en eller flere digitale selvbetjeningsløsninger. 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 af de førnævnte serviceområder i NemLog-in i deres digitale selvbetjeningsløsninger, som minimum anvendes serviceområdet Login og autentifikation. Om brugerorganisationer se bestemmelsens nr. 16.

Med bestemmelsens *nr. 16* foreslås det, at begrebet brugerorganisation skal forstås 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 bemærkningerne til § 8, stk. 3. I modsætning til en tjenesteudbyder stiller en brugerorganisation således ikke digitale selvbetjeningsløsninger til rådighed for tredjeparter.

Til § 3

Hensigten med den foreslåede bestemmelse i *stk. 1*, er at fastslå, 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.

Tilrådhedsstillelsen af MitID-løsningen 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 en 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 tilrådighedsstillelse og anvendelse, der fremgår af § 16.

Digitaliseringsstyrelsen stiller MitID-løsningen til rådighed for juridiske enheder efter § 7.

Det foreslås med bestemmelsens *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. Herved 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.

Hvis en fysisk person er den eneste tegningsberettigede for virksomheden, kan personen anvende sit private MitID (MitID privat til erhverv) uden at oprette sin organisation som brugerorganisation i NemLog-in.

Lovforslaget pålægger ikke privatpersoner eller erhvervsbrugere at anvende løsninger og indeholder omvendt heller ikke et retskrav herom.

Når privatpersoner får udstedt MitID, tildeles denne 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.

Den omfattende digitalisering af den offentlige forvaltning har medført et stigende behov for at sikre klare juridiske rammer for borgernes rettigheder i forhold til fællesoffentlig digital infrastruktur. I denne lov sikres dette blandt andet ved tilrådighedsstillelsen af MitID for privatpersoner og erhvervsbrugere. For at få udstedt MitID skal privatpersoner og erhvervsbrugere opfylde reglerne, som fastsættes af finansministeren i medfør af § 4, stk. 2. Der henvises til bemærkningerne til § 4, stk. 2.

MitID til privatpersoner kan udstedes ved personligt fremmøde hos en registreringsenhed, der er udpeget af Digitaliseringsstyrelsen til at udstede MitID,

fx hos borgerservice eller et pengeinstitut. 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 juridisk enhed, som er oprettet i serviceområdet Erhvervsadministration i NemLog-in, betegnes som en brugerorganisation, jf. § 2, nr. 16. En brugerorganisation kan 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

Det foreslås med § 4, *stk. 1, litra a*, at Digitaliseringsstyrelsen sikrer, at der sker identitetssikring af privat personer, registrering af identiteter, udstedelse, spærring og genåbning af MitID til privatpersoner efter reglerne fastsat i medfør af bestemmelsens stk. 2.

Det sikres desuden, at erhvervsbrugere kan få udstedt et elektronisk identifikationsmiddel efter reglerne fastsat i medfør af bestemmelsens § 4, *stk. 1, litra b*. Erhvervsbrugere kan til forskel fra privatpersoner ikke få en digital identitet i MitID, da disse alene kan udstedes til privatpersoner i MitID. En erhvervsbruger kan derimod få udstedt en digital identitet i NemLog-in i serviceområdet Erhvervsadministration.

Digitaliseringsstyrelsen sikrer registrering og udstedelse af nationale digitale identiteter og elektroniske identifikationsmidler. Begrebet MitID anvendes både for den nationale digitale identitet og for elektroniske identifikationsmidler, jf. § 2, nr. 2. Ved udstedelse af MitID sker der en identitetssikring og registrering af den fysiske person, hvorefter der oprettes en digital identitet og udstedes elektroniske identifikationsmidler. Ved spærring af MitID, kan der foretages spærring af den nationale digitale identitet og af ét eller flere elektroniske identifikationsmidler. En spærring kan således ske helt eller delvist. En privatperson som har fået udstedt MitID, kan således vælge at spærre enten den nationale digitale identitet eller det dertilhørende 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 fuldkommen. 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.

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. Nærmere regler om registreringen vil blive fastsat med hjemmel i § 4, stk. 2. 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-standard.

Når MitID udstedes til en privatperson jf. § 4, stk. 1, litra a, vil der ske en tildeling af en national digital identitet til privatpersonen, og derudover vil den privatpersonen blive tildelt et elektronisk identifikationsmiddel, som overdrages på sikker vis til den pågældende. Et elektronisk identifikationsmiddel er fx kodeviser eller MitID App. For at en privatperson eller en erhvervsbruger kan gøre brug af den digitale identitet, skal denne således være i besiddelse af et elektronisk identifikationsmiddel, som er knyttet til den digitale identitet. Et elektronisk identifikationsmiddel er en materiel enhed, en immateriel enhed eller en kombination af disse, jf. lovens § 2, nr. 14.

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.

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 privat MitID-identifikationsmiddel forudsætter, at både den fysiske person, der er associeret med en juridisk enhed og den juridiske enhed accepterer, at den fysiske person anvender sit private MitID-identifikationsmiddel. Dette forhold kaldes det dobbelte frivillighedsprincip.

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

Med den foreslåede *stk. 2* fastsættes en hjemmel til, at finansministeren fastsætter regler om forvaltningen af MitID-løsningen og MitID, herunder regler om udstedelse, spærring, genåbning af MitID og regler for indbringelse af klage over en afgørelse om udstedelse 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.

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 udpeges i medfør af § 5, stk. 1.

Der vil 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 identitet 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, 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.

Reglerne vil i et vist omfang videreføre de regler, som gælder for privatpersoner i bekendtgørelse nr. 899 af 21. juni 2018 om udstedelse og spærring af NemID med offentlig digital signatur, dog tilpasset de nye krav til sikkerhed fra NSIS-standard.

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 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, at hemmeligholdelse og beskyttelse af det elektroniske identifikationsmiddel, 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. Se mere herom nedenfor. Det forventes, at det bliver fastsat, at den fysiske person kan få udstedt MitID ved personligt fremmøde hos en registreringsenhed i et pengeinstitut eller hos en registreringsenhed i kommunernes borgerservicecentre.

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. Bestemmelsen medfører ikke, at en privatperson har et retskrav på at få MitID. Hvis fx en privatperson ikke kan bekræfte sin identitet, vil det have den konsekvens, at personen ikke kan få udstedt MitID.

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 udgør en forvaltningsretlig afgørelse. Det er nødvendigt at fastsætte nærmere regler om spærring af MitID, da en spærring foretaget af andre end indehaveren selv, tillige udgør en forvaltningsretlig afgørelse. Når der træffes en forvaltningsretlig afgørelse om spærring og afslag på udstedelse, 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 fysiske 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 myndighed digitalt. Det er op til den enkelte myndighed at beslutte, hvordan de vil understøtte en privatperson, som ikke kan betjene sig digitalt. De enkelte myndigheder vil i den sammenhæng være forpligtet til at vejlede borgere efter de forvaltningsretlige regler, hvilket blandt andet indebærer, at en myndighed har pligt til at vejlede og hjælpe borgere inden for de ressortområder, som de er ansvarlige for. Således har en myndighed pligt til at hjælpe en borger, der fx ikke kan få udstedt MitID til at agere inden for myndighedens område og give borgeren adgang til de oplysninger og den offentlige service, som andre borgere kan tilgå ved brug af MitID.

Det er formålet med den foreslåede bestemmelse i stk. 2, at finansministeren bemyndiges til at fastsætte nærmere regler for, hvornår og hvordan MitID kan spærres. Ved en spærring kan MitID suspenderes, således at det er midlertidigt spærret. 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 den udpegede 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, hvis 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. 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 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 § 5, stk. 1, er udpeget til at på vegne af Digitaliseringsstyrelsen at varetage opgaver med blandt andet forvaltningen af MitID samt opgaver i medfør af § 4, stk. 1.

Den foreslåede stk. 2 rummer ligeledes en bemyndigelse til, at finansministeren skal fastsætte nærmere regler om adgangen til at klage over en afgørelse om afslag på udstedelse af MitID, spærring af MitID og genåbning af MitID. Det er hensigten, at en afgørelse om afslag på udstedelse af MitID, spærring af MitID, efter genvurdering hos registreringsenheden, skal kunne indbringes for Digitaliseringsstyrelsen, men at de nærmere regler om klagehåndtering udmøntes i en bekendtgørelse med hjemmel i bestemmelsens stk. 2. Endelig indeholder stk. 2 en hjemmel til at fastsætte nærmere regler om registrering af identiteter ved udstedelse af MitID og om forvaltning af MitID.

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 hensynet til, at privatpersoner og erhvervsbrugere kan få et gennemsigtigt og samlet overblik over de regler, som retter sig mod dem.

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

Til § 5

I medfør af den foreslåede bestemmelse kan Digitaliseringsstyrelsen udpege offentlige myndigheder, offentligretlige organer eller juridiske enheder til på vegne af Digitaliseringsstyrelsen at varetage opgaven med udvikling, drift, vedligeholdelse og forvaltning af MitID-løsningen samt opgaver i medfør af § 4, stk. 1. Enhver sådan udpegning skal ske under overholdelse af udbudsreglerne.

Digitaliseringsstyrelsen og FR1 af 16. september 2015, partnerselskab under bankernes interesseorganisation Finans Danmark. (FR 1) har i 2019 indgået en kontrakt med Nets DanID A/S, om udvikling, drift, vedligeholdelse og forvaltning af MitID-løsningen. Kontrakten løber i 10 år fra idriftsættelsen af løsningen med mulighed for forlængelse. Kontraktindgåelsen er sket på baggrund af EU-udbud, jf. udbudsbekendtgørelse nr. 2017/S 244-509896.

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.

Det følger af den foreslåede bestemmelses *stk. 2*, at kommunale borgerservicecentre skal varetage opgaver i henhold til § 4, stk. 1. Det er hensigten med den foreslåede bestemmelse, at kommunale borgerservicecentre bliver registreringsenheder i medfør af bestemmelsen. Kommunale borgerservicecentre er i dag ikke forpligtet til at håndtere udstedelse og spærring af NemID, selvom de kommunale borgerservicecentre allerede i dag varetager opgaven. Når de kommunale borgerservicecentre fremadrettet forpligtes til at varetage opgaverne med registrering af identiteter, udstedelse, spærring og genåbning af MitID til privatpersoner, sker dette med henblik på at sikre, at det fortsat er let og nemt tilgængeligt for borgere at få hjælp til oprettelsen af MitID. Derudover sikres det, at de kommunale borgerservicecentre kan træffe afgørelser om udstedelse og spærring af MitID, idet de forpligtes til at håndtere denne opgave. De kommunale borgerservicecentre skal ved varetagelsen af opgaverne i henhold til § 4, stk. 1 følge de almindelige forvaltningsretlige regler, som relaterer sig til de pågældende opgaver, herunder skal borgerne tilbydes vejledning, jf. vejledningspligten i forvaltningslovens § 7, stk. 1. Bestemmelsen er således udtryk for den offentlige organisering af opgaven.

Til § 6

Med den foreslåede bestemmelse i § 6, stk. 1 pålægges offentlige myndigheder og offentligretlige organer at sikre, at privatpersoner og erhvervsbrugere kan anvende MitID til at få adgang til de pågældende myndigheders digitale selvbetjeningsløsninger, hvis løsningerne vedrører myndighedsopgaver og kræver sikker autentifikation. Det fremgår af bestemmelsen, at MitID-løsningen i disse tilfælde skal anskaffes fra Digitaliseringsstyrelsen. Anskaffelsen af MitID-løsningen vil i praksis foregå igennem tilslutning til NemLog-in, som den fællesoffentlige broker. Hvis ikke der foretages tilslutning til NemLog-in, vil det i stedet være muligt for offentlige myndigheder og offentlige retlige organer, at anskaffe MitID-løsningen ved at anvende en NSIS-anmeldt broker, som er tilsluttet til NemLog-in eller en lokal identitetsgarant tilsluttet NemLog-in.

Når de offentlige myndigheder og offentlige retlige organer ikke udfører en myndighedsopgave eller når deres digitale selvbetjeningsløsninger ikke kræver sikker autentifikation, har disse i stedet en ret til at anvende MitID-løsningen. Det følger af bestemmelsens foreslåede stk. 2. Det fremgår af bestemmelsen, at MitID-løsningen i disse tilfælde kan anskaffes fra Digitaliseringsstyrelsen. I dette tilfælde skal MitID-løsningen anskaffes gennem en broker, som er certificeret af Digitaliseringsstyrelsen. Betingelserne for anskaffelsen fremgår af § 15, stk. 3 og § 16.

Med anvendelse af MitID forstås, at en privatperson eller en erhvervsbruger ved brug af deres digitale identitet anvender deres elektroniske identifikationsmiddel til

at autentificere sig, så vedkommende kan opnå adgang til den offentlige myndigheds eller det offentligretlige organs digitale selvbetjeningsløsning. Erhvervsbrugere kan alene anvende MitID i den fællesoffentlige infrastruktur, hvis de er tildelt en erhvervsidentitet, jf. § 8, stk. 3.

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.

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, skal anskaffe MitID-løsningen fra Digitaliseringsstyrelsen i medfør af loven.

I de tilfælde hvor offentlige myndigheder og offentligretlige organer forpligtes til at anvende MitID-løsningen, jf. § 6, stk. 1 fra Digitaliseringsstyrelsen, sker det 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 2.3.

Med den foreslåede bestemmelse i *stk.* 2, sikres det, at offentlige myndigheder og offentligretlige organer kan anvende MitID-løsningen, når de ikke udfører en myndighedsopgave, eller når deres digitale selvbetjeningsløsning kræver autentifikation på sikringsniveau lav.

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. 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 bestemmelsen gives en ret til at offentlige myndigheder og offentligretlige organer kan anvende MitID-løsningen uden at gennemføre et selvstændigt udbud, såfremt løsningen anskaffes fra Digitaliseringsstyrelsen gennem NemLog-in som broker.

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

Med den foreslåede § 7 får juridiske enheder en lovbestemt ret til at anvende MitID-løsningen som tjenesteudbydere uafhængigt af hvilket sikringsniveau, deres digitale selvbetjeningsløsning kræver. 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 indgå aftale med 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 MitID-broker eller der kan indgås aftale med en hvilken som helst anden broker, som er certificeret af Digitaliseringsstyrelsen, til at være MitID-broker. Den juridiske enhed skal således igennem en brokeraftale acceptere de aftalevilkår, som er fastsat af Digitaliseringsstyrelsen overfor brokieren, for at kunne anvende MitID-løsningen. Det skal understreges, at retten til at anvende MitID-løsningen skal læses i sammenhæng med den foreslåede § 15, stk. 2 om opkrævning af gebyr og vederlag. Det indebærer, at juridiske enheder skal betale for at anvende MitID-løsningen, selvom de har en lovbestemt ret til at anvende den. Bestemmelsen indeholder ikke et retskrav.

Til § 8

Med den foreslåede bestemmelse i *stk. 1* fastslås, at Digitaliseringsstyrelsen pålægges myndighedsopgaven at stille NemLog-in til rådighed for offentlige myndigheder, offentligretlige organer og juridiske enheder, samt at sikre udvikling, drift, vedligeholdelse og forvaltning af løsningen. I Digitaliseringsstyrelsens opgave med at sikre drift og forvaltning, indgår ligeledes en sikring af, at der sker drift og forvaltning af 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 tilslutningen til serviceområderne. Dele af supportopgaverne er vederlagsbelagte, jf. § 15, stk. 2.

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 *stk. 2* fastlægges det, 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.

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 autentifikationen i den fællesoffentlige infrastruktur af digitale identiteter for privatpersoner sker i MitID-løsningen gennem NemLog-in. Erhvervsbrugerne 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. 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.

Med bestemmelsens *nr. 2* foreslås det, at Digital repræsentation udgør et serviceområde i NemLog-in. Digital repræsentation i NemLog-in finder primært anvendelse for privatpersoner, som kan lade sig repræsentere digitalt af en tredjepart, der enten kan optræde som en anden privatperson eller en erhvervsbruger. Derudover finder serviceområdet Digital repræsentation anvendelse på erhvervsområdet, hvor en tegningsberettigede fra en juridisk enhed kan anvende serviceområdet. Det er alene tegningsberettigede, 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.

Digital repræsentation kan alene anvendes i digitale selvbetjeningsløsninger, hvor en offentlig myndighed eller et offentligretligt organ udfører myndighedsopgaver, og 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 borger eller en tegningsberettiget erhvervsbruger, som ønsker at lade sig repræsentere på ét eller flere myndighedsområder.

Den digitale repræsentationsløsning 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 borger 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 borgernes 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 borger ønsker repræsentation på flere myndighedsområder. Endvidere understøtter den digitale repræsentationsløsning, at værger i nogle tilfælde får mulighed for at agere på baggrund af et værgemål i de digitale selvbetjeningsløsninger og på tværs af myndighedsområder.

Med den foreslåede bestemmelse i *litra a* kan en privatperson 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. Det er også muligt for en privatperson at anmode en anden privatperson om at repræsentere sig gennem Digital repræsentation i NemLog-in. I forvaltningsretlig forstand kan digital repræsentation understøtte partsrepræsentation, som fastsat i forvaltningslovens § 8. 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. Det vil således også være muligt at administrere forhold som læseadgang til Digital Post. Derudover 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 tjenesteudbyderes 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.

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 dette af borgerservice eller tjenesteudbyderne 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.

Den foreslåede bestemmelse i *litra b* skal muliggøre at anvende Digital repræsentation i erhvervsøjemed af en juridisk enhed.

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.

Med bestemmelsens *nr. 3* foreslås det, at digital signering udgør et serviceområde i NemLog-in. I serviceområdet 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, 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.

Tjenesteudbydere kan udstille digital signering af dokumenter i deres digitale selvbetjeningsløsninger tilsluttet NemLog-in, hvorefter private brugere og erhvervsbrugere som led i anvendelsen af den digitale selvbetjeningsløsning kan signere dokumenter hos Tjenesteudbyderen.

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

I den eksisterende løsning er det 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 udelukkende kunne ske ved brug af serviceområdet Digital Signering i NemLog-in, jf. den foreslåede § 8, stk. 2, nr. 3 idet MitID som et dedikeret eID ikke indeholder de signaturgenereringsdata, der er nødvendige for at afgive signaturer.

Det betyder, at i eksisterende 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 eksisterende lovgivning foreskrives anvendelse af NemID, OCES eller digital signatur eller digital signatur med et sikkerhedsniveau svarende til OCES eller højere med henblik på at afgive en underskrift kan det ikke forventes at være opfyldt alene ved anvendelse af

autentifikation med MitID, idet underskrift i den fremtidige infrastruktur kræver anvendelse af serviceområdet digital signatur.

I bestemmelsens foreslåede *litra a* fastsættes, at tjenesteudbydere kan udstille digital signering af dokumenter i digitale selvbetjeningsløsninger gennem NemLog-in.

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.

Certificeringscenteret forestår ligeledes udstedelse af OCES-certifikater og kvalificerede certifikater, der kan udstedes til brugerorganisationer i serviceområdet Erhvervsadministrationen, jf. bemærkningerne til § 8, stk. 3.

I bestemmelsens *litra b* foreslås, at privatpersoner og erhvervsbrugere ved digital signering kan afgive en digital signatur. Serviceområdet Digital signering giver således mulighed for at afgive en digital signatur med samme retsvirkning som en fysisk underskrift. Der henvises i øvrig til eIDAS-forordningens artikel 25. Afgivelsen af en digital signatur vil ske på baggrund af sikker autentifikation.

Digital signering sker i praksis ved at underskriver omfattende både privatpersoner og erhvervsbrugere autentificerer sig ved anvendelsen af sin digitale identitet og elektronisk identifikationsmiddel. På den baggrund er det muligt at identificere afgiveren af den digital signatur. Signeringen sikrer ligeledes det digitale dokumentets integritet, idet det ved efterfølgende verifikation af signaturen vil fremgå, om dokumentet er blevet ændret.

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 digital 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 foreslåede § 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 den foreslåede *stk. 3* foreslås det, at Erhvervsadministration udgør et serviceområde i NemLog-in, som brugerorganisationer, jf. § 2, nr. 16, kan tilslutte sig, såfremt de overholder reglerne om identitetssikring ved oprettelse som brugerorganisation, som nærmere fastsat i medfør af § 9, stk. 2.

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. For at serviceområdet i *litra a* kan anvendes, kræver det, at en offentlig myndighed eller juridiske enheder, oprettes som brugerorganisation i NemLog-in. Det er et krav, at en brugerorganisation overholder tekniske 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. Det er erhvervsbrugeren og brugerorganisationen som vælger identifikationsmidlet.

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.

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 erhvervsbrugerens private MitID-identifikationsmiddel kan benyttes til autentifikation af erhvervsbrugerens 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 (fx 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 § 4, stk. 1. Det påhviler brugerorganisationen at overholde det dobbelte frivillighedsprincip.

Endvidere er det muligt i Erhvervsadministration at sammenkoble lokale erhvervsidentiteter og elektroniske identifikationsmidler til digitale erhvervsidentiteter i erhvervsløsningen i NemLog-in. For sammenkobling af lokale identiteter og 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 udstiller endvidere et erhvervs-API, hvorigennem andre brokere har mulighed for at foretage opslag og validering af en erhvervsbruger oprettet i Erhvervsadministration i NemLog-in. Dette giver mulighed for, at erhvervsbrugeren kan anvende sin erhvervsidentitet ved login til en digital selvbetjeningsløsning gennem en anden broker. Anvendelse af NemLog-in's erhvervs-API fordrer, at den anden broker indgår aftale med NemLog-in herom.

Det foreslås endvidere, at det i bestemmelsens *litra b* fastsættes, at offentlige myndigheder, offentligretlige organer og juridiske enheder i rollen som brugerorganisation kan tildele og administrere rettigheder til erhvervsidentiteter ved login og autentifikation til digitale selvbetjeningsløsninger tilsluttet NemLog-in. Det 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 erhvervsbrugerens erhvervsidentitet. Der er grundlæggende to former for 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 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”.

Digitaliseringsstyrelsen varetager således gennem NemLog-in 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

Det foreslås med § 9, at Digitaliseringsstyrelsen sikrer, at der sker identitetssikring af offentlige myndigheder, offentligretlige organer og juridiske enheder, når de oprettes som brugerorganisationer i serviceområdet Erhvervsadministration i NemLog-in, og at erhvervsbrugerens digitale identiteter kan spærres efter reglerne fastsat i medfør af bestemmelsens stk. 2.

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 Erhvervsadministration sker der registrering af, hvordan denne har identificeret sig og efter identitetssikringen 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 offentlig retlige 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. 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. Der henvises til den foreslåede § 3, stk. 1 for en uddybning af tilrådgivelsesstillelsen af MitID til erhvervsbrugere og til den foreslåede § 4, stk. 1 om forvaltningen og udstedelsen af MitID.

Endvidere er det Digitaliseringsstyrelsens opgave at sikre, at brugerorganisationers adgang til Erhvervsadministrationen 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. 2.

Med den foreslåede *stk. 2* fastsættes 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 Erhvervsadministrationen 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 Erhvervsadministration. 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 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 Erhvervsadministration. Derudover vil reglerne indeholde de betingelser, der løbende skal opfyldes for at være brugerorganisation i Erhvervsadministration og regler for udpegelse af administratorer for den offentlige myndighed, det offentlige organ eller den juridiske enhed.

Reglerne vil i et vist omfang videreføre de regler, som gælder for medarbejdere og administratorer i bekendtgørelse nr. 899 af 21. juni 2018 om udstedelse og spærring af NemID med offentlig digital signatur, dog tilpasset de nye krav til sikkerhed fra NSIS-standard og nye tekniske tilføjelser i serviceområdet Erhvervsadministration.

Regler om forvaltning af NemLog-in fastsættes af hensyn til løsningens og erhvervsbrugernes sikkerhed, samt brugerorganisationens 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 rettighedsstyringen heraf 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. Bestemmelsen medfører ikke at en medarbejder eller andre personer associeret med brugerorganisation har et retskrav på at få en digital identitet. En juridisk enhed der er oprettet som brugerorganisation i Erhvervsadministration beslutter selv hvilke medarbejdere, der skal oprettes som erhvervsbrugere.

Når der træffes en forvaltningsretlig afgørelse om spærring af en brugerorganisation eller en erhvervsbruger, skal der gives mulighed for at indgive

en klage over afgørelsen, ligesom forvaltningslovens regler om afgørelsesvirksomhed skal iagttages. 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 Digital Post 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

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 213-442780. 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

Med den foreslåede § 11 fastsættes de nærmere regler for offentlige myndigheders og offentligretlige organers anvendelse af de enkelte serviceområder i NemLog-in, jf. § 8, stk. 2 og 3. Formålet med § 11 er at skabe pligter og rettigheder for offentlige myndigheder og offentligretlige organer, som anvender en digital selvbetjeningsløsning til at udføre en myndighedsopgave, så der sikres samme høje grad af tillid og sikkerhed på tværs af de offentlige digitale selvbetjeningsløsninger.

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.

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.

Bestemmelsens *stk. 1* forpligter offentlige myndigheder og offentligretlige organer til som tjenesteudbydere at anvende serviceområderne, som nævnt i nr. 1 og nr. 2.

Med den foreslåede *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. 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.

Det foreslås med bestemmelsens *nr. 2*, 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. Pligten gælder, når offentlige myndigheder og offentligretlige organer i deres digitale selvbetjeningsløsninger tilbyder, at en part kan lade sig repræsentere eller bistå af andre. Pligten gælder alene for offentlige myndigheder og offentligretlige organer i rollen som tjenesteudbydere.

Serviceområdet Digital repræsentation gør det muligt for en privatperson at anvende digital repræsentation i digitale selvbetjeningsløsninger på tværs af myndighedsområder i én samlet offentlig digital løsning. Løsningen understøtter, at privatpersoners retskrav på repræsentation kan imødekommes, når en privatperson agerer i mødet med det offentlige på digitale selvbetjeningsløsninger.

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.

Serviceområdet Digital repræsentation understøtter muligheden for at digitalisere partsrepræsentation i medfør af forvaltningslovens § 8. Derudover kan Digital repræsentation i nogle tilfælde anvendes af privatpersoner, som repræsenteres ved værgemål eller på anden måde repræsenteres. Serviceområdet omfatter ikke repræsentation i privatretlige anliggender, og privatpersoner og juriske enheder kan derfor ikke agere i rollen som tjenesteudbydere i dette serviceområde.

Offentlige myndigheder og offentligretlige organer skal stille Digital repræsentation til rådighed, hvis deres digitale selvbetjeningsløsninger tilbyder, at en privatperson kan lade sig repræsentere i et givent tilfælde, 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 privatpersoner og erhvervsbrugere adgang til at anvende serviceområdet Digital repræsentation, såfremt der udføres en myndighedsopgave og er behov for repræsentation i digitale selvbetjeningsløsninger.

Myndigheder kan således vælge at tilbyde funktionalitet ved repræsentationsløsninger, som ligger ud over de funktioner, som er indeholdt i serviceområdet Digital repræsentation. Serviceområdet Digital repræsentation kan derfor betragtes som en basisløsning for offentlig Digital repræsentation. Digital repræsentation kan kun anvendes af offentlige myndigheder og offentligretlige organer.

Med bestemmelsens foreslåede *stk. 2* skabes der en ret i loven for offentlige myndigheder og offentligretlige organer i rollen som tjenesteudbydere, til at anvende serviceområderne i bestemmelsens nr. 1 og nr. 2.

Den foreslåede *nr. 1* giver 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. 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 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 Digital signering. 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.

Med retten til at anvende serviceområdet Digital signering understøttes offentlige myndigheder og offentligretlige organer i at tilbyde privatpersoner og erhvervsbrugere en sagsbehandling og procedure, som fuldt ud kan digitaliseres. Med offentlige myndigheders og offentligretlige organers anvendelse af 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.

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.

Med den foreslåede *stk. 4* præciseres det, at serviceområderne skal eller kan anskaffes fra Digitaliseringsstyrelsen. Betingelserne for anskaffelsen fremgår af § 16 og § 15, stk. 3.

Til § 12

Med den foreslåede § 12 får juridiske enheder en lovbestemt ret til at anvende serviceområder i § 8, stk. 2, nr. 1 og 2 samt stk. 3. Det er således frivilligt for de juridiske enheder, om de vil anvende serviceområderne Login og autentifikation, Digital signering og Erhvervsadministration.

For at anvende serviceområderne i § 8, stk. 2 nr. 1 og 2 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 af Digitaliseringsstyrelsen for at kunne anvende de nævnte serviceområder i NemLog-in. 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 indebærer, at juridiske enheder skal betale for at anvende MitID-løsningen, selvom de har en lovbestemt ret til at anvende den. Bestemmelsen indeholder ikke et retskrav.

Til § 13

Med den foreslåede bestemmelse indføres hjemmel til, at Digitaliseringsstyrelsen kan videregive autentifikationssvar og 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 7.3.1.

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.

Den hjemmel, der indføres til videregivelse af persondata fra Digitaliseringsstyrelsen, indebærer, at en broker kan modtage og behandle risikodata til vurdering af risikoen ved hver enkelt konkret transaktion. Formålet er, at give broderen, der modtager risikodata, mulighed for at vurdere og afgøre om risikodata af sikkerhedsmæssige årsager skal umuliggøre login på den pågældende tjeneste. Ved modtagelsen af data bliver broderen dataansvarlig herfor.

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 risikodata vil det herunder blive fastsat, at broderen alene kan anvende risikodata som anført i den foreslåede bestemmelse, og at enhver behandling herudover kræver, at broderen har en selvstændig hjemmel hertil og over for Digitaliseringsstyrelsen har dokumenteret denne hjemmel.

Med den foreslåede *stk. 2* 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 således 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 denne bestemmelses *stk. 1*.

Broderen foretager ikke vurderinger og træffer ikke 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.

Med den foreslåede *stk. 3* sikres hjemmel til, at en broker kan videregive autentifikationssvar til en tjenesteudbyder, der har indgået en aftale med den pågældende broker om at modtage autentifikationssvar. 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.

Med den foreslåede *stk. 4* kan Digitaliseringsstyrelsen videregive autentifikationssvar til en offentlig myndighed, et offentligretligt 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 7.3.1.2.

Tilslutningen 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.

I medfør af den foreslåede *stk. 5* 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.

Til § 14

Med den foreslåede bestemmelse indføres hjemmel til, at Digitaliseringsstyrelsen kan behandle persondata, jf. databeskyttelsesforordningen artikel 9, stk. 1, i forbindelse med validering af en digital signatur i Digitaliseringsstyrelsens valideringstjeneste under serviceområdet Digital Signering.

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 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 verifikationen 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/hash-værdi, der blev genereret på underskriftstidspunktet, og som er koblet til den digitale signatur.

Valideringstjenesten har i overensstemmelse med dens formål ingen kontrol med indhold og karakteren af de data, der behandles i forbindelse med valideringen. Der kan således potentielt behandles alle former for persondata, herunder følsomme persondata omfattet af persondataforordningens artikel 9.

Til § 15

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, offentligretlige organer, juridiske enheder og privatpersoner.

Det foreslås med bestemmelsens stk. 1, at finansministeren kan fastsætte regler om opkrævning af gebyr hos privatpersoner for registrering og udstedelse af MitID. Bestemmelsen vil ikke kunne anvendes til at fastsætte regler om gebyr for selve registreringen af et MitID. Det er hensigten, at der alene skal fastsættes regler om privatpersoners betaling af gebyr for 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 elektroniske identifikationsmidler, hvorefter der skal betales gebyr for yderligere identifikationsmidler. Det er i den forbindelse hensigten, at MitID-appen kan anvendes som elektronisk identifikationsmiddel uden brugerbetaling.

MitID identifikationsmidler er som udgangspunkt målrettet understøttelse af sikringsniveau ”betydelig”. Det kan bestemmes, at der skal opkræves vederlag for særlige MitID identifikationsmidler til brug for understøttelse af sikringsniveau ”høj”.

Det foreslås med bestemmelsens *stk. 2*, at Digitaliseringsstyrelsen indgår 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 Digitaliseringsstyrelsens omkostninger, være ikke-diskriminerende og skal sikre, at der ikke sker konkurrencefordrejning.

Det foreslås med bestemmelsens *stk. 3*, at når offentlige myndigheder og offentligretlige organer benytter MitID-løsningen og NemLog-in, betaler de gennem fællesoffentlig finansiering og 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-underskudsforhold. 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. 3, er fastlagt af finansministeren. Digitaliseringsstyrelsen kan således ikke forhandle om vederlaget.

Til § 16

Det foreslås med bestemmelsen, at finansministeren fastsætter regler om, hvordan Digitaliseringsstyrelsen skal stille MitID-løsningen og NemLog-in til rådighed for offentlige myndigheder og offentligretlige organer jf. §§ 3 og 8, og om disses tilslutning til og anvendelse af MitID-løsningen og NemLog-in.

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

Det foreslås med bestemmelsens stk. 1, at Digitaliseringsstyrelsen kan meddele offentlige myndigheder og offentligretlige organer påbud med henblik på 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, nr. 1 og 2.

Formålet med nærværende påbudsbestemmelse er, at offentlige myndigheder og offentligretlige organer skal leve op til de forpligtelser, som fastsættes for dem i loven. Bestemmelsen giver således Digitaliseringsstyrelsen mulighed for at udstede påbud og derved tydeliggøre over for offentlige myndigheder og offentligretlige organer, som ikke lever op til de forpligtelser, der følger af loven, at de har pligt hertil.

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

Med bestemmelsens stk. 2 foreslås det, at finansministeren kan fastsætte nærmere regler om meddelelse af påbud. Hermed vil finansministeren fx kunne udstede regler om, at Digitaliseringsstyrelsen vil kunne udstede påbud vedrørende andre dele af MitID og NemLog-in.

Til § 18

Det foreslås med bestemmelsen, at Digitaliseringsstyrelsen påser overholdelse af regler fastsat i medfør af § 4, stk. 2, og § 9, stk. 2.

Bestemmelsen har til formål at fastsætte hvilke dele af loven, der reguleres af Digitaliseringsstyrelsens tilsyn i medfør af bestemmelsen.

Med den foreslåede *stk. 1* udpeges Digitaliseringsstyrelsen til at føre tilsyn med MitID-løsningen. Tilsynet af MitID-løsningen vil rette sig mod de offentlige myndigheder, offentligretlige organer og juridiske enheder, som Digitaliseringsstyrelsen vil udpege efter den foreslåede § 5, stk. 1. Finansministeren vil fastsætte nærmere regler om tilsyn for MitID-løsningen, jf. stk. 2.

MitID-løsningen skal anmeldes til 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 dækker således både behovet efter denne lov samt kravene i medfør af eIDAS-forordningen.

Digitaliseringsstyrelsen udpeges også i den foreslåede stk. 1 til at føre tilsyn med NemLog-in. Tilsynet med NemLog-in vil rette sig mod de offentlige myndigheder, offentligretlige organer og juridiske enheder, som Digitaliseringsstyrelsen vil udpege efter den foreslåede § 10. Finansministeren vil fastsætte nærmere regler om tilsyn for NemLog-in, jf. stk. 2.

Det sker efter samme metode som for MitID, dog med den undtagelse, at 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 om supplerende bestemmelser til forordning om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked (lov nr. 617 af 8. juni 2016) blev Digitaliseringsstyrelsen udpeget til det nationale tilsynsorgan i Danmark.

Digitaliseringsstyrelsen bliver systemejer og tilsynsførende for MitID-løsningen og NemLog-in. Der er ledelsesmæssig og organisatorisk adskillelse i Digitaliseringsstyrelsen, således at tilsyn og forvaltningen af de to løsninger bliver udført uafhængigt forskellige steder i styrelsen med forskellig ledelsesmæssig reference.

Med den foreslåede *stk. 2* bemyndiges finansministeren til at fastsætte nærmere regler om udøvelsen og indholdet af tilsynet, herunder at fastsætte nærmere bestemmelser om Digitaliseringsstyrelsens samarbejde med andre tilsynsmyndigheder og efter aftale med vedkommende minister.

Til § 19

Det foreslås med § 19, at der indføres en særlig tavshedspligt, der medfører, at offentlige myndigheder, offentligretlige organer og privatpersoner, der udøver tilsyn med MitID og NemLog-in, samt enhver der i øvrigt yder bistand til tilsynet, iagttager ubetinget tavshed over for uvedkommende med hensyn til oplysninger om MitID's og NemLog-in's systemers tekniske- og sikkerhedsmæssige indretning samt processer for opretholdelse, vedligeholdelse og drift af sikkerheden i systemerne. Bestemmelsen regulerer tavshedspligten for privatpersoner, der udøver tilsyn med MitID og NemLog-in, jf. § 18.

Det er afgørende, at tilsynet får indsigt i alle oplysninger, der fremkommer i forbindelse med tilsynet om fx risiko- og sikkerhedsvurderinger, herunder eventuelle sårbarheder. Disse oplysninger kan indikere svagheder i både systemer, systeminstallationer samt de sikkerhedsmæssige processer, som kan betyde, at tilsynet vil kræve forbedring af systemer, ændrede sikkerhedsmæssige processer eller lignende. Det er derfor afgørende, at disse oplysninger kan indberettes i fortrolighed 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.

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

Til § 20

Med den foreslåede *stk. 1* fastslås det, at forvaltningsloven og almindelige forvaltningsretlige principper finder anvendelse på afgørelser om udstedelse, spærring og genåbning af MitID, jf. § 4 stk. 2, som træffes af de juridiske enheder, der kan udpeges i medfør af § 5, stk. 1.

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.

Det medfører blandt andet, at afgørelser om udstedelse, spærring og genåbning af MitID, som opfylder afgørelsesbegrebet efter forvaltningslovens § 19, skal ledsages af en begrundelse og en klagevejledning, at reglerne om partshøring skal iagttages, og at borgere og erhvervsbrugere skal vejledes tilstrækkeligt om deres rettigheder mv. 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.

Med *stk. 2* foreslås det, at forvaltningsloven og almindelige forvaltningsretlige principper finder anvendelse på afgørelser om identitetssikring af juridiske enheder, spærring af brugerorganisationers adgang til Erhvervsadministrationen 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 Erhvervsadministrationen 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

Bestemmelsen fastslår, at Digitaliseringsstyrelsen er erstatningsansvarlig over for privatpersoner, offentlig myndigheder, offentligretlige organer eller juridiske enheder, som følge af fejl i forbindelse med registrering, udstedelse og forvaltningen af MitID. Der er tale om et ansvar med omvendt bevisbyrde, hvilket betyder, 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.

eIDAS-forordningen bestemmer i art. 10, nr. 1, at en medlemsstat, der anmelder en eID-løsning til 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. Det findes rimeligt, at erstatningsansvaret dækker fejl i registrering og indrullering, uafhængigt af om MitID bruges i en grænseoverskridende eller national kontekst.

Ved den indgåede kontrakt med Nets DanID A/S om udvikling m.v. af MitID-løsningen er det fastsat, at leverandøren bærer det i den foreslåede bestemmelse nævnte erstatningsansvar. Der er herunder fastsat, at leverandøren tillige 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 nededid 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. Det medfører for eksempel, at manglende adgang til netbank må håndteres af det pågældende pengeinstitut. På samme måde må en offentlig selvbetjeningsløsning eller øvrige selvbetjeningsløsninger håndtere manglende adgang. Eksempler på hvorledes dette konkret er håndteret 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.

Såfremt manglende adgang til en selvbetjeningsløsning skyldes driftsforstyrrelser i MitID-løsningen, 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

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 delegationen kun vedrører dele af beføjelserne.

Med bestemmelsen følger også, at de kompetencer og opgaver, som Digitaliseringsstyrelsen 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

Den foreslåede § 23 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 FR1 af 16. september 2015 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 FR1. Hjemlen til det nuværende partnerskab mellem Digitaliseringsstyrelsen og FR1, fremgår af tekstanmærkning nr. 120 ad § 07.12.02 på finansloven for finansåret 2020 og er en videreførelse fra tidligere finansår.

Både MitID-løsningen og NemLog-in er tilvejebragt gennem EU-udbud, som nærmere beskrevet i de almindelige bemærkninger afsnit 2.2.1 og 2.2.2. Det er også hensigten, at fremtidige løsninger vil skulle tilvejebringes gennem EU-udbud.

Til § 24

Det foreslås med bestemmelsens *stk. 1*, at finansministeren fastsætter tidspunktet for lovens ikrafttræden, herunder at forskellige dele af loven kan træde i kraft på forskellige tidspunkter.

Begrundelsen for at henlægge ikrafttrædelsen til fastsættelse i bekendtgørelse er hensynet til, at eventuelle justeringer i tidsplanerne for de to løsninger ikke skal medføre en lovændring.

Det er forventningen, at MitID-løsningen og NemLog-in er klar til idriftsættelse i andet kvartal 2021.

Det foreslås med *stk. 2*, at lov xx ændres, således at følgende ...

Formålet med dette er at få en ensartet og opdateret terminologi vedrørende MitID og NemLog-in i gældende lovgivning. I det tilfælde, hvor der i dag i eksisterende lovgivning 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 eksisterende lovgivning foreskrives anvendelse af NemID, OCES eller digital signatur eller digital signatur med et sikkerhedsniveau svarende til OCES eller højere med henblik på at afgive en underskrift kan det ikke forventes at være opfyldt alene ved anvendelse af autentifikation med MitID, idet underskrift i den fremtidige infrastruktur kræver anvendelse af serviceområdet digital signatur.

Til § 25

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

For Grønland er der tale om et sagsområde, der ikke er hjemtaget, hvorfor loven ikke skal gælde for Grønland, men loven vil helt eller delvist kunne sættes i kraft i Grønland ved kongelig anordning.

For Færøerne er der tale om et sagsområde, der ikke hører til fællesanliggender, som varetages af rigsmyndighederne. Sagsområdet anses derfor som overgået til Færøerne, hvorfor loven ikke skal gælde på Færøerne.

Den hidtidige aftalebaserede tilgang for udstedelse af NemID med offentlig digital signatur til privatpersoner (NemID) i Grønland og på Færøerne vil fortsat være gældende.