

Høringsnotat

Forslag til endringer i forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

**Digitale fellesløsninger forvaltet av
Digitaliseringsdirektoratet**

Sendt ut: 1. september 2026

Høringsfrist: 10.oktober 2026

1 Innhold

1. Høringsnotatets hovedinnhold.....	4
2. Bakgrunnen for forslaget.....	4
3. Om fellesløsningene forvaltet av Digitaliseringsdirektoratet.....	5
3.1 Fellesløsningene som del av et digitalt økosystem	5
3.2 ID-Porten.....	5
3.3 MinID	6
3.4 Ansattporten.....	6
3.5 Kontakt- og reservasjonsregisteret	7
3.6 Digital postkasse til innbyggere	7
3.7 Maskinporten.....	7
3.8 eFormidling	7
3.9 eSignering	8
3.10 Elektronisk mottakeradresseregister (ELMA)	8
3.11 Altinn studio	8
3.12 Altinn autorisasjon	9
3.13 Altinn varsling.....	9
3.14 Altinn melding.....	9
3.15 Altinn formidling.....	9
3.16 Data.altinn.no	9
3.17 Dialogporten.....	9
3.18 Altinn arbeidsflate.....	10
3.19 Informasjonsportalen i Altinn	10
3.20 Norge.no	10
3.21 Designsystemet.....	10
3.22 Data.norge.no	10
3.23 Virksomheter som kan bruke fellesløsninger forvaltet av Digitaliseringsdirektoratet	11
4. Gjeldende rett	13
4.1. Personopplysningsloven og personvernforordningen	13
4.2. Forholdet til Grunnloven § 102 og EMK artikkel 8.....	14
4.3. Forvaltningsloven	15

4.4. Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)	15
4.5. Digitaliseringsrundskrivet.....	15
5. Departementets vurdering og forslag	16
5.1. Lovtekniske vurderinger – regulering i eForvaltningsforskriften	16
5.2. Supplerende rettsgrunnlag	16
5.2.2. Særlig om behandling av personopplysninger etter personvernforordningen artikkel 9 og 10	18
6. Forslagets personvernkonsekvenser	20
7. Økonomiske og administrative konsekvenser	21
8. Merknader til enkelte bestemmelser	22
9. Forslag til forskrift om endringer i forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften).....	24

1. Høringsnotatets hovedinnhold

I dette høringsnotatet foreslår Digitaliserings- og forvaltningsdepartementet endringer i forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften).

Formålet med bestemmelsene som foreslås, er å tydeliggjøre Digitaliseringsdirektoratets ansvar for å drifte, forvalte eller på annen måte stille til rådighet de digitale fellesløsningene, samt å sikre et klart behandlingsgrunnlag for Digitaliseringsdirektoratets behandling av personopplysninger. I tillegg skal bestemmelsene sikre at skoler har behandlingsgrunnlag for å utlevere personopplysninger til Digitaliseringsdirektoratet i forbindelse med utstedelse av MinID.

2. Bakgrunnen for forslaget

Digitaliseringsdirektoratet skal være regjeringens fremste virkemiddel for raskere og mer samordnet digitalisering av samfunnet, og skal bidra til å utvikle og gjennomføre regjeringens IKT-politikk. Blant direktoratets hovedoppgaver er strategisk planlegging og videreutvikling av en helhetlig digital infrastruktur for offentlig sektor, utvikling av brukervennlige digitale tjenester for innbyggere, kommuner og næringsliv, samt drift og forvaltning av digitale felleskomponenter og -løsninger.

Digitaliseringsdirektoratet drifter, forvalter og stiller til rådighet digitale fellesløsninger. Disse løsningene fungerer som byggeklosser i et felles økosystem for nasjonal tjenesteutvikling og samhandling. De gjør det enklere for offentlige virksomheter å utvikle gode og brukervennlige tjenester, og bidrar samtidig til at innbyggere og næringslivet lettere kan ta dem i bruk. Eksempler på slike løsninger er ID-porten, Kontakt- og reservasjonsregisteret, elnnsyn og Altinn.

Fellesløsningene spiller en viktig rolle i myndighetenes kommunikasjon med befolkningen og må derfor være både sikre og stabile, særlig i krisesituasjoner. Fellesløsningene er kritisk nasjonal infrastruktur med sikkerhets- og beredskapsmessig betydning. Regjeringens arbeid knyttet til digitalt handlingsrom og sikkerhetsdimensjonen ved fellesløsningene er sentralt for regjeringen.

I de fellesløsningene der Digitaliseringsdirektoratet behandler personopplysninger, baserer direktoratet i dag behandlingen på flere rettslige grunnlag. Når direktoratet opptrer som behandlingsansvarlig benyttes ulike behandlingsgrunnlag i personvernforordningen artikkel 6 nr. 1, herunder bokstav a, b og e. Når direktoratet opptrer som databehandler, reguleres behandlingen gjennom databehandleravtaler.

Departementet vurderer at dagens rettslige rammer for Digitaliseringsdirektoratets behandling av personopplysninger fremstår som fragmentert, og at det er behov for en tydeligere og mer helhetlig regulering, særlig i lys av økt omfang og kompleksitet i fellesløsningene. Departementet forslår derfor å innta bestemmelser i eForvaltningsforskriften som klargjør Digitaliseringsdirektoratets oppgaver, og som samtidig gir et mer oversiktlig og samlet behandlingsgrunnlag for direktoratets behandling av personopplysninger i den forbindelse.

Forslaget skal videre legge til rette for nye, mer brukervennlige og lettere tilgjengelige utstedelsesmetoder for MinID i skolen, noe som vil gjøre det enklere for ungdom å få MinID.

MinID er en elektronisk ID som kan brukes til å logge inn på en rekke offentlige tjenester. Høsten 2024 gjennomførte Digitaliseringsdirektoratet en pilot med utstedelse av MinID i skolen sammen med utvalgte skoler og ca. 500 elever. Hensikten med piloten var å øke tilgjengeligheten til eID og forenkle utstedelsesprosessen, blant annet i forbindelse med søknad til videregående opplæring. MinID utstedes normalt ved at innbygger selv initierer prosessen ved å bestille et aktiveringsbrev, som sendes til folkeregistrert adresse. Deretter må innbyggeren registrere MinID enten på MinID.no eller i MinID-appen, ved å bruke aktiveringskoden i aktiveringsbrevet. MinID i skolen gjør det mulig for elever å få MinID gjennom skolen, uten behov for aktiveringsbrev.

I piloten bidro lærere i utstedelsesprosessen ved å utlevere elevenes personopplysninger til Digitaliseringsdirektoratet, og deretter sørge for at rett elev mottok sin aktiveringskode. Piloten var svært vellykket og bekreftet forventningene om at ordningen gjør det enklere både for lærere og elever, og kan bidra til at flere får tilgang til offentlige digitale tjenester, samtidig som sikkerheten ivaretas. Departementet ønsker derfor å videreføre ordningen.

Piloten avdekket imidlertid et behov for tydeligere behandlingsgrunnlag som gir skolene adgang til å utlevere personopplysninger til Digitaliseringsdirektoratet for å igangsette utstedelse av MinID. Departementet ønsker å gjøre ordningen permanent og foreslår derfor bestemmelser som sikrer et tilstrekkelig behandlingsgrunnlag for slik utlevering. Forslaget legger derfor til rette for at skolene kan dele nødvendige personopplysninger med Digitaliseringsdirektoratet i forbindelse med utstedelse av MinID.

3. Om fellesløsningene forvaltet av Digitaliseringsdirektoratet

3.1 Fellesløsningene som del av et digitalt økosystem

I felles digitalt økosystem samarbeider offentlige og private virksomheter om å bygge helhetlige og sammenhengende tjenester. I økosystemet kan de samhandle, gjenbruke fellesløsninger samt følge standarder, prinsipper og referansearkitekturer. På denne måten blir digitaliseringen mer bærekraftig. Fellesløsninger som ID-porten og Altinn, nasjonale fellesregistre som Folkeregisteret og Enhetsregisteret, samt sektorspesifikke løsninger som den kommunale FIKS-plattformen og Feide, er viktige for å kunne etablere digital samhandlingsevne og levere sammenhengende offentlige tjenester.

Nedenfor omtales fellesløsninger som leveres, driftes og forvaltes av Digitaliseringsdirektoratet.

3.2 ID-Porten

ID-porten er en innloggingsportal hvor innbyggere kan bruke sin foretrukne eID for å logge seg på offentlige løsninger. ID-porten er utviklet, driftes og forvaltes av Digitaliseringsdirektoratet. I tillegg opptreer direktoratet som innkjøpssentral gjennom ID-

porten ved å inngå avtaler med leverandører av eID på vegne av hele offentlig sektor. Per i dag er BankID, Buypass, Commfides og MinID tilgjengelige autentiseringsmetoder i ID-porten. I tillegg finnes funksjonalitet for å opptre som verge basert på oppslag i folkeregisteret.

Det er også mulig å bruke ID-porten til å logge inn med enkelte andre lands eIDer, som er meldt til EU-kommisjonen og fagfellevurdert til å ivareta kravene til eID-ordninger. Denne løsningen er laget for å understøtte Norges plikt til gjensidig anerkjennelse av eID-ordninger etter artikkel 6 i europaparlaments- og rådsforordning (EU) 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (eIDAS 1), som er gjort til norsk rett gjennom lov om elektroniske tillitstjenester av 15. juni 2018 nr. 44. Denneplikten videreføres med eIDAS 2 som ikke er innført i norsk rett.

Målgruppen for ID-porten er offentlige virksomheter og private virksomheter som utfører tjenester på vegne av det offentlige. 1979 virksomheter har per 1. januar 2026 tatt i bruk ID-porten og i 2025 ble det gjennomført i overkant av 331 millioner innlogginger med ID-porten.

3.3 MinID

MinID er en eID-ordning som oppfyller kravene til sikkerhetsnivå betydelig i henhold til selvdeklarasjonsforskriften. Ordningen er én av fire tilgjengelige autentiseringsmetoder i ID-porten.

MinID er en eID-løsning for innbyggere som enten ikke ønsker eller ikke har mulighet til å skaffe seg eID på høyere sikkerhetsnivå. Autentisering kan gjennomføres via mobilapp, engangskoder sendt på SMS, eller ved bruk av tidsbegrensede engangskoder (TOTP).

Målgruppen for MinID er innbyggere som har behov for en eID på sikkerhetsnivå betydelig for innlogging til offentlige tjenester. Sammenlignet med eID-er på høyere nivå er MinID mer tilgjengelig.

MinID er tilgjengelig for alle som tar i bruk ID-porten. Det er tjenesteeier selv som vurderer behovet for eID på nivå betydelig eller høyt. I løpet av 2025 ble det gjennomført over 8 millioner innlogginger med MinID.

3.4 Ansattporten

Ansattporten er en fellesløsning som løser behovet for autentisering og autorisering av ansatte, både interne og eksterne, hos offentlige virksomheter. Den er en frittstående teknisk løsning med et annet design enn ID-porten, men med et utgangspunkt som er teknisk likt som ID-porten og bruker de samme eIDene i tillegg til EntraID.

Ansattporten er et relativt ferskt produkt som har hatt sitt pilotprosjekt i 2023 og 2024. Målgruppen for Ansattporten er offentlige virksomheter og private virksomheter som utfører tjenester på vegne av det offentlige. Fra 2025 er pilotperioden over og Ansattporten har gått over i ordinær drift.

3.5 Kontakt- og reservasjonsregisteret

Kontakt- og reservasjonsregisteret (KRR) er en fellesløsning som fungerer som et nasjonalt grunndataregister for opplysninger om innbyggers digitale kontaktinformasjon og reservasjonsstatus. Det skal benyttes ved varsling om digital sending av vedtak og andre viktige meldinger, og til å sjekke reservasjonsstatus for innbyggerne. Registeret kan benyttes til andre formål innenfor virksomhetenes offentlige tjenesteyting.

Målgruppen for Kontakt- og reservasjonsregisteret er offentlige virksomheter og private virksomheter som utfører tjenester på vegne av det offentlige. Bruk av KRR er pålagt i forskrift, jf. eForvaltningsforskriften § 8. 904 virksomheter har per 1. januar 2026 tatt i bruk Kontakt- og reservasjonsregisteret og det ble i 2025 gjort over 2790 millioner oppslag med registeret.

3.6 Digital postkasse til innbyggere

Digital postkasse til innbyggere (DPI) tilbyr offentlige virksomheter en måte å sende post digitalt til innbyggere. For å motta post velger den enkelte innbygger selv en digital postkasse fra leverandører som har avtale med Digitaliseringsdirektoratet. Tjenesten omfatter en meldingsformidlertjeneste, to ulike digitale postkasser innbygger kan velge mellom og en tjeneste for utskrift og forsendelse av post på papir. Enkelttjenestene i DPI er anskaffet i markedet av eksterne tredjepartsleverandører på vegne av offentlige virksomheter. Avtalene forvaltes av Digitaliseringsdirektoratet. Direktoratet fungerer med det som en innkjøpssentral for tjenesten.

Offentlige virksomheter og private virksomheter som utfører tjenester på vegne av det offentlige er gjennom digitaliseringsrundskrivet punkt 1.10 pålagt å bruke DPI. 1045 virksomheter har per 1.1.2026 tatt i bruk DPI og per 1.9.2026 har 3 806 270 innbyggere en digital postkasse.

3.7 Maskinporten

Maskinporten er en fellesløsning som tilbyr tilgangsstyring for virksomheter som utveksler data gjennom maskin-til-maskin-kommunikasjon.

Løsningen sørger for sikker autentisering og tilgangskontroll for datautveksling mellom virksomheter. Der utvekslingen av data krever det, kan Maskinporten kombineres med autentisering av person gjennom ID-porten.

Målgruppen for Maskinporten er offentlige virksomheter og private virksomheter som utfører tjenester på vegne av det offentlige. 59 virksomheter har per 1.1.2026 tatt i bruk Maskinporten som tilbydere av data, og 49 115 virksomheter er konsumenter av data i Maskinporten per 30.7.26.

3.8 eFormidling

eFormidling er en fellestjeneste som bidrar til en mer sikker, samordnet og effektiv meldingsutveksling. Dette gjør det mulig å kommunisere på en enkel måte, uten å måtte ta hensyn til om mottakeren er en privat virksomhet, offentlig virksomhet eller innbygger. Fellesløsningen inneholder en teknisk løsning kalt integrasjonspunktet som den enkelte

virksomhet installerer lokalt tilknyttet sak/arkiv- eller fagsystem, samt vedlikehold av standarder og knytninger til autoritative kilder.

Målgruppen for eFormidling er offentlige virksomheter og private virksomheter som utfører tjenester på vegne av det offentlige. 204 virksomheter hadde per 1.1.2026 tatt i bruk eFormidling og det ble i 2025 totalt sendt over 10,6 millioner forsendelser i løsningen.

3.9 eSignering

eSignering er en fellesløsning som tilbyr digitale signeringstjenester for offentlige virksomheter. eSignering gjør det mulig for innbyggere å signere dokumenter fra det offentlige digitalt ved bruk av elektronisk personsignatur. Pålogging og signering i eSignering skjer ved bruk av ønsket eID i ID-porten. Fellesløsningen er anskaffet i markedet av ekstern tredjepartsleverandør på vegne av offentlige virksomheter. Digitaliseringsdirektoratet fungerer som en innkjøpssentral for tjenesten.

Målgruppen for eSignering er offentlige virksomheter eller private virksomheter som utfører tjenester på vegne av det offentlige. 775 virksomheter hadde per 1.1.2026 tatt i bruk eSignering og det ble i 2025 gjennomført over 2,72 millioner signeringer.

3.10 Elektronisk mottakeradresseregister (ELMA)

Elektronisk mottakeradresseregister (ELMA) er en fellesløsning som fungerer som et av flere norske registre over foretak som tar imot ulike typer digitale forsendelser i samsvar med internasjonale og nasjonale Peppolstandarder, som for eksempel EHF og eGovernment.

Bruk av ELMA er omtalt i digitaliseringsrundskrivet punkt 1.13. Bruk av EHF i anskaffelser er pålagt gjennom forskrift om elektronisk faktura i anskaffelser. Pliktsubjektene er offentlige og private virksomheter som både mottakere og avsendere av dokumentformat som benytter ELMA som register. I Prop. 44 L (2025–2026) Endringer i bokføringsloven og enkelte andre lover på finansmarkedsområdet (pliktig digital bokføring og e-fakturering mv.) er det lagt til grunn at bruken av ELMA er såpass utbredt at det ikke er behov for vesentlig overgangsordning. 140 aksesspunkt har per 1.1.2026 tatt i bruk ELMA som adresseregister for sine kunder(mottakere). Det er per 1.1.2026 registrert 343 989 mottakere i ELMA og det ble i 2025 sendt over 264 millioner forsendelser ved bruk av ELMA.

3.11 Altinn studio

Altinn Studio er en selvbetjent plattform der virksomheter i offentlig sektor kan utvikle, drifte og forvalte digitale dialoger og tjenester med både grafisk brukergrensesnitt og API-er for maskin-til-maskin integrasjon.

Altinn Studio inneholder sikre og separate kjøretidsmiljø for den enkelte tjenesteeier, verktøy for datamodellering, hendelser for å støtte sammenhengende tjenester, arbeidsflyt og enkel konfigurering av autorisasjon. Tjenestene som utvikles kan enkelt tilgjengeliggjøres i Dialogporten for å gi en samlet oversikt til sluttbrukerne.

3.12 Altinn autorisasjon

Altinn Autorisasjon er en nasjonal fullmaktsløsning for virksomheter og personer. Produktet gir mulighet for å styre hvem som skal (kunne) gjøre hva og når med hvilke data i det offentlige, og i samspillet mellom offentlig og privat. Altinn autorisasjon tilbyr funksjonalitet for tilgangsstyring og -kontroll for digitale tjenester både på Altinn-plattformen og andre plattformer.

Komponenten har fem hovedegenskaper:

- Autorisasjonsregler
- Fullmakt/Tilgangsstyring
- Samtykke
- Tilgangskontroll
- Autoritative kilder

3.13 Altinn varsling

Altinn varsling er en tjeneste som tjenesteeiere kan benytte til å sende varsel til virksomheter og personer via kanaler som SMS og e-post. Produktet støtter krav til varsel i henhold til eForvaltningsforskriften § 8, herunder gjentatt varsling etter § 8 femte ledd. Produktet benytter data fra Enhetsregisteret og Kontakt- og reservasjonsregisteret for å rute varsel korrekt. Varsling på SMS og epost driftes, forvaltes og videreutvikles av Digitaliseringsdirektoratet. Selve SMS-utsendelsen leveres av SMS-leverandør.

3.14 Altinn melding

Altinn melding muliggjør sending og lagring av sikker digital post og vedlegg fra offentlig sektor til virksomheter og innbyggere.

3.15 Altinn formidling

Produktet Altinn formidling muliggjør en-til-flere, en-til-en og mange-til-mange overføringer av store datamengder på en trygg og effektiv måte. Det kan sees på som et grensesnitt for utveksling av store datamengder mellom etater eller fra næringsliv til etat og omvendt. Innholdet kan forbli kryptert hele veien med garantert levering og sporbarhet for transport av data.

3.16 Data.altinn.no

Data.altinn.no er en løsning for datadeling fra datatilbydere i offentlig sektor til offentlige eller private aktører. Gjennom et enkelt og generisk API kan ulike datasett utveksles på en måte som sikrer konfidensialitet, integritet og tilgjengelighet, uten mellomlagring.

3.17 Dialogporten

Dialogporten gir virksomheter i offentlig sektor mulighet til å sammenstille og tilgjengeliggjøre digitale dialoger, tjenester, data og post på tvers av virksomheter og tekniske plattformer. Dialogporten tillater plattformuavhengig tilgang til dialoger og muliggjør samordnet bruk av andre nasjonale fellesløsninger. Dialogporten etableres som nytt produkt, og er en forutsetning for moderniseringsarbeidet i Skatteetaten. Dialogporten gjør det mulig for sluttbrukeren å få presentert oversiktlig informasjon fra offentlige virksomheter uavhengig av om sluttbrukeren er innlogget i Altinn eller hos den enkelte virksomhet.

3.18 Altinn arbeidsflate

Altinn arbeidsflate erstatter dagens innboks og profil i Altinn-løsningen. Arbeidsflate er brukergrensesnittet hvor sluttbrukere finner sine dialoger med ulike offentlige virksomheter samlet i en felles flate. Både som privatperson og i kraft av å ha en rolle i en organisasjon, vil sluttbrukeren ha tilgang til egne påbegynte dialoger, innsendte skjema og mottatte meldinger, uavhengig om de er opprettet gjennom Altinn eller andre løsninger. Produktet muliggjør at meldinger knyttet til én sak vises i en sammenheng, for å gjøre det mer oversiktlig for sluttbrukeren. Arbeidsflaten legger også til rette for at ulike roller i en virksomhet lettere kan samarbeide om å utføre ulike handlinger på dialoger/meldinger. Produktet vil utvikle seg videre for å møte sluttbrukernes behov.

3.19 Informasjonsportalen i Altinn

Informasjonsportalen i Altinn (info.altinn.no) inneholder oversikt over offentlige digitale tjenester for virksomheter og innbyggere. Her finnes oversikt over skjema og tjenester til bruk ved søknader og rapportering til offentlig sektor.

Informasjonsportalen inneholder også informasjon for gründere og små og mellomstore bedrifter under "Starte og drive bedrift". Der finnes det også oversikt over statlige støtteordninger til næringslivet. Videre er informasjonsportalen nasjonalt kontaktpunkt i henhold til EUs tjenstedirektiv og yrkeskvalifikasjonsdirektiv. All informasjon i informasjonsportalen er tilgjengelig uten innlogging.

3.20 Norge.no

Norge.no er en fellesløsning som fungerer som en inngangsport som viser vei til ulike offentlige tjenester på nett. De digitale tjenestene er delt inn i aktuelle livssituasjoner. Det er definert åtte slike livssituasjoner så langt. De digitale tjenestene er tilgjengelige via søk og en temameny. Norge.no gir også informasjon om hvordan man kan kommunisere på nett med det offentlige, velge digital postkasse og oppdatere KRR-informasjon.

3.21 Designsystemet

Designsystemet er en verktøykasse med grunnleggende UI-komponenter og interaksjonsmønstre for å lage brukervennlige digitale tjenester på tvers av nivåer og virksomheter i offentlig sektor. Det kan brukes av designere og utviklere i statlig, kommunal, privat sektor og frivillige organisasjoner. Designsystemet er godkjent som et «Digital public goods» og er tilgjengelig for bruk også utenfor Norge. Designsystemet videreutvikles kontinuerlig for å holdes relevant i takt med endrede behov og teknologisk utvikling, blant annet innen kunstig intelligens (KI). Systemet forvaltes og videreutvikles av Digitaliseringsdirektoratet i samarbeid med flere andre offentlige virksomheter.

3.22 Data.norge.no

Data.norge.no gir en oversikt over hvilke data offentlig sektor har og kan dele. Katalogen tilrettelegger for å gi datakonsumenter enklere tilgang til denne typen data. Katalogen fremmer også rettferdige konkurransevilkår ved å muliggjøre viderebruk av data for både kommersielle og ikke-kommersielle formål.

Data.norge.no gir en omfattende oversikt over datasett, begreper, API-er, informasjonsmodeller, tjenester og hendelser i offentlig sektor, inkludert beskyttede data. Her får man hjelp til å oppdage, vurdere og ta i bruk data, med tydelig informasjon om blant annet datatilbydere, tilgjengelighet og datakvalitet. Man kan finne informasjon om dataene er åpne eller om tilgangen til dataene er begrenset. Man kan også finne informasjon om hvordan dataene er relatert til hverandre, og hva de betyr.

Innholdet på Data.norge.no leveres av virksomhetene selv. Det er hver enkelt virksomhet som er ansvarlig for forvaltningen av sitt innhold i katalogene.

Registreringsløsningen som den enkelte offentlige virksomhet benytter for registrering og tilgjengeliggjøring av ovennevnte opplysninger, behandler personopplysninger i forbindelse med innlogging av virksomhetens ansatte, samt opplysninger om hvem som har registrert eller endret opplysninger til hvilket tidspunkt.

3.23 Virksomheter som kan bruke fellesløsninger forvaltet av Digitaliseringsdirektoratet

Hvilke virksomheter som kan benytte seg av fellesløsninger forvaltet av Digitaliseringsdirektoratet, følger blant annet av anskaffelser som ligger til grunn løsningene, eForvaltningsforskriften og ulike statsstøtterettslige og anskaffelsesrettslige problemstillinger. Det er Digitaliseringsdirektoratet som avgjør om en virksomhet kan benytte fellesløsningene.

I dag kan offentlige virksomheter og virksomheter som utfører oppgaver på vegne av, og som helt eller delvis er finansiert av, det offentlige benytte seg av fellesløsningene forvaltet av direktoratet. Dette omfatter blant annet alle sentrale og lokale statlige organer, herunder tilsyn, ombud og direktorater, alle fylkeskommuner, kommuner og kommunale etater, samt offentlig eide selskaper som bare leverer tjenester til det offentlige (egenregi). I tillegg omfattes private virksomheter som treffer vedtak etter forvaltningsloven, og private virksomheter som yter tjenester etter avtale med og på vegne av det offentlige, men da begrenset til den delen av virksomheten som omfattes av forvaltningsloven eller utføres på vegne av det offentlige.

Fellesløsningene skal også være mulig å knytte til andre virksomheter eller utøvere av aktiviteter, som ikke faller direkte inn under avgrensningene ovenfor, men som likevel må anses som offentlig virksomhet. Offentlig virksomhet må i denne sammenheng avgrenses mot virksomhet som anses som ervervsvirksomhet i henhold til konkurranse- og statsstøttereguleringen. Relevante momenter i denne vurderingen vil blant annet være om virksomheten faller inn under forvaltningslovens og/eller offentlighetslovens virkeområde, om de aktuelle tjenester utøves i allmennhetens interesse, om tjenestene tilbys i konkurranse med private aktører, om det offentlige helt eller delvis finansierer tjenestene, og om det tas betalt for tjenestene fra sluttbrukerne utover det som er nødvendig for dekning av utøverens kostnader.

Statsaksjeselskaper og offentlig eide virksomheter som helt eller delvis driver i konkurranse med private virksomheter, kan ikke benytte fellesløsningene, med mindre de treffer vedtak etter forvaltningsloven eller utfører oppgaver på vegne av, og helt eller delvis er finansiert av

det offentlige, men da begrenset til den delen av virksomheten som omfattes av forvaltningsloven eller utføres på vegne av det offentlige.

4. Gjeldende rett

4.1. Personopplysningsloven og personvernforordningen

Lov 15. juni 2018 nr. 38 (personopplysningsloven), som gjennomfører europaparlaments- og rådsforordning (EU) 2016/679 (personvernforordningen) i norsk rett, har som formål å ivareta den enkeltes personvern og legge til rette for harmoniserte regler i EU/EØS for å sikre fri flyt av personopplysninger. Forordningens saklige virkeområde er avgrenset til helt eller delvis automatisert behandling av personopplysninger, samt ikke-automatisert behandling av personopplysning som inngår i eller skal inngå i et register, jf. personvernforordningen artikkel 2 nr. 1. En personopplysning er enhver opplysning om en identifisert eller identifiserbar fysisk person, jf. personvernforordningen artikkel 4 nr. 1. Begrepet «behandling» er vidt definert i artikkel 4 nr. 2, og omfatter enhver operasjon eller en rekke operasjoner som utføres med personopplysninger, enten automatisert eller ikke.

Behandling av personopplysninger forutsetter i henhold til personvernforordningen artikkel 5 at behandlingen er lovlig, rettferdig og åpen, at det foreligger et spesifikt, uttrykkelig angitt og berettiget formål, og at prinsippene om dataminimering, riktighet, lagringsbegrensning, integritet, konfidensialitet og ansvarlighet overholdes.

Reglene om behandlingsgrunnlag følger av personvernforordningen artikkel 6. Behandling av personopplysninger er bare lovlig dersom og i den grad minst ett av behandlingsgrunnlagene i artikkel 6 nr. 1 bokstav a til f er oppfylt, hvorav bokstav e er det mest aktuelle i forbindelse med dette høringsnotatet.

Etter personvernforordningen artikkel 6 nr. 1 bokstav e kan den behandlingsansvarlige behandle personopplysninger dersom «behandlingen er nødvendig for å utføre en oppgave i allmenhetens interesse». Begrepet «nødvendig» innebærer at det ikke er tilstrekkelig at personopplysningene kan være nyttige. De må enten alene eller sett i sammenheng med andre personopplysninger ha avgjørende betydning for ivaretagelse av den eller de aktuelle interessene.

Det følger videre av personvernforordningen artikkel 6 nr. 3 bokstav a og b at «grunnlaget for behandlingen» som nevnt i artikkel 6 nr. 1 bokstav c og e «skal fastsettes» i unionsretten eller i medlemsstatenes nasjonale rett. Dette innebærer at bokstav c eller e ikke alene kan utgjøre et behandlingsgrunnlag, men at den behandlingsansvarlige i tillegg må kunne vise til et supplerende rettsgrunnlag for behandlingen.

I Prop. 56 LS (2017–2018) punkt 6.3.2, redegjøres det for hva et slikt supplerende rettsgrunnlag kan være, og hvilke krav som stilles til det. For så vidt gjelder hva som kan utgjøre supplerende rettsgrunnlag uttales det at «[e]tter departementets syn må det legges til grunn at i alle fall lov- og forskriftsbestemmelser kan utgjøre supplerende rettsgrunnlag. Departementet antar at også vedtak fattet i medhold av lov eller forskrift omfattes, ettersom det også i disse tilfellene foreligger et lov- eller forskriftsgrunnlag.» Når det gjelder andre krav til det supplerende rettsgrunnlaget uttales det at ordlyden i artikkel 6 nr. 3 samlet sett taler for at det må påvises et supplerende rettsgrunnlag i unionsretten eller nasjonal rett, men at det

ikke er nødvendig at det supplerende rettsgrunnlaget uttrykkelig regulerer behandling av personopplysninger. For nærmere omtale henvises det Prop. 56 LS (2017–2018).

Videre følger det av personvernforordningen artikkel 9 nr. 1 at behandling av særlige kategorier av personopplysninger i utgangspunktet er forbudt. Særlige kategorier av personopplysninger omfatter personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering. For at behandling av personopplysninger som omfattes av forbudet skal være lovlig, må vilkårene i et av unntakene i artikkel 9 nr. 2 bokstav a til j være oppfylt.

4.2. Forholdet til Grunnloven § 102 og EMK artikkel 8

Grunnloven § 102 lyder:

«Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller.

Statens myndigheter skal sikre et vern om den personlige integritet.»

Grunnloven § 102 gir ikke anvisning på noen adgang til eller vilkår for å gjøre inngrep i rettigheten. Høyesterett har imidlertid lagt til grunn at det kan gjøres inngrep i retten etter Grunnloven § 102 dersom tiltaket har en tilstrekkelig hjemmel, forfølger et legitimt formål og er forholdsmessig, se Rt. 2014 side 1105 avsnitt 28 og Rt. 2015 side 93 avsnitt 60.

Grunnloven § 102 har klare likhetstrekk med EMK artikkel 8, og må tolkes i lys av denne. Ved siden av Grunnloven § 102 må også legalitetsprinsippet, jf. Grunnloven § 113, tas i betraktning. Det følger av Grunnloven § 113 at «[m]yndighetenes inngrep overfor den enkelte må ha grunnlag i lov».

EMD har i sin praksis lagt til grunn at offentlige myndigheters lagring av personopplysninger som knytter seg til privatlivet i bestemmelsens forstand, utgjør et inngrep i retten etter EMK artikkel 8 nr. 1, se Amann mot Sveits 16.2.2000 avsnitt 65 og S. og Marper mot Storbritannia 4.12.2008 avsnitt 67. Begrepet «privatliv» skal i henhold til EMDs praksis tolkes vidt, se S. og Marper mot Storbritannia avsnitt 66 til 67 med videre henvisninger.

Inngrep i retten etter EMK artikkel 8 nr. 1 må kunne rettferdiggjøres etter artikkel 8 nr. 2, som krever at inngrepet må ha tilstrekkelig hjemmel, ha et legitimt formål og være forholdsmessig. Hva som er tilstrekkelig rettsgrunnlag for inngrep, beror på en konkret vurdering, blant annet av hvor inngripende behandlingen er. For nærmere omtale, se Prop. 56 LS (2017–2018).

Dette høringsnotatets forslag til bestemmelser i eForvaltningsforskriften vil utgjøre rettsgrunnlaget og tilstrekkelig hjemmel for å rettferdiggjøre eventuell inngripen etter EMK og Grunnloven.

4.3. Forvaltningsloven

Lov 10. februar 1967 om behandlingsmåten i forvaltningssaker er én av flere sektorovergripende lover som regulerer virksomheten til offentlige organer. Loven gjelder som et utgangspunkt for all virksomhet som drives av forvaltningsorganer.

Forvaltningsloven § 15 a tredje ledd ble innført ved lov 21. desember 2001 nr. 117, jf. Ot.prp.nr. 108 (2000-2001) for å tilrettelegge for elektronisk kommunikasjon med og i forvaltningen. Bestemmelsen gir adgang til å fastsette forskrift om elektronisk kommunikasjon mellom forvaltningen og publikum, samt om elektronisk saksbehandling og kommunikasjon i forvaltningen.

4.4. Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

eForvaltningsforskriften er gitt med hjemmel i forvaltningsloven § 15 a tredje ledd, og har som formål å «legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Den skal fremme forutsigbarhet og fleksibilitet og legge til rette for samordning av sikre og hensiktsmessige tekniske løsninger». Forskriften skal videre legge til rette for at enhver på en enkel måte kan utøve sine rettigheter og oppfylle sine plikter i forhold til det offentlige, jf. § 1 første ledd.

eForvaltningsforskriften inneholder utfyllende regler om elektronisk kommunikasjon med og i forvaltningen, og fastsetter blant annet krav til bruk av elektroniske kommunikasjonsløsninger, krav til informasjonssikkerhet og regler om digital kontaktinformasjon og reservasjonsordninger. Forskriften inneholder også et eget kapittel om Kontakt- og reservasjonsregisteret, der det blant annet fremgår av § 30 at Digitaliseringsdirektoratet er behandlingsansvarlig for register over digital kontaktinformasjon og reservasjon med tilhørende infrastruktur.

Samtidig inneholder forskriften i dag ingen uttrykkelig bestemmelse som klargjør hvem som har det overordnede forvaltningsansvaret for øvrige digitale fellesløsninger som Digitaliseringsdirektoratet forvalter. De digitale fellesløsningene har utviklet seg til å bli en grunnleggende del av den digitale infrastrukturen i offentlig sektor. De er nødvendige for å oppfylle forskriftens krav til blant annet sikker identifisering, forsvarlig informasjonsutveksling og effektiv kommunikasjon.

4.5. Digitaliseringsrundskrivet

Statlige etaters bruk av flere av fellesløsningene forvaltet av blant annet Digitaliseringsdirektoratet er regulert i Digitaliseringsrundskrivet. Digitaliseringsrundskrivet er en instruks fra regjeringen til statlige etater og gjelder for departementene, statens ordinære forvaltningsorganer, forvaltningsorganer med særskilte fullmakter og forvaltningsbedrifter.

I rundskrivet punktene 1.9 og 1.10 er det satt krav til bruk av enkelte løsninger. Dette gjelder ID-porten, Altinn, Meldingsboksen i Altinn, Digital postkasse til innbyggere, Felles datakatalog, Kontakt- og reservasjonsregisteret, Folkeregisteret, Enhetsregisteret, Matrikkelen og Oppgaveregisteret. Bruk av enkelte av disse løsningene følger også av andre lover og forskrifter.

5. Departementets vurdering og forslag

5.1. Lovtekniske vurderinger – regulering i eForvaltningsforskriften

Departementet foreslår at reguleringen av digitale fellesløsninger som forvaltes av Digitaliseringsdirektoratet, tas inn som i et eget kapittel i eForvaltningsforskriften. Et alternativ til forskriftsregulering er lovregulering. Digitaliseringsdirektoratet har ingen sektorlover som regulerer direktoratets virksomhet. Departementet har derfor vurdert å foreslå en egen lov om de digitale fellesløsningene som Digitaliseringsdirektoratet forvalter. Departementet mener imidlertid at de foreslåtte bestemmelsene egner seg bedre for regulering i forskrift enn i lov.

Forskriftshjemmelen i forvaltningsloven § 15 a tredje ledd har en vid utforming. I Ot.prp.nr. 108 (2000-2001) punkt 2.1.1 fremgår det at begrepet «elektronisk kommunikasjon» skal forstås vidt, og at det «omfatter all elektronisk samhandling». Videre fremgår det av proposisjonen punkt 2.1.2 at elektronisk kommunikasjon forutsetter at det «teknisk og praktisk legges til rette» for slik kommunikasjon, og at dette forutsettes nærmere regulert i forskrift.

Elektronisk kommunikasjon i forvaltningen er avhengig av en velfungerende digital infrastruktur. De digitale fellesløsningene som Digitaliseringsdirektoratet forvalter bidrar til utvikling av helhetlige og brukervennlige digitale tjenester, og legger til rette for en mer effektiv og sammenhengende offentlig forvaltning. Departementet legger til grunn at forhold knyttet til slike løsninger faller naturlig innenfor forvaltningsloven § 15 a tredje ledd og eForvaltningsforskriftens saklige virkeområde.

Stortinget har i juni 2025 vedtatt lov 20. juni 2025 nr. 81 om saksbehandlingen i offentlig forvaltning som skal erstatte lov 10. februar 1967 om behandlingsmåten i forvaltningssaker. I den nye forvaltningsloven er elektronisk kommunikasjon regulert i § 10, som gjelder elektronisk kommunikasjon med og i forvaltningen.

I forarbeidene til den nye loven, Prop. 79 L (2024-2025), vises det i punkt 9.2.2 til at forvaltningslovutvalget foreslo i NOU 2019: 5 punkt 18.3.5 å videreføre forskriftshjemmelen i § 15 a med enkelte språklige forenklinger. I Justis- og beredskapsdepartementets vurderinger i lovproposisjonen punkt 9.2.4 går det fram at også departementet viderefører forskriftshjemmelen «i en noe enklere utforming». Departementet vurderer, basert på ordlyden i bestemmelsene og forarbeidene til den nye forvaltningsloven, at det materielle innholdet i forskriftsbestemmelsen videreføres i den nye forvaltningsloven. Dette innebærer at vurderingene i dette høringsnotatet også vil kunne legges til grunn etter at den nye forvaltningsloven trer i kraft.

5.2. Supplerende rettsgrunnlag

Personvernforordningen artikkel 6 nr. 1 bokstav e gir adgang til behandling av personopplysninger når det er nødvendige for å «utføre en oppgave i allmenhetens interesse». For behandling hjemlet i personvernforordningen artikkel 6 nr. 1 bokstav e stilles det imidlertid krav om at det må foreligge et supplerende rettsgrunnlag jf. artikkel 6 nr. 3, se nærmere omtale av dette under punkt 4. om gjeldende rett ovenfor.

Departementet foreslår i forslaget til ny § 36 i eForvaltningsforskriften at Digitaliseringsdirektoratet skal drifte, forvalte eller på annen måte stille til rådighet digitale fellesløsninger som kan dekke funksjonalitet som er angitt i bestemmelsen. Bokstavene a til j angir hvilke funksjonaliteter fellesløsningene kan omfatte, og avgrenser dermed rekkevidden av direktoratets plikt. Bestemmelsen er imidlertid ikke til hinder for at direktoratet også kan tilby fellesløsninger med en annen funksjonalitet. Digitaliseringsdirektoratet har allerede i dag et ansvar for å forvalte slike fellesløsninger som kan, og i enkelte tilfeller skal, brukes av offentlig sektor i deres oppgaveløsning. Dette følger av blant annet eForvaltningsforskriften § 29 annet ledd, Prop. 1 S, hovedinstruks for Digitaliseringsdirektoratet, de årlige tildelingsbrevene og Digitaliseringsrundskrivet.

I de fellesløsningene der Digitaliseringsdirektoratet behandler personopplysninger, baserer direktoratet i dag behandlingen på flere rettslige grunnlag, jf. kapittel 2 ovenfor. Departementet vurderer at dagens rettslige rammer for Digitaliseringsdirektoratets behandling av personopplysninger fremstår som fragmentert, og at det er behov for en tydeligere og mer helhetlig regulering. Forslaget inneholder derfor en bestemmelse om Digitaliseringsdirektoratets behandling av personopplysninger i tilknytning til direktoratets ansvar for å drifte, forvalte eller på annen måte stille til rådighet digitale fellesløsninger, jf. forslaget til ny § 37 første ledd.

I dag behandler Digitaliseringsdirektoratet personopplysninger i forbindelse med at innbyggerne selv tar initiativ til å bestille MinID. Departementet mener pilotprosjektet med MinID i skolen (se punkt 2 over) viser tydelig at det innebærer store fordeler at direktoratet kan samarbeide med skoler ved utstedelse av MinID. Elevene opplevde piloten med MinID i skolen som brukervennlig og den effektiviserte direktoratets utstedelse av MinID. Departementet mener også at muligheten for samarbeid om utstedelse av MinID vil bidra til å nå regjeringens mål om økt digital inkludering, ved at ungdom får enklere tilgang til en elektronisk identitet.

Løsningen innebærer at skoler, når de bidrar ved utstedelsen av MinID, må dele nødvendige personopplysninger med Digitaliseringsdirektoratet og bekrefte personens identitet. Delingsadgangen vil omfatte elevopplysninger som skolen allerede har, slik som navn og fødselsnummer, samt navn på lærer. Skolens deling av personopplysninger innebærer behandling av personopplysninger som utleveres fra andre enn innbygger selv og som behandles uten at innbyggeren initierer prosessen. Når behandling av personopplysninger ikke er basert på samtykke må det finnes et annet rettslig grunnlag.

Departementet foreslår derfor i forslaget til ny § 37 andre ledd at skoler kan dele personopplysninger med Digitaliseringsdirektoratet når det er nødvendig for at eleven skal få utstedt en eID som gir tilgang til offentlige tjenester. Forslaget gir behandlingsgrunnlag for at skoler kan dele personopplysninger med Digitaliseringsdirektoratet i forbindelse med utstedelse av MinID i skolen. Departementet foreslår imidlertid at bestemmelsen utformes generelt, slik at den regulerer utstedelse av eID, og ikke kun begrenses til utstedelse av MinID. På denne måten legges det til rette for at utstedelse er produktnøytral, slik at bestemmelsen til enhver tid omfatter den eIDen som til enhver tid utstedes av Digdir og som er vanlig å benytte til å søke opptak til videregående skole.

Med bakgrunn i prinsippet om likebehandling av private og offentlige skoler, har departementet vurdert å inkludere private skoler i reguleringen som foreslås i § 37 andre ledd. Departementet har imidlertid ikke hjemmel i forvaltningsloven § 15 a til å regulere private skoler. Med «skoler» i forslaget til § 37 andre ledd menes derfor offentlige skoler.

Departementet legger til grunn at Digitaliseringsdirektoratets ansvar for å drifte, forvalte og stille til rådighet digitale fellesløsninger, herunder utstedelse av eID, utgjør oppgaver som utføres i allmennhetens interesse, jf. personvernforordningen artikkel 6 nr. 1 bokstav e. Tilsvarende legger departementet til grunn at offentlige virksomheters utlevering av personopplysninger til Digitaliseringsdirektoratet når det er nødvendige for å utstede en eID, skjer som ledd i utførelsen av oppgaver i allmenhetens interesse. Å sikre at innbyggere har tilgang til elektronisk identitet for bruk av sentrale offentlige digitale tjenester bidrar til å forebygge digitalt utenforskap og legger til rette for effektiv kommunikasjon mellom forvaltningen og innbyggerne.

Departementet legger til grunn at de foreslåtte nye §§ 36 og 37 samlet vil utgjøre et supplerende rettsgrunnlag etter personvernforordningen artikkel 6 nr. 3 første ledd bokstav e og annet ledd. Formålet med bestemmelsene er å tydeliggjøre behandlingsgrunnlaget for Digitaliseringsdirektoratet og andre offentlige virksomheter, og bidra til større forutberegnelighet. Samtidig understrekes det at de grunnleggende prinsippene for behandling av personopplysninger fortsatt gjelder, jf. personvernforordningen artikkel 5 nr. 1. Dette innebærer blant annet at personopplysningene bare kan behandles til uttrykkelig angitte og berettigede formål, at de skal være nødvendige for formålet, at de skal være riktige og ikke lagres i lenger tid enn det som er nødvendig for formålet, samt god informasjon om behandlingen til alle berørte.

Departementet vurderer at personopplysningene som omfattes av forslaget til § 37 andre ledd ikke er omfattet av taushetsplikt og foreslår i dette høringsnotatet ingen regler om unntak fra lovbestemt taushetsplikt. Departementet ber likevel om høringsinstansenes innspill på om det kan være behov for unntak fra lovbestemt taushetsplikt i tilknytning til departementets forslag til regulering av Digidirs utvikling, drift og forvaltning av digitale fellesløsninger eller behandling av personopplysninger i forbindelse med utstedelse av MinID.

5.2.2. Særlig om behandling av personopplysninger etter personvernforordningen artikkel 9 og 10

Personvernforordningen stiller særlige krav til lovligheten av behandlingen når personopplysningene som behandles er «særlige kategorier» av personopplysninger. Etter personvernforordningen artikkel 9 nr. 1 er behandling av slike personopplysninger i utgangspunktet forbudt. For at behandling av personopplysninger som omfattes av forbudet skal være lovlig, må vilkårene i et av unntakene i artikkel 9 nr. 2 bokstav a til j være oppfylt. Etter artikkel 9 nr. 2 bokstav g er ikke behandlingen ulovlig dersom behandlingen:

«[...] er nødvendig av hensyn til viktige allmenne interesser, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten

til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser.»

Departementet foreslår i forslaget til ny § 37 første ledd at Digitaliseringsdirektoratet kan behandle særlige kategorier personopplysninger, jf. personvernforordningen artikkel 9 nr. 1, når dette er nødvendig for å utvikle, drifte, forvalte og stille digitale fellesløsninger til rådighet.

Departementet legger til grunn at det i forbindelse med Digitaliseringsdirektoratets ansvar for å drifte, forvalte og stille til rådighet funksjonalitet som nevnt i forslaget til ny § 36, kan være nødvendig å behandle personopplysninger som omfattes av personvernforordningen artikkel 9 nr. 1. De digitale fellesløsningene dekker grunnleggende funksjoner for offentlig oppgaveløsning, herunder blant annet innlogging, tilgangsstyring, representasjon, datadeling og samhandling på tvers av virksomheter. I denne sammenheng kan det inngå opplysninger som direkte eller indirekte omfattes av artikkel 9 nr. 1, for eksempel helseopplysninger eller opplysninger som inngår i identitets- eller sikkerhetsrelaterte kontroller, herunder biometriske opplysninger.

Forslaget til ny § 37 første ledd regulerer også behandling av personopplysninger som er omfattet av personvernforordningen artikkel 10, om straffedommer og lovovertridelser. Det vil kunne oppstå behov for at Digitaliseringsdirektoratet behandler opplysninger som for eksempel indikerer at personer har bostedsadresse i et fengsel. Et eksempel er direktoratets ansvar for lagring av innbyggeres meldinger i Altinn innboks.

Etter departementets vurdering ivaretar de digitale fellesløsningene sentrale hensyn knyttet til sikker, effektiv og helhetlig oppgaveløsning i offentlig sektor. Løsningene er en grunnleggende forutsetning for at innbyggere og virksomheter skal kunne benytte offentlige digitale tjenester, og bidrar til å forebygge digitalt utenforskap, samt legge til rette for sikker og effektiv kommunikasjon mellom forvaltningen og innbyggerne. Disse hensynene tilsier at behandlingen anses nødvendig av hensyn til viktige allmenne interesser.

Departementet har avgrenset hjemmelen for behandling av personopplysninger etter personvernforordningen artikkel 9 og 10 til de tilfellene hvor slik behandling er nødvendig for å oppfylle formålene som følger av bestemmelsene. På denne måten gis det ikke grunnlag for å behandle slike opplysninger til andre formål enn det som er vurdert som nødvendig og forholdsmessig.

Departementet legger videre til grunn at behandlingen vil ha grunnlag i nasjonal rett og at hjemmelen er forenlig med det grunnleggende innholdet i retten til vern av personopplysninger, jf. forslaget til nye §§ 36 og 37. Videre vurderer departementet at det ikke er behov for å fastsette egnede og særlige tiltak i de foreslåtte bestemmelsene for å verne den registrertes rettigheter og interesser. Etter departementets syn er den registrertes rettigheter og interesser tilstrekkelig ivaretatt gjennom gjeldende rett, herunder personvernforordningens krav til informasjonssikkerhet og dataminimering.

På denne bakgrunn mener departementet at vilkårene i artikkel 9 nr. 2 bokstav g er oppfylt ved reguleringen i forslaget til ny § 37, idet behandlingen er nødvendig av hensyn til viktige allmenne interesser på grunnlag av medlemsstatenes nasjonale rett.

6. Forslagets personvernkonsekvenser

Forslaget til ny § 36 innebærer ingen endringer i bruken av de digitale fellesløsningene forvaltet av Digitaliseringsdirektoratet. Formålet med bestemmelsen som foreslås er å sikre et juridisk rammeverk for fellesløsningene Digitaliseringsdirektoratet forvalter.

Forslaget til ny § 37 første ledd, som sikrer et tydelig behandlingsgrunnlag for direktoratets behandling av nødvendige personopplysninger i forbindelse med utvikling, drift, forvaltning og tilgjengeliggjøring av digitale fellesløsninger innebærer ingen realitetsendring i direktoratets behandling av personopplysninger. Digitaliseringsdirektoratet behandler allerede personopplysninger i de digitale fellesløsningene som direktoratet forvalter, og benytter ulike rettslige grunnlag for slik behandling, herunder personvernforordningen artikkel 6 nr. 1 bokstav a, b, og e. Direktoratet behandler også personopplysninger etter personvernforordningen artiklene 9 nr. 1 og 10 i den forbindelse. Forslaget medfører dermed ingen utvidelse av behandlingen, verken når det gjelder omfanget av behandlingen eller hvilke kategorier av personopplysninger som behandles. Departementet vurderer at personvernkonsekvensene er positive, ettersom det rettslige grunnlaget for behandlingen blir tydeligere.

I tillegg skal forslaget til ny § 37 andre ledd sikre behandlingsgrunnlag for skolers utlevering av personopplysninger til Digitaliseringsdirektoratet i forbindelse med utstedelse av eID. Dette omfatter opplysninger som skolene allerede besitter, slik som navn og fødselsnummer til elever, samt informasjon om læreren, og innebærer ikke innhenting av nye opplysninger.

Å innhente personopplysninger fra andre enn den registrerte selv innebærer et inngrep i personvernet, ved at den enkelte i mindre grad har kontroll over behandlingen av egne opplysninger. Den registrerte vil ikke nødvendigvis være kjent med hvilke opplysninger som utleveres eller når utleveringen skjer. Dette kan svekke åpenheten og forutsigbarheten i behandlingen, og redusere den registrertes reelle mulighet til å utøve sine rettigheter, herunder retten til innsyn, retting og sletting. Slike konsekvenser gjør seg særlig gjeldende for grupper som i mindre grad er i stand til å ivareta egne interesser, herunder mindreårige.

Samtidig ivaretar utlevering av personopplysninger i forbindelse med utstedelse av en eID viktige samfunnsformål. Tilgang til eID er en forutsetning for å kunne benytte en rekke digitale offentlige tjenester, og manglende tilgang kan føre til digitalt utenforskap. Ved å legge til rette for flere og mer tilgjengelige utstedelsesmetoder, kan forslaget bidra til at flere får tilgang til slike tjenester, herunder grupper som i dag kan ha utfordringer med å skaffe seg eID på egen hånd, slik som skoleelever. Forslaget vil styrke den enkelte elevs mulighet til å ivareta egne rettigheter og interesser i møte med det offentlige, og vurderes å være forholdsmessige ettersom inngrepet i personvernet er begrenset.

Etter personvernforordningen skal personopplysninger samles inn for spesifikke, uttrykkelig angitte og legitime formål, og behandlingen skal være begrenset til det som er nødvendig for å oppnå disse formålene, jf. artikkel 5 nr. 1 bokstav b. Departementet legger til grunn at prinsippet om formålsbegrensning ivaretas ved at forslaget avgrenser behandlingen til personopplysninger som er nødvendige for å gjennomføre utstedelse av eID, innenfor klare

og definerte rammer. Et tydelig behandlingsgrunnlag og klart angitte formål vil også bidra til økt forutsigbarhet for den enkelte.

Samlet sett vurderer departementet at de positive sidene ved de foreslåtte forskriftsbestemmelsene oppveier de negative konsekvensene for den enkeltes personvern.

7. Økonomiske og administrative konsekvenser

For MinID i skolen er det gjennomført en forenklet samfunnsøkonomisk analyse. De prissatte virkningene gir en netto nåverdi på om lag minus 0,95 mill. kroner over analyseperioden (analyseperiode på 10 år, og alle beløpene er oppgitt som nåverdier i 2024-kroner). I analyseperioden er investeringskostnadene anslått til om lag 9,8 mill. kroner, drifts- og forvaltningskostnader til om lag 4,1 mill. kroner, samt skattefinansieringskostnader til om lag 1,15 mill. kroner. Samtidig er redusert tidsbruk for lærere og rådgivere anslått til om lag 6,9 mill. kroner. Alle beløpene er målt i nåverdi (2024-kroner). Analysen er følsom for forutsetningene som er lagt til grunn, særlig anslagene for tidsbesparelser i skolen.

De ikke-prissatte virkningene er samlet vurdert som positive, blant annet i form av redusert belastning for skolepersonell og redusert tidsbruk for elever, foresatte og Digdir, samt gevinster som følge av økt digital deltakelse. Samlet sett tilsier de prissatte og ikke-prissatte virkningene at tiltaket vurderes som samfunnsøkonomisk lønnsomt.

MinID i skolen kan medføre både økt og redusert tidsbruk for skolepersonell, og innebære omfordeling av oppgaver. For skolene vil tiltaket medføre enkelte administrative konsekvenser knyttet til gjennomføringen av utstedelse av MinID. Skolene har også i dag en rolle i å bistå elever med å skaffe seg MinID, som en del av elevenes behov i forbindelse med søknad til videregående opplæring. Tiltaket innebærer i stor grad en strukturering og standardisering av oppgaver som delvis allerede utføres i skolen.

MinID i skolen vurderes derfor ikke å medføre vesentlige økonomiske eller administrative konsekvenser. Kostnader knyttet til bruk av løsningen vil i stor grad motsvares av bortfall av eksisterende kostnader til utsending av aktiveringsbrev. Tiltaket vurderes samlet sett å kunne håndteres innenfor gjeldende budsjettammer. Løsningen er samtidig forventet å bidra til økt sikkerhet i utstedelsesprosessen for MinID.

Forslaget for øvrig innebærer ingen endringer i bruken av fellesløsningene forvaltet av Digitaliseringsdirektoratet. Formålet med de bestemmelsene som foreslås i dette høringsnotat er å sikre et juridisk rammeverk for behandling av personopplysninger i de fellesløsningene Digitaliseringsdirektoratet forvalter. Det rettslige grunnlaget vil tydeliggjøre Digitaliseringsdirektoratets ansvar for å levere digitale fellesløsninger og gi direktoratet et klarere grunnlag for direktoratets behandling av personopplysninger i løsningene. Forslagene anses derfor å ha begrensede eller ingen økonomiske og administrative konsekvenser.

8. Merknader til enkelte bestemmelser

Til ny § 36 Digitale fellesløsninger

Paragrafen pålegger Digitaliseringsdirektoratet å drifte, forvalte eller på annen måte stille til rådighet digitale fellesløsninger til bruk i offentlig oppgaveløsning. Bokstavene a til j regulerer funksjonalitet som fellesløsningene kan omfatte. Det vil si at plikten direktoratet har til å drifte, forvalte eller på annen måte stille til rådighet digitale fellesløsninger er begrenset til funksjonalitet som omtales i bokstavene a til j. Dette betyr ikke at direktoratet er forhindret fra å tilby fellesløsninger med annen funksjonalitet.

Offentlig oppgaveløsning vil for eksempel omfatte saksbehandling, herunder enkeltvedtak, og drift eller utvikling av tjenester som understøtter det offentliges grunnleggende oppgaver. Offentlig oppgaveløsning kan omfatte aktiviteter av privatrettslig karakter dersom disse er nødvendige for at det offentlige skal kunne drifte seg selv og dermed utføre sine offentlige oppgaver. Det avgjørende er at bruken av fellesløsningene er knyttet til ikke-økonomisk aktivitet. Som ikke-økonomisk aktivitet regnes all aktivitet som ikke leverer tjenester i et marked. Hvilke oppgaver som er offentlig oppgaveløsning, og dermed gir mulighet for å bruke fellesløsningene, må vurderes i det enkelte tilfelle.

En ansettelsesprosess i for eksempel et kommunalt foretak som driver økonomisk aktivitet, vil derfor ikke kunne benytte fellesløsningene til å understøtte denne prosessen. En slik ansettelsesprosess er å regne som økonomisk aktivitet. Samtidig vil en ansettelse til planavdelingen i kommunen være underlagt forvaltningsloven (jf. forvaltningsloven § 2) og regnes som ikke-økonomisk aktivitet.

«Drifte, forvalte eller på annen måte stille til rådighet» innebærer ikke at Digitaliseringsdirektoratet må utføre disse oppgavene selv, men kan utføres av andre på direktoratets vegne. Underleverandører kan eksempelvis benyttes.

Bokstav a er ment å dekke det som pr i dag er verktøy, infrastrukturtjenester og standarder som er grunnleggende for å etablere og drifte de produktene som utgjør Altinn-løsningen. Det vil også dekke loggtjenester, infrastrukturtjenester, tilgangsstyring og kontrollsystemer knyttet til felles driftsplattform for tillitstjenester i Digitaliseringsdirektoratet.

Bokstav b er ment å dekke det som pr i dag er produktet Altinn studio.

Bokstav c er ment å dekke det som pr i dag er produktene Altinn autorisasjon, MinID, selvregistrert innlogging, ID-porten inkludert vergeporten og eIDAS-noden og Ansattporten. Det er også ment å omfatte tilstøtende funksjoner, som for eksempel elektroniske attester og andre former for bevis som kan brukes uavhengig av eID-ordninger. Behandlingsgrunnlaget for MinID skal omfatte all nødvendig behandling av personopplysninger både ved de ulike utstedelsesprosessene og når løsningen er i bruk av innbygger.

Bokstav d er ment å dekke det som pr i dag er samtykkefunksjonaliteten i produktet Altinn autorisasjon.

Bokstav e er ment å dekke det som pr i dag er produktet Altinn varsling.

Bokstav f er ment å dekke det som pr i dag er produktene Altinn melding, Altinn formidling, data.altinn.no, Dialogporten, Altinn arbeidsflate, data.norge.no., maskinporten, digital postkasse til innbyggere og eFormidling.

Bokstav g er ment å dekke det som pr i dag er produktene funksjonalitet for signering i Altinn studio og eSignering.

Bokstav h er ment å dekke det som pr i dag er produktene Altinn arbeidsflate, herunder profil, aktivitetslogg, samtykkelogg, meldinger og kvitteringer fra tjenesteeiere som benytter produktene Melding og Formidling. I tillegg gir dette grunnlag for å anskaffe tilsvarende tjenester i markedet.

Bokstav i er ment å dekke det som pr i dag er produktene informasjonsportalene altinn.no, norge.no, Altinn brukerservice, Altinn servicedesk, Digdir brukerstøtte, Digdir servicedesk.

Bokstav j er ment å dekke det som i dag er ELMA.

Paragrafen regulerer hvilken funksjonalitet som levers av Digitaliseringsdirektoratet, ikke de konkrete produktene ved navn. Dette gir fleksibilitet til å endre produktporteføljen som direktoratet leverer.

Til ny § 37 Behandling av personopplysninger

Bestemmelsens første ledd gir Digitaliseringsdirektoratet hjemmel til å behandle personopplysninger når dette er nødvendig for å drifte, forvalte og stille til rådighet funksjoner som nevnt i forslaget § 36. Bestemmelsen åpner også for behandling av personopplysninger ved digital ID-kontroll, herunder bruk av biometriske opplysninger, når det er nødvendig for ID-kontrollen.

Den konkrete ansvarsdelingen mellom offentlige etater og kommuner som bruker fellesløsningene som Digitaliseringsdirektoratet forvalter, vil fremgå av blant annet avtaler. Dette omfatter blant annet hvor grensene for hvem som er databehandler eller behandlingsansvarlig går.

Andre ledd gir hjemmel for skoler til å dele personopplysninger med Digitaliseringsdirektoratet når det er nødvendig for å utstede en eID. Med eID menes her den eIDen som til enhver tid utstedes av Digdir og som er vanlig å benytte til å søke opptak til videregående skole og enkelte andre offentlige tjenester. For tiden er dette MinID. Dette innebærer at skoler kan dele opplysninger om elever og lærere i den hensikt å tilrettelegge for at Digitaliseringsdirektoratet kan utstede MinID til elevene. Opplysningene kan deles uavhengig av den registrertes samtykke. Med «skoler» menes offentlige skoler.

9. Forslag til forskrift om endringer i forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

I

Nytt kapittel 8 skal lyde:

Kapittel 8. Digitale fellesløsninger forvaltet av Digitaliseringsdirektoratet

§ 36. *Digitale fellesløsninger*

Digitaliseringsdirektoratet skal drifte, forvalte eller på annen måte stille til rådighet digitale fellesløsninger til bruk i offentlig oppgaveløsning, som kan dekke følgende:

- a. Plattformfunksjonalitet
- b. Funksjonalitet for tjenesteproduksjon
- c. Funksjonalitet for å sikre fysiske og juridiske personer tilgang til offentlige tjenester gjennom innlogging, tilgangsstyring og mulighet til å opptre på vegne av andre
- d. Samtykkefunksjonalitet
- e. Funksjonalitet for varslings
- f. Funksjonalitet for hendelsesdistribusjon og datadeling, inkludert meldings- og dialogtjenester
- g. Funksjonalitet for signering
- h. Funksjonalitet for tilgjengeliggjøring av informasjon til sluttbruker
- i. Funksjonalitet for brukerstøtte
- j. Funksjonalitet for oppslag i offentlige registre

§ 37. *Taushetsplikt og behandling av personopplysninger*

Digitaliseringsdirektoratet kan behandle personopplysninger, herunder opplysninger som nevnt i personvernforordningen artiklene 9 og 10, når dette er nødvendig for å drifte, forvalte eller stille til rådighet funksjoner som nevnt i § 36.

Skoler kan dele personopplysninger med Digitaliseringsdirektoratet når dette er nødvendig for å utstede en eID til elever ved skolen.

II

Nåværende kapittel 8 blir kapittel 9.

Nåværende §§ 36 til 39 blir §§ 38 til 41.

§ 27 første ledd bokstav d skal lyde:

«d. at sertifikatet er utstedt av en sertifikatutsteder som anbefales eller er anerkjent av koordineringsorganet, jf. § 39, eller som forvaltningsorganet kan akseptere i henhold til sin sikkerhetsstrategi.»

III

Ikrafttredelse

Forskriften trer i kraft 1. januar 2027.