

1 Generelle

1.1 Om bruksvilkår

Digitaliseringsdirektoratet (heretter Digdir) forvalter flere nasjonale fellesløsninger som offentlige virksomheter (heretter benevnt som «Kunde») skal, eller kan benytte for å tilby bedre og mer enhetlige tjenester, og effektivisere driften.

Disse bruksvilkårene for offentlige virksomheter gjelder for alle fellesløsningene, for utenom elnnsyn som har [egne bruksvilkår](#). Vilkårene er bygget opp med ett kapittel som gjelder alle løsninger og deretter ett kapittel per løsning. Digdir er forpliktet til å levere i samsvar med bruksvilkårene når bemyndiget person hos kunde har signert avtaledokumentet. Kapittel som gjelder de enkelte løsningene, trer i kraft når kunden tar de enkelte løsningene i bruk.

1.2 Virksomheter som kan benytte fellesløsningene

Følgende virksomheter kan benytte seg av fellesløsningene:

*Offentlig virksomhet og virksomheter som utfører oppgaver på vegne av, og som helt eller **delvis** er finansiert av, det offentlige. 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.*

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

Det er Digitaliseringsdirektoratet som avgjør om en virksomhet kan benytte fellesløsningene.

1.3 Finansiering

Det kan påløpe brukskostnader på fellesløsningene. Dette skjer i samsvar med de gjeldende kostnadsmodellene for hver fellesløsning som finnes på Samarbeidsportalen. Kunden faktureres i EHF-format, og skal oppgi ett fakturamottak og referanse ved etablering.

Fra 1.1.2026 er Digdir mva-pliktig. Dette medfører at Digdir vil ha merverdiavgiftspliktig aktivitet for deler av sin virksomhet. Dette gjelder Digital postkasse til innbyggere, eSignering, ID-porten og Maskinporten. Faktura fra Digdir vil for disse produktene vise spesifisert merverdiavgift.

Kunden betaler selv for [tilleggstjenester](#) som bestilles i samsvar med gjeldende prisliste.

Kundens kostnader med integrasjon mot fellesløsningene dekkes av kunden selv. Dette gjelder også bistand fra Digdirs underleverandører når dette er bestilt som tilleggstjeneste.

1.4 Samarbeid

Det er opprettet flere samarbeidsorganer for å gi kundene mulighet til å påvirke den videre utvikling av fellesløsningene.

1.4.1 Styringsråd

Styringsrådet er et rådgivende organ for Digdir og skal særlig behandle viktige saker som gjelder fellesløsningene. Styringsrådet bistår Digdir med å sikre at fellesløsningene utvikles i tråd med offentlig sektors behov, og for å sikre en samordnet modell for felles styring, organisering og finansiering. Styringsrådet består av 12-14 medlemmer, normalt på avdelingsdirektørnivå, og det gjennomføres fire møter i løpet av året. [Mandat for styringsrådet](#) er tilgjengelig på Samarbeidsportalen.

1.4.2 Produktråd

Ved behov kan styringsrådet og Digdir opprette produktråd for Digdirs produkter eller produktgrupper. Produktrådet er et rådgivende organ for Styringsrådet og Digdirs produktgrupper. I produktrådet drøftes eksempelvis utviklingsretning, veikart og

handlingsplaner. Produktrådene kan være permanente eller for en periode, og rapporterer til styringsrådet. Produktrådet består av 6-10 representanter. [Mandat for produktrådet](#) er tilgjengelig på Samarbeidsportalen.

1.4.3 Brukerråd

Brukerrådet er en heldigital konferanse og møteplass for Digdir, våre kunder og leverandører. På Brukerrådet presenterer vi utviklingsplaner for fellesløsningene, viser eksempler på bruk av løsningene og inviterer til innspill og diskusjoner. Deltakelse i brukerrådet er åpen for alle kunder og alle kunder kan foreslå saker til brukerrådet.

1.4.4 Brukerstøtteforum

Brukerstøtteforum skal bidra til å effektivisere og koordinere brukerstøtten overfor sluttbruker og er et forum for informasjons- og erfaringsutveksling mellom Digdir og kundenes brukerstøttefunksjoner. [Mandat for brukerstøtteforumet](#) er tilgjengelig på Samarbeidsportalen.

1.5 Digdirs ansvar

Digdir har ansvaret for forvaltning, drift og videreutvikling av fellesløsningene.

Digdir skal ivareta kundenes interesser på en god måte og skal i drift og videreutvikling av fellesløsningene forsøke å ivareta kundenes samlede og omforente behov.

1.5.1 Samarbeidsportalen

[Samarbeidsportalen](#) er den primære informasjons- og varslingskanalen fra Digdir om fellesløsningene. Her finnes beskrivelse av fellesløsningene, teknisk dokumentasjon, hvordan de kan tas i bruk, informasjon om kostnader, statistikk, leveranseplan og release-logg. Du kan finne kommende arrangementer, se tidligere avholdte webinarer, lese nyheter og følge våre pågående prosjekter.

På Samarbeidsportalen finner du varslingskanalen Status Digdir (status.digdir.no). Der publiseres informasjon om hendelser og vedlikehold på fellesløsningene. Kunde er selv ansvarlige for å sette opp og vedlikeholde varslingspunkt for å sikre at de mottar varsel ved alvorlige hendelser, endringer, vedlikehold eller annen viktig informasjon. Det er mulig å abonnere på varsel.

Kunder som godtar bruksvilkår, får tilgang til en innlogget del på Samarbeidsportalen som gir tilgang til selvbetjening og vedlikehold av virksomhetsinformasjon i våre systemer. Kunden har selv ansvar for å holde nødvendig informasjon om egne tjenester oppdatert på Samarbeidsportalen.

1.5.2 Planer og rapporter

1.5.2.1 Utviklingsplan

Digdir utarbeider utviklingsplaner (roadmap) som gir oversikt over ønsket og planlagt funksjonalitet for fellesløsningene. Utviklingsplanene er tilgjengelig under hvert produkt/fellesløsning på Samarbeidsportalen

1.5.2.2 Statistikk

Digdir leverer månedlig statistikk for fellesløsningene. Denne statistikken inneholder oversikt over bruk av fellesløsningene, tilgjengelighet og responstider i løsningene.

[Statistikken](#) gjøres tilgjengelig på Samarbeidsportalen innen den 20. i påfølgende måned.

1.5.3 Brukerstøtte

Digdir drifter brukerstøtte og [hjelpesider for fellesløsningene](#).

Ved henvendelser til brukerstøtte på telefon skal sluttbruker normalt få kontakt med en veileder innen to minutter. Ved henvendelser til brukerstøtte på chat skal sluttbruker normalt få kontakt med en veileder innen et minutt. Ved henvendelser på e-post skal sluttbrukeren normalt få svar innen en virkedag.

1.5.4 Endringer

Digdir kan endre tjenestene som inngår som en del av fellesløsningene. Slike endringer kan typisk være forbedring av funksjonalitet, endring i grensesnittet mot kunde, oppgradering av programvare og maskinvare og mindre endringer i tjenestenivå

Endringer som kan ha betydning for kunden varsles på Status Digdir. Dersom endringen påvirker kundene, skal det så langt som mulig tas hensyn til kritiske perioder.

Versjonslogg er tilgjengelig på Samarbeidsportalen under Release-logg (release.digdir.no)

1.5.4.1 Produksjonssettinger

Det gjennomføres hyppige leveranser i fellesløsningene. Varsling av produksjonssettinger skjer på Status Digdir/Samarbeidsportalen.

1.5.4.2 Tjenestenivå

Alle krav som er spesifisert i bruksvilkåret skal følges opp slik at tjenester og ytelser blir levert med avtalt og tilfredsstillende kvalitetsnivå.

Driftsperioden for Digdir sine fellesløsninger er 24 timer/7 dager i uken/365 dager i året. Måleperiode for alle tjenester og ytelser er månedlig (per kalendermåned).

1.5.5 Hendelseshåndtering

En hendelse er et ikke planlagt avbrudd eller reduksjon i kvalitet i en tjeneste eller fellesløsning. Ved hendelser følger Digdir intern prosess for hendelseshåndtering.

1.5.5.1 Tilgjengelighet og responstid

Digdir har beredskap for å håndtere kritiske og alvorlige hendelser 24 timer/7 dager i uken/365 dager i året.

1.5.5.2 Varsling ved hendelser

Etter at Digdir har identifisert og kategorisert en hendelse, blir den varslet og fortløpende oppdatert på Samarbeidsportalen på Digdirs varslingskanal [Status Digdir](#).

Dersom hendelsen involverer kunden, plikter kunden å være tilgjengelig for Digdir for best mulig håndtering av hendelsen.

1.5.5.3 Håndtering av informasjon ved hendelser

Ved hendelser knyttet til fellesløsningene skal Digdir håndtere informasjon overfor sluttbruker og media med mindre partene avtaler noe annet for det enkelte tilfellet.

Digdir skal ved brudd på personopplysningssikkerheten, som behandlingsansvarlig, sende melding til Datatilsynet i samsvar med personopplysningsloven artikkel 33, jf. § 1.

Digdir skal ved brudd på personopplysningssikkerheten, som databehandler, underrette den behandlingsansvarlige og bistå denne med å sende melding til Datatilsynet i samsvar med personopplysningsloven.

1.5.6 Krise og beredskap

Digdir skal ha krise- og beredskapsplaner for drift av fellesløsningene og sørge for at slike planer også er etablerte og oppdaterte hos Digdirs leverandører.

1.6 Kundens ansvar

1.6.1 Selvbetjening på ID-porten, Ansattporten og Maskinporten

Digdir tilbyr selvbetjening både via API og et grafisk grensesnitt. Her kan kunder opprette og administrere klienter i ID-porten, Ansattporten og Maskinporten.

Tilgang til grafisk grensesnitt er styrt gjennom rettigheter i Altinn. Kundene er selv ansvarlig for å delegere nødvendige tilganger til personer som skal administrere på vegne av virksomheten.

Se “Ta i bruk” på produktsidene på Samarbeidsportalen for mer informasjon.

1.6.1.1 Logger

Selvbetjeningsløsningen logger endringer, aktiviteter og hvem som utfører endringene. Digdir lagrer logger i 12 måneder.

1.6.2 Datadeling – ID-porten, Ansattporten og Maskinporten - API-tilbyders ansvar

Digdir gjør ingen kvalitetskontroll eller overprøver tilbyders beslutning om hvilke konsumenter som skal ha tilgang til sine data.

Tilbyder av data skal ha rutiner for å administrere konsumenter som skal ha tilganger.

Tilbyder av data skal sikre at konsument som delegerer ansvaret for sin integrasjon til en underleverandør er informert om konsekvensene av delegeringen. For eksempel kan tilbyder sin avtale med konsument inneholde informasjon om at konsumenten kan delegerer sin tilgang videre til en leverandør, men at ansvaret fortsatt ligger hos API-konsument.

Autentisering med ID-porten blir fakturert i samsvar med [kostnadsmodellen for ID-porten](#), der det er API-tilbyder som bærer kostnaden.

1.6.3 Informasjon fra Digdir

Kunden er selv ansvarlig for å holde seg oppdatert på nyheter, varsel og viktig informasjon på Samarbeidsportalen, beskrevet i kapittel 1.5.

1.6.4 Nye eller endrede tjenester

Ved ny eller endret bruk av fellesløsningene eller endringer i egne systemer som vil påvirke integrasjonen mot fellesløsningen, skal kunden informere Digdir minimum 1 måned før planlagt oppstart/endring.

Kunden skal følge integrasjonskrav og etablerte standarder som fastsettes av Digdir. Kunden skal stille med nødvendig kompetanse og dekke egne kostnader for å gjennomføre eget arbeid i forbindelse med integrasjon mot fellesløsningene.

Ved oppretting av ny tjeneste i selvbetjening skal kunde beskrive formålet med tjenesten.

1.6.5 Varssling

Kunden skal så raskt som mulig informere Digdir om hendelser i tilknytning til fellesløsningene eller i egne tjenester som kan ha betydning for fellesløsningene.

Dersom det oppstår en kritisk eller alvorlig hendelse hos kunden, kan Digdir koble tjenesten fra fellesløsningene inntil kunden har dokumentert overfor Digdir at hendelsen er utbedret, eller relevante tiltak er iverksatt.

1.6.6 Krise- og beredskap

Kunden skal ha nødvendige krise- og beredskapsplaner.

1.6.7 Brukerstøtte

Kunden skal ha nødvendig brukerstøtte overfor sluttbruker for egne tjenester.

1.7 Generelt om personopplysninger (databehandleravtale)

Digdir behandler på vegne av kunde personopplysninger på ulike måter og i ulik grad i de forskjellige fellesløsningene. I noen tilfeller er det Digdir som er databehandler og i noen tilfeller benytter Digdir databehandler for å behandle personopplysninger på vegner av kunden. Bruksvilkårene og tilknyttede dokumenter er Digdirs garanti for at behandlingen oppfyller kravene i personvernforordningen.

Behandlingsansvarlig og databehandler er definert i kapittel tilhørende de enkelte fellesløsningene, der dette er relevant.

Med henvisning til personvernforordningen art. 28, punkt 3, jf. personopplysningsloven § 1 angis følgende:

1. Digdir behandler personopplysninger i henhold til bruksvilkårene som nærmere definert i de enkelte kapittel nedenfor.
2. Digdir og alle personer som er autorisert til å behandle personopplysninger er underlagt taushetsplikt om alle forhold de får innsyn i ved å behandle personopplysninger i henhold til denne avtalen, jf. også signeringsdokumentet punkt 4.
3. Digdir treffer tekniske og organisatoriske tiltak etter forordningen art 32 for å ivareta konfidensialitet, integritet og tilgjengelighet i samsvar med funksjonene i de enkelte løsningene.
4. I de tilfeller Digdir engasjerer databehandlere er dette beskrevet i kapittelet tilhørende de enkelte fellesløsningene. Kunden gir generell tillatelse til at Digdir kan endre databehandlere. Dette skal likevel skje i samsvar med bestemmelsene om endringer i bruksvilkårene definert i signeringsdokument punkt 7.
5. Digdir har rutiner for å oppfylle den registrertes rettigheter etter forordningen kap. III.

6. Digdir bistår med oppfylldg av plikter etter forordningen art 32-36.
7. Sletting og tilbakelevering er regulert i kapittelet til den enkelte fellesløsning.
8. Se punkt 1.8 nedenfor.

1.8 Innsyn og revisjon

Digdir skal gjennom revisjon og verifikasjon sikre at tilknyttede leverandører overholder avtalte forpliktelser.

Digdir skal på forespørsel fremlegge dokumentasjon fra gjennomførte revisjoner av fellesløsningene dersom kunden ved kvalitetsrevisjon eller sertifisering av egne tjenester, eller i forbindelse med etterlevelse av rettslige forpliktelser, etterspør dette. Kunden kan også be om ytterligere informasjon og bistand i henhold til de avtaler Digdir har med sine leverandører.

I samråd med styringsrådet kan det opprettes en revisjonskomité bestående av utvalgte kunder. Revisjonskomitéens mandat fastsettes ved opprettelse.

2 ID-porten

2.1 Om ID-porten

ID-porten er en fellesløsning for identitetshåndtering. Ved bruk av kjente elektroniske ID-er (e-ID) får innbygger tilgang til digitale tjenester på tvers av offentlig sektor.

Digdir er avtalepart overfor eksterne e-ID-leverandører, og gjennom avtalen med Digdir kan innbygger bruke sin foretrukne e-ID til innlogging i ID-porten.

Følgende e-ID-er kan benyttes i ID-porten:

- MinID – offentlig e-ID på betydelig sikkerhetsnivå, levert av Digdir
- BankID – e-ID på høyt sikkerhetsnivå, levert av Stø AS
- Buypass – e-ID på høyt sikkerhetsnivå, utstedt av Buypass AS
- Commfides – e-ID på høyt sikkerhetsnivå, utstedt av Commfides Norge AS.

Mer informasjon om hva ID-porten er og hvordan den fungerer er tilgjengelig på [Samarbeidsportalen](#).

2.1.1 Beskrivelse og funksjonalitet

ID-portens tekniske dokumentasjon er tilgjengelig på produksiden på Samarbeidsportalen ([Digdir Docs](#)).

2.1.1.1 Autentisering av sluttbrukere

ID-porten tilbyr en enhetlig autentisering av sluttbrukere, uavhengig av hvilken e-ID sluttbruker foretrekker, så lenge valgt e-ID tilfredsstiller nødvendig sikkerhetsnivå på tjenesten hos kunden.

2.1.1.2 Single sign-on

ID-porten tilbyr engangspålogging (single sign-on), slik at sluttbruker får tilgang på tvers av offentlige tjenester gjennom én pålogging til ID-porten.

Kunder som ikke ønsker single sign-on for enkelte av sine tjenester, kan reservere den enkelte tjeneste mot å inngå i denne funksjonaliteten.

2.1.1.3 Pseudonymisert innlogging

Pseudonymisert innlogging gir en sterk innlogging samtidig som klienten ikke mottar fødselsnummeret. På den måten utveksles ikke mer personopplysninger enn nødvendig og klienter slipper behandlingsansvar.

2.1.2 Prinsipper for bruk

Bruk av e-ID via ID-porten skal bygge på to hovedprinsipper, brukervennlighet og likebehandling.

Brukervennlighet for sluttbrukeren ivaretas ved at:

- Bruk av ID-porten er gratis for sluttbruker.
- e-ID-er på et sikkerhetsnivå skal også kunne benyttes for tilgang til tjenester som krever et lavere sikkerhetsnivå
- ID-porten tilbyr ett brukergrensesnitt for valg av tilknyttede e-ID-er.

e-ID-leverandørene skal behandles likt, dette ivaretas ved at:

- Kunden kan ikke reserve sine tjenester mot en eller flere e-ID-er som er tilknyttet ID-porten. Det vil si at alle kunder som tilbyr tjenester på nivå høyt, må akseptere

alle tilknyttede e-ID-er på nivå høyt. Kunder som tilbyr tjenester på nivå betydelig, må akseptere alle tilknyttede e-ID-er på nivå betydelig og høyt.

- Alle e-ID-er som er tilknyttet ID-porten, må ha tilfredsstillende risikonivå. Gjennom risikovurderinger, revisjon og godkjenning vil Digdir sikre at tilknyttede e-ID-leverandører opprettholder nødvendig kvalitet og tillitsnivå.
- Alle e-ID-er som er tilknyttet ID-porten på sikkerhetsnivå høyt, skal tilby tjenester for autentisering.
- Kunde skal bruke ID-portens navn og logo på alle nettsider og apper. e-ID-leverandørers navn og logo skal ikke brukes. [Les mer om bruk av logo på Samarbeidsportalen.](#)
- Kunden kan ikke benytte ID-porten til å utstede ny e-ID.

2.2 Finansiering

[Kostnadsmodell for ID-porten](#) er tilgjengelig på Samarbeidsportalen.

2.3 Årsplan

På bakgrunn av innspill fra kundene utarbeider Digdir en [årsplan](#) for ID-porten.

Årsplanen inneholder høyvolumperioder og kritiske perioder. Årsplanen er tilgjengelig på Samarbeidsportalen.

2.4 Digdirs ansvar

2.4.1 Tjenestenivå

Driftsperioden for ID-porten er 24 timer/7 dager i uken/365 dager i året. Måleperioden for alle tjenester er månedlig (per kalendermåned).

Beskrivelse	Krav
Tilgjengelighet til ID-porten (sluttbrukerløsningen)	99,90 %
Responstid	Mindre enn 3 sekunder for 90 % av forespørslene i gjennomsnitt
Ytelse	300 000 innlogginger i timen

2.5 Behandling av personopplysninger

2.5.1 Digdirs ansvar

Digdir er behandlingsansvarlig for behandling av personopplysninger i ID-porten i forbindelse med organisering av engangspålogging. Digdir er databehandler for kunden i forbindelse ordinære autentiseringer.

Ved autentisering lagrer og videreformidler Digdir sluttbrukers fødselsnummer, sikkerhetsnivå for gjennomført autentisering, sluttbrukers språkvalg og hvilken e-ID som ble benyttet for autentiseringen. I tillegg loggføres hvilken tjeneste sluttbruker logger inn i og noe informasjon knyttet til enheten som brukes for innlogging.

Digitaliseringsdirektoratet lagrer opplysningene om autentisering i ett år.

2.5.2 Kundens ansvar

Kunden er behandlingsansvarlig for opplysninger om autentiseringsoperasjoner utført gjennom ID-porten i forbindelse med autentisering av sluttbrukere.

Kunden må ha lovlig grunnlag for behandling av personopplysninger i henhold til personopplysningsloven §1, jf forordningen artikkel 6. Kunden må ha lovlig grunnlag for å behandle fødselsnummer i henhold til personopplysningsloven § 12.

Kunden skal påse at det bare er ansatte med tjenstlige behov som har tilgang til de personopplysninger som utleveres fra ID-porten.

3 Ansattporten

3.1 Om Ansattporten

Ansattporten er en innloggingsløsning som er tilpasset bruk som ansatt. Løsningen er primært tenkt til innlogging på tvers av virksomheter. Ved å bruke Ansattporten er det lett å lage tjenester som krever representasjon, siden brukeren sitt valgte representasjonsforhold følger med i påloggingen.

Gjennom en ansattpålogging kan personen som autentiserer seg knyttes til virksomheten hen representerer, med eventuelle roller og rettigheter hen har på vegne av virksomheten. Dette gjøres ved bruk av ekstern autoritativ kilde.

Følgende e-ID-er kan benyttes i Ansattporten:

- MinID – offentlig e-ID på betydelig sikkerhetsnivå, levert av Digdir

- BankID – e-ID på høyt sikkerhetsnivå, levert av Stø AS
- Buypass – e-ID på høyt sikkerhetsnivå, levert av Buypass AS
- Commfides – e-ID på høyt sikkerhetsnivå, levert av Commfides Norge AS

Mer informasjon om hva Ansattporten er, hvordan den fungerer og hvem som kan ta den i bruk er tilgjengelig på [Samarbeidsportalen](#).

3.1.1 Beskrivelse og funksjonalitet

Ansattporten leveres uten engangspålogging (Single Sign-On).

Ansattporten kan brukes til ordinær sluttbrukerinnlogging, og sluttbrukerinnlogging med autorisering hentet fra autoritative kilder. Ansattporten kan også brukes med pseudonymisering av sluttbruker, men med autoriseringsinformasjon fra autoritative kilder.

Ansattportens tekniske dokumentasjon er tilgjengelig på produksiden på [Samarbeidsportalen \(Digdir Docs\)](#).

3.1.2 Prinsipper for bruk

Prinsippene for bruk av Ansattporten er de samme som for ID-porten, se pkt. 2.1.2.

3.2 Finansiering

[Kostnadsmodell for Ansattporten](#) er tilgjengelig på Samarbeidsportalen.

3.3 Digdirs ansvar

3.3.1 Tjenestenivå

Driftsperioden for Ansattporten er 24 timer/7 dager i uken/365 dager i året.

Måleperioden for alle tjenester er månedlig (per kalendermåned).

Tilgjengelighetskravet gjelder for Ansattporten sluttbrukerløsning, ikke mot Altinn, AA-registeret eller andre autoritative kilder.

Beskrivelse	Krav
Tilgjengelighet til Ansattporten (sluttbrukerløsningen)	99,90 %

Responstid	Mindre enn 3 sekunder for 90 % av forespørsleene i gjennomsnitt
Ytelse	100 000 innlogginger i timen

3.4 Behandling av personopplysninger

3.4.1 Digdirs ansvar

Digdir er databehandler for behandling av personopplysninger i Ansattporten i forbindelse med autentisering og oppslag i autoritative kilder.

Ved autentisering lagrer og videreformidler Digdir sluttbrukers fødselsnummer, sikkerhetsnivå for gjennomført autentisering, sluttbrukers språkvalg og hvilken e-ID som ble benyttet for autentiseringen. Det blir også lagret autorisasjonsinformasjon om potensielle og valgte virksomhet som sluttbruker representerer i forespurte roller. Digitaliseringsdirektoratet lagrer opplysningene om autentisering i ett år.

3.4.2 Kundens ansvar

Kunden er behandlingsansvarlig for opplysninger om autentiseringsoperasjoner som er utlevert fra Ansattporten i forbindelse med autentisering og autorisasjon av sluttbrukere.

Kunden må ha lovlig grunnlag for behandling av personopplysninger i henhold til personopplysningsloven §1, jf. forordningen artikkel 6, og behandling av fødselsnummer i henhold til personopplysningsloven § 12. Kunden må ha lovlig grunnlag for å behandle opplysninger om representasjonsforhold mellom innbygger og virksomhet.

Kunden skal påse at det bare er ansatte med tjenstlige behov som har tilgang til de personopplysninger som utleveres fra Ansattporten.

4 Maskinporten

4.1 Om Maskinporten

Maskinporten sikrer korrekt tilgang til data i kommunikasjon mellom maskiner. Kunden kan definere hva andre virksomheter skal ha tilgang til, hvordan andre virksomheter skal kunne bruke tilgangen, og hvem som skal ha tilganger.

Mer informasjon om hva Maskinporten er og hvordan den fungerer er tilgjengelig på [Samarbeidsportalen](#).

4.1.1 Beskrivelse og funksjonalitet

Maskinportens tekniske dokumentasjon er tilgjengelig på Samarbidsportalen ([Digdir Docs](#)).

4.1.2 Prinsipper for bruk

Maskinporten er basert på at kundene selv konfigurerer løsningen ved hjelp av selvbetjeningsfunksjonalitet. Av sikkerhets- og integritetshensyn har Digitaliseringsdirektoratet ikke anledning til å manuelt tildele tilganger til API som tilhører tilbyder av data.

4.1.2.1 Tilbyder av data

Tilbyder av data skal ha rutiner for å administrere konsumenter som skal ha tilganger.

Tilbyder av data skal sikre at konsument som delegerer ansvaret for sin integrasjon forstår virkningen av sin delegering. For eksempel kan tilbyder av data sin avtale med konsument av data inneholde informasjon om at konsumenten kan delegerer sin tilgang videre til en leverandør, men at ansvaret fortsatt ligger hos konsument.

Tilbyder som åpner sine scope for utenlandske virksomheter med europeiske virksomhetssertifikater må selv vurdere og akseptere risikoen med dette før funksjonaliteten tas i bruk.

4.1.2.2 Konsument av data

Konsument av data skal følge gode prinsipper for tilgangsstyring, slik at kun personell og systemer med tjenstlig behov har tilgang til token fra maskinporten og data utlevert fra tilbyder av data. Konsument skal i samsvar med prinsipp om dataminimering sørge for at det ikke hentes ut eller lagres mer data enn nødvendig.

Konsument som bruker underleverandør for å få tilgang til API må sørge for å delegerer tilgang til underleverandøren. Konsument og underleverandør må ha avtaler som regulerer forholdet mellom dem.

4.2 Finansiering

[Kostnadsmodell for Maskinporten](#) er tilgjengelig på Samarbeidsportalen.

4.3. Tjenestenivå

Driftsperioden for ID-porten er 24 timer/7 dager i uken/365 dager i året. Måleperiode for alle tjenester og ytelser er månedlig (per kalendermåned).

Beskrivelse	Krav
Tilgjengelighet til maskinporten og selvbetjenings-API	99,90 %
Responstid	Mindre enn 1 sekund for 95 % av utstedelsene i gjennomsnitt
Ytelse	720 000 tokenutstedelser i timen for tjenesten totalt.

4.4 Behandling av personopplysninger

4.4.1 Digdirs ansvar

Digitaliseringsdirektoratet vil være databehandler for fødselsnummer og eventuell annen informasjon i tokenet som sammen med fødselsnummeret kan regnes som personopplysninger.

4.4.2 Kundens ansvar

API-tilbyder kan begrense tilgangen til data ved å kreve at konsument oppgir fødselsnummer i token for å hente ut informasjon. Ved utveksling av data vil bruk av personnummer i token gi lavere risiko for misbruk av token på avveie. Det vil også støtte opp om kravet til dataminimering i personopplysningsloven.

Både konsument av data og tilbyder av data må ha behandlingsgrunnlag for personopplysninger i token (personopplysningsloven art. 6, jf § 1) og saklig og nødvendig behov for behandling av fødselsnummer (personopplysningsloven § 12).

Innhold i token blir ikke loggført av Digitaliseringsdirektoratet.

5 Kontakt- og reservasjonsregisteret

5.1 Om Kontakt- og reservasjonsregisteret

Kontakt- og reservasjonsregisteret (KRR) er et register som inneholder innbyggerne sin digitale kontaktinformasjon.

Kontakt- og reservasjonsregisteret benyttes i forbindelse med saksbehandling og utføring av forvaltningsoppgaver for øvrig, og skal benyttes til varsling av enkeltvedtak o.l. jf. eForvaltningsforskriften § 8 og 29.

Mer informasjon om hva KRR er, innhold i registeret, retningslinjer og prinsipper for bruk med mer er tilgjengelig på [Samarbeidsportalen](#).

5.1.1 Beskrivelse og funksjonalitet

Kontaktregisterets tekniske dokumentasjon er tilgjengelig på Samarbeidsportalen ([Digdir Docs](#)).

5.1.2 Prinsipper for bruk

- I eForvaltningsforskriften (FOR-2004-06-25-988) reguleres register over digital kontaktinformasjon og reservasjon med tilhørende infrastruktur.
- Opplysninger i register over digital kontaktinformasjon og reservasjon kan benyttes i forbindelse med saksbehandling og utføring av forvaltningsoppgaver for øvrig, og skal benyttes til varsling etter § 8 tredje ledd, jf § 29 andre ledd.
- Etter eForvaltningsforskriften § 8 kan et forvaltningsorgan benytte elektronisk kommunikasjon når det henvender seg til andre. Etter § 9 kan innbyggere reservere seg mot å motta følgende meddelelser elektronisk fra forvaltningen:
 - enkeltvedtak
 - forhåndsvarsel etter forvaltningsloven § 16
 - andre meldinger som har betydning for vedkommendes rettsstilling eller for behandlingen av saken
 - meldinger som det av andre grunner er av særlig betydning å sikre at vedkommende mottar
- Bruk av kontakt- og reservasjonsregisteret er regulert i [Retningslinjer for bruk av Kontakt- og reservasjonsregisteret](#).
- For å hente ut informasjon fra Kontakt- og reservasjonsregisteret, må kunden kjenne fødselsnummeret til mottaker av brevet. Skattedirektoratet har bestemt at *«Offentlige myndigheter kan [...] få online tilgang med treffliste til Det sentrale folkeregister for å sikre entydig identitet på borgeren i forbindelse med elektronisk kommunikasjon.»*

- Kunden må selv vurdere behandlingsgrunnlag etter personopplysningsloven §1, jf. forordningen artikkel 6.
- Prinsipp for oppslag for å ivareta ferske data og akseptabel belastning på sentrale tjenester er omtalt i Digdir docs.

5.2 Finansiering

[Kostnadsmodell for Kontakt- og reservasjonsregisteret](#) er tilgjengelig på Samarbeidsportalen.

5.3 Digdirs ansvar

5.3.1 Tjenestenivå

Driftsperioden for kontakt- og reservasjonsregisteret er 24 timer/7 dager i uken/365 dager i året. Måleperiode for alle tjenester og ytelser er månedlig (per kalendermåned).

Tilgjengeliget for REST-grensesnitt:

Beskrivelse	Krav
Tilgjengelighet til kontakt- og reservasjonsregisteret	99,90 %
Responstid for oppslag av én innbygger*	Mindre enn 0,5 sekunder for 99% av forespørslene i gjennomsnitt og mindre enn 0,25 sekunder for 95% av forespørslene i gjennomsnitt.
Responstid for samtidig oppslag av opptil tusen innbyggere*	Mindre enn 4 sekunder for 99% av forespørslene i gjennomsnitt.*

* Fra forespørsler er mottatt i eksternt API til respons er sendt.

5.4 Behandling av personopplysninger

5.4.1 Digdirs ansvar

Digitaliseringsdirektoratet er behandlingsansvarlig for kontakt- og reservasjonsregisteret og utleveringen av opplysninger til kunde. Behandlingen er hjemlet i eForvaltningsforskriften § 30.

Digitaliseringsdirektoratet logger kundens oppslag mot registeret, og endringer sluttbruker gjør i registeret. Loggene oppbevares i 1 år.

5.4.2 Kundens ansvar

Kunden er behandlingsansvarlig for bruk av opplysningene som er utlevert fra registeret. Kunden må selv sørge for å ha behandlingsgrunnlag for bruk av opplysningene.

Kunden skal logge behandling av registerinformasjon i overensstemmelse med de krav som følger av personopplysningsloven

6 Digital postkasse til innbyggere

6.1 Om digital postkasse

Digital postkasse til innbyggere er en fellesløsning for å sende post digitalt til innbyggernes valgte postkasse. Den enkelte innbygger velger selv en digital postkasse og hvilken leverandør de vil inngå avtale med, blant leverandørene som Digdir har avtale med.

Tjenesten omfatter flere tekniske løsninger; aksesspunkt som formidler Peppol eGovernment meldinger, flere postkasser innbygger kan velge mellom og en tjeneste for utskrift og forsendelse av post på papir, se kapittel 5.4.5.

Bruk av Digital postkasse til innbyggere forutsetter at kunden kan gjøre oppslag i Kontakt- og reservasjonsregisteret. Kunden må integreres mot oppslagstjenesten, senest samtidig med at kunden tar i bruk digital postkasse.

Mer informasjon om hva digital postkasse er, og hvordan den fungerer er tilgjengelig på [Samarbeidsportalen](#).

6.1.1 Beskrivelse og funksjonalitet

Digital postkasse sin tekniske funksjonalitet er tilgjengelig på Samarbeidsportalen ([Digdir docs](#)).

6.1.2 Prinsipper for bruk

Bruk av Digital postkasse til innbyggere skal bygge på prinsipper om brukervennlighet, trygghet og valgfrihet.

- Innbygger kan fritt velge blant tilknyttede postkasser. Mottak og lagring av digital post etter disse bruksvilkårene er gratis for innbygger.
- Pålogging til post sendt i samsvar med disse bruksvilkårene skjer ved bruk av ID-porten, som er gratis for innbygger.

- Kunden skal i sin portalløsning (fra sin egen nettsjeneste) lenke til Kontakt- og reservasjonsregisteret, slik at innbygger kan oppdatere sin digitale kontaktinformasjon i det felles registeret.
- Innbygger har rett til å reservere seg mot å få vedtak og andre viktige brev digitalt, etter eForvaltningsforskriften §9. Kunden skal i sin portalløsning lenke til Digdirs tjeneste for reservasjon mot kommunikasjon på nett.
- Kunden skal sørge for at meldingene som sendes er i tråd med regelverket for universell utforming, jf. «Forskrift om universell utforming av informasjons- og kommunikasjonsteknologiske (IKT)-løsninger».
- Varslingsplikten etter eForvaltningsforskriften § 8 påligger kunden
- Alle postkasseleverandører som er tilknyttet løsningen tilbyr sikker lagring av meldinger mottatt etter disse bruksvilkårene, så lenge innbygger ønsker.
- Kunden kan ikke reservere sine tjenester mot noen av postkasseleverandørene.

6.2 Finansiering

[Kostnadsmodellen for Digital postkasse til innbyggere](#) er tilgjengelig på Samarbeidsportalen.

6.3 Digdirs ansvar

6.3.1 Tjenestenivå

Driftsperioden for digital post er 24 timer/7 dager i uken/365 dager i året. Måleperiode er månedlig (per kalendermåned). Kvitteringer vil bli levert innen 1 time. Løsningen har en tilgjengelighet på 99,50 %

6.4 Behandling av personopplysninger

6.4.1 Digdirs ansvar

Digdir opptre som *databehandler* for kunden når Digdir, i henhold til disse bruksvilkårene, formidler tilgang til tjenester fra aksesspunktleverandør og postkasseleverandører og følger opp disse i henhold til avtaler mellom Digdir og leverandørene. Tietoevry Norway AS, Posten Norge AS og e-Boks A/S er i denne sammenheng underleverandører til Digdir. Digdir kan engasjere andre

underleverandører på tilsvarende vilkår som gjelder for Tietoevry Norway AS, Posten Norge AS og e-Boks A/S.

Digdir kan ikke behandle personopplysningene på annen måte enn det som er nødvendig for å utføre sine oppgaver i henhold til disse bruksvilkårene, herunder å følge opp at digital post som sendes fra kunden formidles i henhold til avtale med underleverandørene.

Det skal føres logg over opplysninger om digital post som sendes på vegne av kunden. Loggen kan inneholde de opplysninger som er nødvendig for å avklare eventuelle feilsituasjoner og når posten ble mottatt av henholdsvis aksesspunktleverandør og postkasseleverandør. Innholdet i loggene er nærmere beskrevet i avtalene med underleverandørene. Loggen skal oppbevares i maksimalt 24 måneder etter at posten er levert til postkasseleverandøren eller feilmelding er sendt til kunden.

Digdir skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger, se kapittel 1.8. Sikkerhetsdokumentasjon kan gjøres tilgjengelig for kunden på forespørsel.

Kunden kan når som helst pålegge Digdir å stanse behandlingen av personopplysninger på vegne av kunden. Med mindre annet fremgår av pålegget fra kunden, skal Digdir gjennomføre sending av digital post som er påbegynt før pålegget ble mottatt. Med mindre kunden pålegger Digdir å slette opplysningene om sending av post som er lagret i underleverandørenes logger på vegne av kunden, skal loggene oppbevares frem til det tidspunkt de ville blitt slettet dersom databehandleroppdraget ikke var blitt avsluttet, jf. fjerde avsnitt ovenfor.

6.4.2 Kundens ansvar

Kunden er *behandlingsansvarlig* for personopplysninger i brev som kunden sender til digital postkasse frem til disse er gjort tilgjengelig for innbygger i innbyggers postkasse. Det er kunden selv som bestemmer hvilke personopplysninger brevene inneholder. Logger hos Digdir og underleverandører inneholder adressen til innbyggers digitale postkasseadresse, meldings-ID og avsender.

Etter at brev er gjort tilgjengelig for innbygger, behandles personopplysninger i samsvar med de til enhver tid gjeldende bruksvilkår mellom postkasseleverandør og innbygger, der postkasseleverandør er behandlingsansvarlig.

Kunden kan benytte andre aksesspunktleverandører enn Tietoevry Norway AS som beskrevet tidligere. Ved bruk av andre leverandører vil disse bruksvilkårene ikke omfatte eller regulere forholdet mellom kunde og Digdir før melding er kommet frem til Posten Norge AS sitt aksesspunkt. Behandling av personopplysninger før dette må reguleres i avtalen mellom kunde og aksesspunktleverandør.

7 eSignering

7.1 Om eSignering

eSignering er en felles signeringstjeneste for offentlige virksomheter. Digitaliseringsdirektoratet er sentralforvalter for eSignering.

Mer informasjon om hva eSignering er, og hvordan den fungerer er tilgjengelig på [Samarbeidsportalen](#)

7.1.1 Beskrivelse og funksjonalitet

eSignering sin tekniske dokumentasjon er tilgjengelig på Samarbeidsportalen ([Digdir Docs](#)).

7.1.1.1 Varsling av innbygger

Varslingsplikten etter eForvaltningsforskriften § 8 ligger hos kunden. Kunden kan ved oppretting av signeringsoppdrag bestemme at innbygger skal varsles per SMS eller e-post om at det er foreliggende dokument til signering.

7.1.1.2 Leverandør

eSignering blir driftet og utviklet av Posten Norge AS.

7.1.2 Prinsipper for bruk

Pålogging og signering i eSignering skjer ved bruk av ID-porten, som er gratis for innbygger.

Kunden er ansvarlig for innholdet i dokument som skal signeres, og for utformingen av alt tekstlig i forbindelse med oppretting og utsending av signeringsoppdrag gjennom eSignering.

Kunden er ansvarlig for at ferdig signerte oppdrag hentes ut og arkiveres i henhold til lover og krav for arkivering av dokument.

7.2 Finansiering

[Kostnadsmodell for eSignering](#) er tilgjengelig på Samarbeidsportalen.

7.3 Digdirs ansvar

7.3.1 Tjenestenivå

Digitaliseringsdirektoratet skal følge opp at tjenester til eSignering levert av eksterne leverandører holder det tjenestenivå som fremgår av de til enhver tid gjeldende avtaler Digitaliseringsdirektoratet har med disse leverandørene.

Driftsperioden for eSignering er 24 timer/7 dager i uken/365 dager i året. Måleperiode for alle tjenester og ytelser er månedlig (per kalendermåned). Løsningen har en tilgjengelighet på 99,50 %.

7.4 Behandling av personopplysninger

7.4.1 Digdirs ansvar

Digitaliseringsdirektoratet opptrer som databehandler for kunden når Digdir, i henhold til disse bruksvilkårene, administrerer tilgang til signeringstjenesten og følger opp tjenesten i henhold til avtaler mellom Digitaliseringsdirektoratet og leverandør av signeringstjenesten. Posten Norge AS er i denne sammenheng underleverandør til Digitaliseringsdirektoratet. Digitaliseringsdirektoratet kan engasjere andre underleverandører enn Posten Norge AS på samme vilkår.

Det føres logg over signeringsoppdrag som behandles på vegne av kunden. Leverandøren fører logg over hendelser som har betydning for sikkerheten, denne lagres i to år. ID-porten logger autentiseringstransaksjoner i eSignering i 13 måneder. Leverandør av sertifikatet innbygger bruker lagrer valideringstransaksjoner i 10 år. Loggene inneholder de opplysninger som er nødvendige for å sikre konfidensialitet, integritet og uavviselighet, og for å avklare eventuelle feilsituasjoner. Loggene er beskrevet i dokumentasjon i Samarbeidsportalen.

7.4.2 Kundens ansvar

Kunden er behandlingsansvarlig for personopplysninger som kunden overfører til signeringstjenesten. Kunden er ikke behandlingsansvarlig for kopi av signert dokument som er sendt til sluttbrukers digitale postkasse eller som sluttbruker har lastet ned.

Kunden kan når som helst pålegge Digitaliseringsdirektoratet å stanse behandlingen av personopplysninger på vegne av kunden. Med mindre kunden pålegger Digitaliseringsdirektoratet å slette opplysningene om signering som er lagret i underleverandørens logger på vegne av kunden, skal loggene oppbevares frem til det

tidspunkt de ville blitt slettet dersom databehandleroppdraget ikke var blitt avsluttet, jf. tredje avsnitt ovenfor.

8 eFormidling

8.1 Om eFormidling

eFormidling er en sikker, samordnet og effektiv meldingsutveksling. Integrasjonspunkt for eFormidling (heretter Integrasjonspunktet) er en infrastrukturkomponent for sikker utveksling av dokumenter og meldinger med strukturert informasjon mellom offentlige etater, innbyggere og private virksomheter.

8.1.1 Beskrivelse og funksjonalitet

eFormidling sin tekniske dokumentasjon er tilgjengelig på Samarbeidsportalen ([Digdir docs](#))

8.1.2 Prinsipper for bruk

Kunden er selv ansvarlig for drift av sitt eget integrasjonspunkt. Kunden må tilrettelegge for automatisk oppdatering av integrasjonspunktet, eller selv ta ansvar for at dette til enhver tid er oppdatert.

- Kunden har ansvar for innhold i meldinger og at meldinger er riktig adressert.
- Kunden er ansvarlig for å følge opp hendelser varslet fra Digitaliseringsdirektoratet.
- Kunden er selv ansvarlig for risikovurdering av egen bruk av løsningen.

8.2 Finansiering

[Kostnadsmodell for eFormidling](#) er tilgjengelig på Samarbeidsportalen.

8.3 Digdirs ansvar

8.3.1 Tjenestenivå

Driftsperioden for Integrasjonspunktet er 24 timer/7 dager i uken/365 dager i året. Måleperiode for alle tjenester og ytelser er månedlig (per kalendermåned).

Løsningen har en tilgjengelighet på 99,90 %. Dette gjelder driftsplattformen til eFormidling. Tilgjengelighet for ELMA, FIKS og Enhetsregisteret i Brønnøysund er ikke en del av denne beregningen.

Kundens lokale integrasjonspunkt følger tjenestenivået for systemet som det er integrert med. Tjenestenivå på kundens lokale integrasjonspunkt reguleres av kunden eller evneutell tredjepart denne har avtale med for drift av lokalt integrasjonspunkt.

8.4 Behandling av personopplysninger

8.4.1 Digdirs ansvar

Digitaliseringsdirektoratet opptrer som *databehandler* for kunden når Digitaliseringsdirektoratet, i henhold til disse bruksvilkårene, formidler tilgang til tjenester fra våre underleverandører og følger opp disse i henhold til avtaler mellom Digitaliseringsdirektoratet og leverandørene. Digitaliseringsdirektoratet har ansvar for at integrasjonspunktets utforming er i tråd med denne avtalen.

Digitaliseringsdirektoratet kan ikke behandle personopplysningene på annen måte enn det som er nødvendig for å utføre sine oppgaver i henhold til disse bruksvilkårene, herunder å følge opp at meldinger som sendes fra kunden formidles i henhold til avtale med underleverandørene.

Digitaliseringsdirektoratet kan ikke behandle de sentraliserte loggopplysningene på annen måte enn det som er nødvendig for å utføre sine oppgaver i henhold til disse bruksvilkårene, herunder å følge opp at meldinger som sendes fra kunden formidles i henhold til avtale med underleverandørene. De sentralt lagrede fellesloggene skal ikke inneholde personopplysninger. For adressering til privatpersoner blir personnummer aidentifisert. Fødselsnummer skal bare lagres lokalt hos Kunde, og blir ikke sendt til sentrallogg. Sentralloggen skal oppbevares i 24 måneder etter melding er håndtert av integrasjonspunkt.

Integrasjonspunktet slår opp i Kontakt- og reservasjonsregisteret, og når brevet er adressert, blir det pakket med unik meldingsID før sending. Formidleren har ikke mulighet til å se fødselsnummer.

8.4.2 Kundens ansvar

Kunden er *behandlingsansvarlig* for personopplysninger i meldinger som kunden sender til integrasjonspunktet frem til disse er mottatt av offentlig mottakers integrasjonspunkt. Det er kunden selv som bestemmer hvilke personopplysninger meldingene inneholder. Kunden er ansvarlig for sikkerheten i eget system og er selv ansvarlig for å ha databehandleravtale med sin meldingsformidler.

Ved sending av meldinger til *Digital postkasse til innbyggere* (Digitaliseringsdirektoratet) og *Digital postkasse for virksomheter* (Digitaliseringsdirektoratet) og *FIKS (KS)*, vil bruksvilkår eller avtale for de enkelte løsningene også omfatte databehandleravtale.

Kunden kan når som helst pålegge Digitaliseringsdirektoratet å stanse behandlingen av personopplysninger på vegne av kunden. Med mindre annet fremgår av pålegget fra kunden, skal Digitaliseringsdirektoratet gjennomføre sending av meldinger som er påbegynt før pålegget ble mottatt. Med mindre kunden pålegger Digitaliseringsdirektoratet å slette opplysningene om sending av post som er lagret i Digitaliseringsdirektoratet eller underleverandørenes logger på vegne av kunden, skal loggene oppbevares frem til det tidspunkt de ville blitt slettet dersom databehandleroppdraget ikke var blitt avsluttet, jf. fjerde avsnitt ovenfor.

9 Digital post til virksomheter

9.1 Om Digital post til virksomheter

Digital post til virksomheter (DPV) er et ferdig sett meldingstjenester i Altinn-løsningen, som kan tas i bruk av kunder uten at det må utføres tjenesteutvikling.

9.1.1 Beskrivelse og funksjonalitet

Tjenesten Digital post til virksomheter i Altinn dekker behov for forsendelse, statusoppdatering, varslinger og gjentatt varsling om meldinger som ikke er åpnet. Det er også mulighet for:

- Å sende post på vegne av annen virksomhet. En mottaker vil da kunne se hvem som er den faktiske avsender, ikke den tekniske avsender. Altinn loggfører både hvem som er teknisk- og hvem som er faktisk avsender.
- Styrt brukertilgang til post via rollen «Post/Arkiv»
- Å lese status på inntil 10.000 meldinger av gangen

9.1.1.1 Meldingskategori for ordinær post

Digital post til virksomheter består av flere fellestjenester som alle kunder kan benytte uten noen form for tjenesteutvikling på forhånd. Det er foreløpig utviklet 10 ulike meldingstjenester innenfor ulike tjenesteområder, inkludert en generell kategori:

- Post fra det offentlige innenfor administrasjon
- Post fra det offentlige innenfor plan, bygg og geodata
- Post fra det offentlige innenfor helse, sosial og omsorg
- Post fra det offentlige innenfor oppvekst og utdanning
- Post fra det offentlige innenfor kultur, idrett og fritid
- Post fra det offentlige innenfor trafikk, reiser og samferdsel
- Post fra det offentlige innenfor natur og miljø
- Post fra det offentlige innenfor næringsutvikling
- Post fra det offentlige innenfor skatter og avgifter
- Post fra det offentlige innenfor tekniske tjenester

9.1.1.2 Hvem får tilgang til meldinger som sendes som ordinær post?

Alle disse meldingstjenestene er knyttet opp til rollen “Post/Arkiv”. Nøkkelroller for virksomheten i Enhetsregisteret får rollen Post/Arkiv (les mer om rollen [her](#)) og dermed automatisk tilgang til alle meldinger. De 10 ulike meldingstjenestene kan tilgangsstyres på tre nivå; gjennom rollen Post/arkiv, ved å gi tilgang til post av en bestemt kategori (eks post fra det offentlige innenfor administrasjon) eller ved å videresende meldinger enkeltvis.

9.1.1.2 Meldingskategori for post med sensitiv og/eller taushetsbelagt informasjon

Skal kunde sende post til en virksomhet som inneholder sensitiv og/eller taushetsbelagt informasjon, er det viktig å legge til rette for at innsyn i innholdet begrenses til de personer/roller i virksomheten som har tjenstlig behov. Avsender må i slike tilfeller vurdere om det er riktig at nøkkelroller fra enhetsregisteret automatisk får/må ha tilgang til meldingen (se pkt 8.1.1.1.1 “Hvem får tilgang til meldinger som sendes som ordinær post”). Hvis det ikke er meningen at de skal ha slik tilgang, kan IKKE meldingskategorier for ordinær post benyttes.

Det er opprettet tre DPV-tjenester som støtter mottak av post med sensitiv og/eller taushetsbelagt informasjon:

- Taushetsbelagt post fra det offentlige innenfor helse, sosial og omsorg
- Taushetsbelagt post fra det offentlige innenfor oppvekst og utdanning
- Taushetsbelagt post fra det offentlige innenfor administrasjon

På forespørsel kan Altinn opprette flere kategorier for sending av sensitiv og/eller taushetsbelagt informasjon.

9.1.1.3 Hvem får tilgang til meldinger med sensitiv og/eller taushetsbelagt informasjon?

I utgangspunktet får ingen i organisasjonen tilgang til disse meldingene.

Hovedadministrator for virksomheten har rett til å administrere tilgang til denne type meldinger, og delegere til de ansatte som behandler slike typer post. Altinn har laget en [beskrivelse](#) av hvordan virksomhetene bør håndtere tilgangsstyringen i slike tilfeller.

9.1.1.4 Varsling til virksomheter som mottar meldinger med sensitiv og/eller taushetsbelagt informasjon

Det er viktig at avsender benytter varsling knyttet til meldinger for å sikre at virksomheten oppfatter at en melding som ingen i utgangspunktet har tilgang til er mottatt. Varslelet bør informere om at det gjennom tilgangsstyring er nødvendig å sikre at riktig ansatt i virksomheten får tilgang til posten. Avsender bør, i en oppstartsfase, gjennom sjekk av status på meldingen sikre en oppfølging av de virksomhetene som ikke åpner mottatt post.

9.1.2 Leverandør

DPV driftes av Basefarm og forvaltes av Accenture.

9.1.3 Prinsipper for bruk

Før Digital post til virksomheter tas i bruk, må den enkelte kunde utføre en risikovurdering om slike tilganger imøtekommer avsenders behov for tilgangsstyring- og kontroll, herunder bestemmelser som regulerer taushetsplikt.

9.2 Finansiering

[Kostnadsmodell for Digital post til virksomheter](#) og varsling på SMS er tilgjengelig på Samarbeidsportalen.

9.3 Digdirs ansvar

9.3.1 Tjenestenivå

Måleperiode for alle tjenester og ytelser er månedlig (per kalendermåned).

Driftsperioden for Digital post til virksomheter er 24 timer/7 dager i uken/365 dager i året. Løsningen har en tilgjengelighet på 99,8 % i driftstiden.

9.4 Behandling av personopplysninger

9.4.1 Digdirs ansvar

Digdir er databehandler på vegne av den enkelte kunde ved bruk av tjenesten Digital post til virksomheter

Digdir er behandlingsansvarlig for fellesfunksjonalitet i Altinn-løsningen, herunder:

Lagring av grunndata:

- Det sentrale folkeregister (DSF) Utdrag fra Folkeregisteret i henhold til tillatelse fra Skattedirektoratet: Navn, fødsels- og D-nummer, adresse.
- Kontakt- og reservasjonsregisteret (KRR): Navn, fødsels- og D-nummer, e-postadresse og mobilnummer
- Enhetsregisteret (ER): Navn, fødsels- og D-nummer, adresse, roller i ER, varslingsadresse (epostadresse og mobilnummer).

Lagring av opplysninger oppgitt av bruker eller generert av systemet: Lagring av personopplysninger for å kunne utføre korrekt kontroll av autentisering og autorisasjon til data. Dette er fødselsnummer/D-nummer, navn, mobil, e-post, pinkoder, brukernavn, brukerID, roller og rettigheter til tjenester.

Digdir er forpliktet til å ivareta det ansvar for informasjonssikkerhet som følger av personopplysningslovens § 1, jf personvernforordningen artikkel 32.

Informasjonssikkerhet omfatter:

- Sikring av konfidensialitet; beskyttelse mot at uvedkommende får innsyn i opplysningene
- Sikring av integritet; beskyttelse mot utilsiktet endring av opplysningene
- Sikring av tilgjengelighet; sørge for at tilstrekkelige og relevante opplysninger er til stede.

Digdir plikter for øvrig å etterkomme krav til databehandlingen som ellers følger av relevante lover og forskrifter. Databehandlingen vil i tillegg utføres i henhold til gjeldende systemdokumentasjon og øvrige rutinebeskrivelser for tjenesten. Dokumentasjon på

dette skal på forespørsel være tilgjengelig for kunden DPV, Datatilsynet og Personvernemnda.

9.4.2 Kundens ansvar

Kunden DPV er behandlingsansvarlig for personopplysninger som behandles i tjenesten, og kundens egne systemer ved forespørsler på informasjon fra Altinn, uavhengig av hvilket teknisk grensesnitt og funksjonalitet som benyttes i løsningen. Kunden DPV innestår for å ha rettslig grunnlag etter personopplysningsloven for bruken av disse personopplysningene, jf. personopplysningsloven § 1, jf. personvernforordningen artikkel 6 nr 1 e) og artikkel 9 og 10, og ha oversikt over hvilke personopplysninger som overføres ved bruk av tjenesten DPV. Kunden DPV skal kunne godtgjøre det foreligger tillatelse fra Skattedirektoratet til å motta ønskede folkeregisteropplysninger. Kunden DPV/avsender er ansvarlig for feilsendte meldinger, herunder oppfølging av sletting, informasjon til berørte og varsling til Datatilsynet.