Bruksvilkår for offentlige kunder

Digitaliseringsdirektoratet (Digdir) har samlet sine bruksvilkår for fellesløsningene i et og samme dokument for fellesløsningene, utenom eInnsyn som har sitt eget bruksvilkår. Det vil si at offentlige kunder bare signerer et dokument for å ta i bruk fellesløsningene. Bruksvilkåret er strukturert slik at det først kommer en overordnet del for fellesløsningene, mens hver fellesløsning har hvert sitt kapittel. Kapittelet er ikke gjeldende for virksomheten før fellesløsningen er tatt i bruk. Versjon 1.7 er gjeldende fra 06.01.2022.

[1. Generelle 1](#_Toc89690404)

[2. ID-porten 7](#_Toc89690405)

[3. Maskinporten 10](#_Toc89690406)

[4. Kontakt- og reservasjonsregisteret 12](#_Toc89690407)

[5. Digital postkasse til innbyggere 15](#_Toc89690408)

[6. eSignering 19](#_Toc89690409)

[7. eFormidling 21](#_Toc89690410)

[8. Digital post til virksomheter 23](#_Toc89690411)

# 1. Generelle

1.1 Om bruksvilkår

Digitaliseringsdirektoratet forvalter flere nasjonale fellesløsninger som offentlige virksomheter (heretter benevnt som «Kunde») skal[[1]](https://samarbeid.difi.no/bruksvilkar/bruksvilkar-difis-felleslosninger#_ftn1) eller kan benytte for å tilby bedre tjenester og effektivisere driften.

Disse bruksvilkårene for offentlige virksomheter gjelder for alle fellesløsningene. Vilkårene er bygget opp med ett kapittel som gjelder alle løsninger og deretter ett kapittel per løsning. eInnsyn har [egne bruksvilkår](https://samarbeid.digdir.no/einnsyn/bruksvilkar-einnsyn/71). Digitaliseringsdirektoratet er forpliktet til å levere i samsvar med bruksvilkårene når bemyndiget person hos kunden 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 statsstøtteregelverket. 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.

Kunden betaler selv for[tilleggstjenester](https://samarbeid.digdir.no/digital-postkasse/tilleggstjenester-og-priser/122) som bestilles i samsvar med gjeldende prisliste.

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

1.4 Samarbeid

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

*1.4.1 Samarbeidsportalen*

[Samarbeidsportalen](https://samarbeid.digdir.no/%22%20%5Ct%20%22_blank) er den primære informasjons- og varslingskanalen fra Digitaliseringsdirektoratet om fellesløsningene. Vi forvalter og drifter Samarbeidsportalen. Du finner løsningsinformasjon, teknisk dokumentasjon og stegvis guide for hvordan ta i bruk de ulike fellesløsningene, statistikk for bruk og drift av fellesløsningene, status og driftsmeldinger, utviklingsplaner osv.

Kunder som godtar bruksvilkår, får tilgang til [Min profil](https://minside-samarbeid.digdir.no/) som gir tilgang til selvbetjening og vedlikehold av virksomhetsinformasjon i våre systemer.

Kunden har selv ansvar for å holde listen over kontaktpunkter i egen virksomhet og annen nødvendig informasjon om egne tjenester oppdatert i Min profil. Spesielt viktig er varslingspunkt for kundens tjenester, da dette varslingspunktet vil motta varsler fra Digitaliseringsdirektoratet ved kritiske og alvorlige hendelser.

*1.4.2 Styringsråd*

Styringsrådet er et rådgivende organ for Digitaliseringsdirektoratet og skal særlig behandle viktige saker som gjelder fellesløsningene. [Mandat for styringsrådet](https://samarbeid.digdir.no/digital-postkasse/mandat-styringsradet-digdirs-digitale-felleslosninger/128) er tilgjengelig på Samarbeidsportalen.

*1.4.3 Produktråd*

Ved behov kan styringsrådet og Digdir opprette produktråd for Digdirs produkter eller grupper av produkter. Produktrådene kan være permanente eller for en periode, og rapporterer til styringsrådet. [Mandat for produktrådet](https://samarbeid.digdir.no/1054) er tilgjengelig på Samarbeidsportalen.

*1.4.4 Brukerråd*

Brukerrådet skal diskutere status, endringsønsker og videreutviklingsprosjekter for fellesløsningene, samt annet av relevans for kundenes bruk av fellesløsningene. [Mandat for brukerrådet](https://samarbeid.digdir.no/digital-postkasse/mandat-brukerradet-digdirs-digitale-felleslosninger/129)er tilgjengelig på samarbeidsportalen.

*1.4.5 Integrasjons- og sikkerhetsforum*

Integrasjons- og sikkerhetsforumet skal bidra til å holde integrasjons- og sikkerhetsansvarlig hos kundene oppdatert på tekniske forhold ved fellesløsningene. [Mandat for integrasjons- og sikkerhetsforum](https://samarbeid.digdir.no/eformidling/mandat-integrasjons-og-sikkerhetsforum/1020) er tilgjengelig på samarbeidsportalen.

*1.4.6 Brukerstøtteforum*

Brukerstøtteforum skal bidra til å effektivisere og koordinere brukerstøtten overfor sluttbruker og er et forum for informasjons- og erfaringsutveksling mellom Digitaliseringsdirektoratet og kundenes brukerstøttefunksjoner. [Mandat for brukerstøtteforumet](https://samarbeid.digdir.no/digital-postkasse/mandat-brukerstotteforum-digdirs-digitale-felleslosninger/130) er tilgjengelig på Samarbeidsportalen.

1.5 Digdirs ansvar

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

Digitaliseringsdirektoratet 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 Planer og rapporter*

Digitaliseringsdirektoratet skal sørge for at kunden får god informasjon om aktuelle saker, tema og aktiviteter knyttet til fellesløsningene. Informasjon presenteres på Samarbeidsportalen. I tillegg vil det bli gitt informasjon ved møter i de fora som er beskrevet i kapittel 1.4.

Digitaliseringsdirektoratet vil utarbeide følgende planer og rapporter:

1.5.1.1 Årsplan

På bakgrunn av innspill fra kundene skal Digitaliseringsdirektoratet utarbeide og holde oppdatert en årsplan. I årsplanen skal høyvolumperioder, kritiske perioder og andre aktiviteter som krever særskilt oppmerksomhet i forvaltningen av fellesløsningene, inngå. Årsplanen er tilgjengelig på Samarbeidsportalen.

1.5.1.2 Leveranseplan

Digitaliseringsdirektoratet skal utarbeide en leveranseplan som gir en oversikt over leveransene som er planlagt for fellesløsningene. Leveranseplanen viser planlagte nye versjoner og planlagt ny funksjonalitet for fellesløsningene. Leveranseplanen er tilgjengelig på Samarbeidsportalen.

1.5.1.3 Statistikk

Digitaliseringsdirektoratet skal månedlig utarbeide statistikk for fellesløsningene. Denne statistikken skal blant annet inneholde oversikt for bruk av fellesløsningene og tilgjengelighet og responstider i løsningene.

[Statistikken](https://samarbeid.digdir.no/statistikk/15) gjøres tilgjengelig på Samarbeidsportalen senest innen den 20. i påfølgende måned.

*1.5.2 Brukerstøtte*

Digitaliseringsdirektoratet drifter brukerstøtte og [hjelpesider for fellesløsningene](https://eid.difi.no/).

Ved henvendelser til brukerstøtte på telefon skal sluttbruker normalt få kontakt med en operatør innen 50 sekunder. Ved henvendelser på e-post skal sluttbrukeren normalt få svar innen en virkedag.

*1.5.3 Endringer*

Digitaliseringsdirektoratet 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.

1.5.3.1 Planlagte endringer

Gjennomføring av endringer skal være planlagt. I forbindelse med planlagte endringer skal det utarbeides risiko- og konsekvensanalyse av endringen, testprosedyrer for endringen samt en detaljert aktivitets- og tidsplan, med mindre dette vil være urimelig i forhold til endringens omfang og kompleksitet.

Digitaliseringsdirektoratet skal sørge for at kunden får informasjon om endringer som kan ha betydning for kunden. Dersom endringen påvirker kundene, skal det så langt som mulig tas hensyn til kritiske perioder for berørte kunder. Informasjon om planlagte endringer legges ut på Samarbeidsportalen.

Mindre endringer produksjonsettes fortløpende uten varsling.

 1.5.3.2 Hasteendringer

Dersom det inntreffer en hendelse som medfører at tjenestene som inngår som en del av fellesløsningene ikke kan driftes tilfredsstillende og i tråd med vilkårene, har Digitaliseringsdirektoratet rett og plikt til å gjennomføre hasteendringer for å gjenopprette ordinær drift.

Hvis hasteendring igangsettes uten risiko- og konsekvensvurdering, skal Digdir gjøre slik vurdering i ettertid. Resultater av risiko- og konsekvensvurderinger av hastendringer skal gjøres tilgjengelig på Samarbeidsportalen.

Hvis det avdekkes risiko for at det kan inntreffe hendelser som følge av hasteendringen, skal det gjennomføres tester for å avdekke dette, og relevante tiltak skal iverksettes.

*1.5.4 Vedlikehold og produksjonssettinger*

1.5.4.1 Planlagt vedlikehold

Vedlikeholdsvindu er avtalt tid der tjenesten kan være utilgjengelig, og som holdes utenfor ved beregning av tilgjengelighet. Vedlikehold for de ulike fellesløsningene er beskrevet nærmere i kapittelet for fellesløsningene.

1.5.4.2 Ekstraordinært vedlikehold

I forbindelse med forebyggende vedlikehold og kritisk feilretting, som ikke kan vente til vedlikeholdsvindu, skal Digdir varsle om vedlikehold utenfor vedlikeholdsvinduene. Varsling av ekstraordinært vedlikehold skal skje på Samarbeidsportalen.

1.5.4.3 Produksjonssettinger

Det gjennomføres hyppige leveranser i fellesløsningene som produksjonssetter utenfor vedlikeholdsvinduene. Dette er produksjonssettinger som ikke ventes å medføre nedetid. Varsling av produksjonssettinger skjer på Samarbeidsportalen.

*1.5.5 Hendelseshåndtering*

En hendelse er et ikke planlagt avbrudd eller reduksjon i kvalitet i en tjeneste eller fellesløsning.

Alle hendelser skal registreres hos Digdir og prioriteres etter kategoriene:

|  |  |
| --- | --- |
| Kategori  | Beskrivelse  |
| A – Kritisk  | En hendelse skal prioriteres som kritisk (A) dersom hendelsen medfører redusert konfidensialitet, integritet og/eller tilgjengelighet. Det finnes ikke en midlertidig løsning på hendelsen. I perioder med høyt volum senkes terskelen. Eller Kategorien kritisk (A) skal benyttes ved begrunnet mistanke om at personopplysninger har kommet på avveie, eller at personopplysninger har blitt slettet ved feil, uhell eller av uautoriserte. Eller Kategorien kritisk (A) skal benyttes dersom hendelsen anses som omdømmekritisk for Digitaliseringsdirektoratet.   |
| B – Alvorlig  | En hendelse skal prioriteres som alvorlig (B) dersom hendelsen medfører redusert tilgjengelighet, integritet og/eller tilgjengelighet. Det kan finnes en midlertidig løsning på den alvorlige hendelsen Eller Kategorien alvorlig (B) skal benyttes dersom personopplysningene til alle brukere er midlertidig utilgjengelige, uten at personopplysningene har kommet på avveie eller at de er endret ved feil, uhell eller uautoriserte. Eller Kategorien alvorlig skal benyttes dersom hendelsen anses å påvirke omdømme for Digitaliseringsdirektoratet.   |
| C –  Mindre alvorlig  | En hendelse skal prioriteres som mindre alvorlig (C) dersom det finnes en midlertidig løsning, og partene kan akseptere hendelsen i en kortere periode. Hendelsen kan løses innen gitte frister og har liten betydning for sluttbrukeren, kunde og/eller leverandør. Eller Kategorien mindre alvorlig (C) benyttes dersom hendelsen anses å påvirke omdømme i mindre grad.   |

1.5.5.1 Tilgjengelighet og responstid

Digitaliseringsdirektoratet 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 Digitaliseringsdirektoratet har identifisert og kategorisert en hendelse, blir den varslet på [Status Digdir](https://status.digdir.no/) som du når via Samarbeidsportalen.

Varsling til kundene skjer i henhold til gjeldende rutiner etter hendelsens kategori. Ved kritiske og alvorlige hendelser får kundens varslingspunkt for tjenesten varsel om hendelsen. Digitaliseringsdirektoratet informerer kundene om videre håndtering.

Fortløpende informasjon om hendelser gis på Status Digdir, som er hovedkanalen for varsling og kommunikasjon mot kundene.

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

1.5.5.3 Handtering av informasjon ved hendelser

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

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

Digitaliseringsdirektoratet 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*

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

1.6 Kundens ansvar

*1.6.1 Nye eller endrede tjenester*

Ved ny eller endret bruk av fellesløsningene, skal kunden informere Digitaliseringsdirektoratet minimum 1 måned før det er planlagt oppstart/endring av bruken. Kunden skal følge integrasjonskrav og etablerte standarder som fastsatt av Digitaliseringsdirektoratet. Kunden skal stille med nødvendig kompetanse og dekke egne kostnader for å gjennomføre eget arbeid i forbindelse med integrasjon mot fellesløsningene.

Kunden skal fortløpende informere Digitaliseringsdirektoratet om eventuelle endringer knyttet til kundens tjenester, herunder vesentlige endringer i estimert bruksvolum.

Dersom kunden planlegger endringer i egne systemer som vil påvirke integrasjonen mot fellesløsningene, skal kunden varsle Digitaliseringsdirektoratet i god tid. Partene skal i fellesskap planlegge hvordan endringene skal implementeres med sikte på minst mulig belastning og forstyrrelser for fellesløsningene.

Kunden må stille med nødvendig kompetanse for å gjennomføre eget arbeid i forbindelse med integrasjonen mot fellesløsningene. Kunden dekker selv alle kostnader ved integrasjon og gjennomføring av endringer i egne systemer.

*1.6.2 Kundens tjenester*

Kunden skal til enhver tid sørge for at Digitaliseringsdirektoratet har oversikt over kundens tjenester som er tilknyttet fellesløsningene, og varsle om eventuelle kritiske perioder.

*1.6.3 Varsling*

Kunden skal så raskt som praktisk mulig informere [Digitaliseringsdirektoratet](https://samarbeid.digdir.no/digital-postkasse/kontakt-oss/83) 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 Digitaliseringsdirektoratet koble tjenesten fra fellesløsningene inntil kunden har dokumentert overfor Digitaliseringsdirektoratet at hendelsen er utbedret, eller relevante tiltak er iverksatt.

*1.6.4 Varslingspunkt*

Kunden har ansvar for å holde listen over kontaktpunkter i egen virksomhet og annen nødvendig informasjon om egne tjenester oppdatert på [Min profil](https://minside-samarbeid.digdir.no/) på Samarbeidsportalen. Spesielt viktig er varslingspunkt for kundens tjenester, da dette varslingspunktet vil motta varsler fra Digitaliseringsdirektoratet ved kritiske og alvorlige hendelser.

*1.6.5 Krise- og beredskap*

Kunden skal ha nødvendige krise- og beredskapsplaner.

*1.6.6 Brukerstøtte*

Kunden skal ha nødvendig brukerstøtte overfor sluttbruker for egne tjenester.

1.7 Generelt om personopplysninger (databehandleravtale)

Digitaliseringsdirektoratet behandler på vegne av kunde personopplysninger på ulike måter og i ulik grad i de forskjellige fellesløsningene. I noen tilfeller er det Digitaliseringsdirektoratet som er databehandler og i noen tilfeller benytter Digitaliseringsdirektoratet databehandler for å behandle personopplysninger på vegner av kunden. Bruksvilkårene og tilknyttede dokumenter er Digitaliseringsdirektoratets 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. Digitaliseringsdirektoratet behandler personopplysninger i henhold til bruksvilkårene som nærmere definert i de enkelte kapittel nedenfor.
2. Digitaliseringsdirektoratet 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. Digitaliseringsdirektoratet treffer tiltak etter forordningen art 32.
4. I de tilfeller Digitaliseringsdirektoratet engasjerer databehandlere er dette beskrevet i kapittelet tilhørende de enkelte fellesløsningene. Kunden gir generell tillatelse til at Digitaliseringsdirektoratet kan endre databehandlere. Dette skal likevel skje i samsvar med bestemmelsene om endringer i bruksvilkårene definert i signeringsdokument punkt 7.
5. Digitaliseringsdirektoratet har rutiner for å oppfylle den registrertes rettigheter etter forordningen kap. III.
6. Digitaliseringsdirektoratet bistår med oppfylling av plikter etter forordningen art 32-36.
7. Sletting og tilbakelevering er regulert i den enkelte fellesløsnings kapittel.
8. Se punkt 1.8 nedenfor.

1.8 Innsyn og revisjon

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

Digitaliseringsdirektoratet 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 Digitaliseringsdirektoratet 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 et samlebegrep for offentlig sektors fellesløsninger for identitetshåndtering og bruk av e-ID. Bak de funksjonelle løsningene i ID-porten ligger det flere tekniske løsninger. ID-porten omfatter også avtaler som er inngått av Digdir for levering av felles e-ID-løsninger til det offentlige, herunder tjenester som kan integreres direkte med den enkelte kunde.

Offentlige e-ID-er og de e-ID-er Digdir til enhver tid har avtale med, kan benyttes til elektronisk identitetshåndtering gjennom ID-porten.

Digdir er avtalepart overfor eksterne e-ID-leverandører, og gjennom avtalen med Digdir kan kunden benytte leverandørenes e-ID-er i ID-porten.

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

* MinID – offentlig e-ID på betydelig sikkerhetsnivå
* BankID – e-ID på høyt sikkerhetsnivå, levert av Vipps AS
* BankID på mobil - e-ID på høyt sikkerhetsnivå, levert av Vipps AS
* Buypass og Buypass ID i mobil – e-ID på høyt sikkerhetsnivå, utstedt av Buypass AS
* Commfides – e-ID på høyt sikkerhetsnivå, utstedt av Commfides Norge AS.

*2.1.1 Beskrivelse og funksjonalitet*

2.1.1.1 Funksjonalitet

**Autentisering av sluttbrukere**
ID-porten skal ved autentisering av sluttbruker tilby kunden en enhetlig autentisering som er uavhengig av hvilken e-ID sluttbruker foretrekker, forutsatt at valgt e-ID tilfredsstiller sikkerhetsnivået som er nødvendig for tilgang til den aktuelle tjenesten.

ID-porten er et selvstendig tillitsanker i den forstand at ID-porten tar et selvstendig ansvar for den påstanden (fødselsnummer) som fremsettes overfor kunden. Kunden baserer innloggingen til sin tjeneste på opplysningene fra ID-porten og ikke på noen bestemt e-ID-leverandør.

e-ID-leverandøren er ikke involvert i kommunikasjonen mellom ID-porten og kunden. Ved behov vil ID-porten kunne initiere en ny autentisering ved bruk av en valgt e-ID. e-ID-leverandøren holder ikke statusinformasjon om eksisterende pålogginger, slik at e-ID-leverandøren vil håndtere dette som om sluttbrukeren tidligere ikke var autentisert.

Både kundens tjenester og ID-porten vil ha påloggingsinformasjon knyttet til autentiseringen. På bakgrunn av dette kan det tilbys verdiøkende tjenester som engangspålogging (single sign-on) på tvers av offentlige tjenester når dette er sikkerhetsmessig akseptabelt, samt policymessig styring av behov for ny autentisering, for eksempel dersom det har gått for lang tid siden autentisering ble foretatt.

**Single-sign-on**Der det ut fra en sikkerhetsmessig vurdering er akseptabelt, vil ID-porten tilby engangspålogging (single sign-on), slik at sluttbruker får tilgang til tjenester på tvers av kundene gjennom én pålogging til ID-porten.

For den enkelte kunde vil grensesnittet mot ID-porten være det samme enten sluttbruker autentiseres på nytt mot ID-porten eller single sign-on funksjonaliteten brukes. Kunder som ikke ønsker single sign-on for enkelte av sine tjenester, kan reservere den enkelte tjeneste mot å inngå i denne funksjonaliteten. Reservasjonen må ha saklig grunn.

**Anonymisert pålogging**I noen tjenester kan det være behov for å sikre autentisering av innbygger, men at innbygger likevel ikke skal identifiseres av tjenesten. ID-porten tilbyr anonym innlogging.

**API-sikring**ID-porten kan også la sluttbrukere autorisere en tjeneste til å opptre på vegne av sluttbrukeren opp mot APIer. APIene kan være tilbudt av kunden selv, eller andre kunder av ID-porten. Autorisasjonen skjer vanligvis implisitt ved autentisering, såkalt "autentiseringsnær autorisasjon", men også eksplisitte samtykker.

Kunder som tilbyr nett-tjenester som bruker tredjeparts APIer må inkludere informasjon til sluttbruker om hvilke API-er blir brukt og inngå eventuell avtale med API-eier om bruk. Også databehandleravtale kan være nødvendig.

Kunder som tilbyr APIer («API-eiere») må beskrive tekstlig hvilke rettigheter som kan delegeres, beslutte om autorisasjonen skal være eksplisitt eller implisitt, samt fortløpende godkjenne hvilke tjenester som kan få tilgang til APIet.

2.1.1.2 Leverandør

ID-porten blir driftet av TietoEVRY Norway AS.

2.1.1.3 Selvbetjening

På [Min profil](https://minside-samarbeid.digdir.no/) på Samarbeidsportalen får kunden tilgang til selvbetjening for ID-porten, og kan opprette og redigere sine tjenester.

*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 tilknyttede e-ID-er i ID-porten er i utgangspunktet gratis for sluttbruker. Sluttbruker skal fritt kunne velge blant tilknyttede e-ID-er som tilfredsstiller kravene til sikkerhetsnivå for den aktuelle tjenesten.
* e-ID-er på et sikkerhetsnivå skal også kunne benyttes for tilgang til tjenester som krever et lavere sikkerhetsnivå.
* ID-porten skal tilby ett brukergrensesnitt for valg av tilknyttede e-ID-er.

For å sikre en effektiv tjenesteproduksjon med høy kvalitet på tjenestene overfor sluttbruker, er det av avgjørende betydning at de tilknyttede e-ID-er behandles likt. Likebehandling ivaretas ved at:

* Kunden ikke kan 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 4, må akseptere alle tilknyttede e-ID-er på nivå 4. Alle kunder som tilbyr tjenester på nivå 3, må akseptere MinID (nivå 3) og alle tilknyttede e-ID-er på nivå 4.
* Alle e-ID-er som er tilknyttet ID-porten, må ha tilfredsstillende risikonivå. Gjennom risikovurderinger, revisjon og godkjenning vil Digitaliseringsdirektoratet sikre at tilknyttede e-ID-leverandører opprettholder nødvendig kvalitet og tillitsnivå i tilknyttede løsninger/tjenesteregimer.
* Alle e-ID-er som er tilknyttet ID-porten på sikkerhetsnivå 4, skal tilby tjenester for autentisering. I tillegg er det ønsket støtte for signering og meldingskryptering.

2.2 Finansiering

[Kostnadsmodell for ID-porten](https://samarbeid.digdir.no/id-porten/kostnadsmodell-id-porten/66) er tilgjengelig på Samarbeidsportalen.

2.3 Digdirs ansvar

*2.3.1 Tjenestenivå*

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

Digdir skal følge opp at eID’er levert gjennom ID-porten holder det tjenestenivå som fremgår av de til enhver tid gjeldende avtaler Digitaliseringsdirektoratet har avtale med eksterne e-ID leverandører om levering av sertifikattjenester til offentlig sektor.

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

Driftsperioden for ID-porten er 24 timer/7 dager i uken/365 dager i året.

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

Digdir har følgende krav til tilgjengelighet overfor sin driftsleverandør og de tilknyttede e-ID-leverandørene:

* Driftsleverandør – 99,90 %
* Buypass – 99,50 %
* Commfides – 99,50 %
* BankID – 99,50 %
* BankID på mobil – 99,50 %

*2.3.2 Vedlikeholdsvindu*

Vedlikeholdsvindu for ID-porten er natt til tirsdag mellom kl. 00:30 - 05:00.

2.4 Behandling av personopplysninger

*2.4.1 Digdirs ansvar*

Digdir er behandlingsansvarlig for behandling av personopplysninger i ID-porten i forbindelse med autentisering.

Ved autentisering lagrer og videreformidler Digdir sluttbrukers fødselsnummer, sikkerhetsnivå for gjennomført autentisering, sluttbrukers språkvalg og hvilken e-ID som ble benyttet for autentiseringen. Digitaliseringsdirektoratet lagrer opplysningene om autentisering i ett år.

*2.4.2 Kundens ansvar*

Kunden er behandlingsansvarlig for opplysninger om autentiseringsoperasjoner som er utlevert fra 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. Maskinporten

3.1 Om Maskinporten

Maskinporten er en løsning for å sikre korrekt tilgang til data i kommunikasjon mellom maskiner. Løsningen er i stor grad selvbetjent. Kunden kan definere hva andre virksomheter skal ha tilgang til, hvordan andre virksomheter skal kunne bruke tilgangen, og hvem som skal ha tilganger.

*3.1.1 Beskrivelse og funksjonalitet*

3.1.1.1 Funksjonalitet

**Administrasjon av Maskinporten**

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.

Selvbetjeningsfunksjonalitet er tilgjengelig både over API og som web-løsning på Samarbeidsportalen.

**Logger**
Selvbetjeningsløsningen logger endringer, aktivitet og hvem som utfører endringene. Maskinporten logger utstedelser av token. Digitaliseringsdirektoratet lagrer logger i 13 måneder.

Kunden kan be om å få utlevert opplysninger som Digitaliseringsdirektoratet på opphørstidspunktet har lagret i Maskinporten på vegne av kunden.

3.1.1.2 Leverandør

Maskinporten blir driftet av TietoEVRY Norway AS.

3.1.1.3 Selvbetjening

På [Min profil](https://minside-samarbeid.digdir.no/) på Samarbeidsportalen får kunden tilgang til selvbetjening for Maskinporten, og kan opprette og redigere sine tjenester.

Selvbetjeningen er også tilgjengelig over API.

Løsning støtter også at konsumenter kan delegere en tildelt tilgang videre til en underleverandør. Delegeringshandlingen skjer i en egnet autorativ kilde (som for eksempel Altinn Autorisasjon).

*3.1.2 Prinsipper for bruk*

**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 delegere sin tilgang videre til en leverandør, men at ansvaret fortsatt ligger hos konsument.

**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 delegere tilgang til underleverandøren. Konsument og underleverandør må ha avtaler som regulerer forholdet mellom dem.

3.2 Finansiering

[Kostnadsmodell for Maskinporten](https://samarbeid.digdir.no/maskinporten/kostnadsmodell-maskinporten/64) er tilgjengelig på Samarbeidsportalen.

3.3 Digdirs ansvar

*3.3.1 Tjenestenivå*

Alle krav som er spesifisert i disse spesielle bruksvilkår for Maskinporten, skal følges opp slik at tjenester og ytelser blir levert med avtalt og tilfredsstillende kvalitetsnivå.

Digitaliseringsdirektoratet skal følge opp at autorisasjonstjenester levert gjennom Maskinporten holder det tjenestenivå som fremgår av de til enhver tid gjeldende avtaler Digitaliseringsdirektoratet har med eksterne leverandører.

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

Driftsperioden for ID-porten er 24 timer/7 dager i uken/365 dager i året.

|  |  |
| --- | --- |
| **Beskrivelse**  | **Krav**  |
| Tilgjengelighet til Maskinporten og selvbetjenings API  | 99,90 %.  |
| Responstid  | Mindre enn 1 sekund for 95 % av utstedelsene i gjennomsnitt.  |
| Ytelse  | 720 000 token utstedelser i timen for tjenesten.  |

Digitaliseringsdirektoratet krever 99,90 % oppetid fra sin driftsleverandør.

*3.3.2 Vedlikeholdsvindu*

Vedlikeholdsvindu for Maskinporten er natt til tirsdag mellom kl. 00:30 - 05:00.

3.4 Behandling av personopplysninger

*3.4.1 Digdirs ansvar*

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

*3.4.2 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).

Token blir ikke loggført av Digitaliseringsdirektoratet.

# 4. Kontakt- og reservasjonsregisteret

4.1 Om Kontakt- og reservasjonsregisteret

Hensikten med et felles register for digital kontaktinformasjon er at innbyggerne skal ha ett sted å oppdatere sin kontaktinformasjon.

Forvaltningen bør forholde seg til Kontakt- og reservasjonsregisteret på samme måte som til det sentrale folkeregisteret, et register hvor man får tilgang til oppdatert informasjon på utvalgte områder. Offentlige virksomheter skal hente oppdatert informasjon fra Kontakt- og reservasjonsregisteret, og ikke ha egne registre med den samme informasjonen.

*4.1.1 Beskrivelse og funksjonalitet*

4.1.1.1 Funksjonalitet

**Registrert informasjon**

Følgende informasjon om innbygger er registrert og utleveres ved oppslag i registeret:

* fødselsnummer
* e-postadresse
* mobilnummer
* reservasjonsstatus
* adresse til digital postkasse valgt for mottak av digital post fra offentlig sektor
* krypteringssertifikat
* status
* sist verifisert og sist oppdatert
* varslingsstatus
* Innbyggers valgte målform.

**Standard funksjonalitet og tilleggstjenester**

Etter integrasjon mot registeret kan kunden gjøre oppslag på en eller flere innbyggere, og få utlevert informasjonen som er listet opp i punkt 4.1.1.1.

Det er innbygger selv som oppdaterer sin digitale kontaktinformasjon. Kunden bør lenke til Digitaliseringsdirektoratet tjeneste for å oppdatere digital kontaktinformasjon slik at alle oppdateringer skjer ett sted. Kunden skal ikke tilby egne løsninger der innbygger kan oppdatere sin digitale kontaktinformasjon («lokalt vedlikehold»).

Innbygger har rett til å reservere seg mot å få vedtak og andre viktige brev digitalt, etter eForvaltningsforskriften § 9. Kunden kan i sin portalløsning lenke til Digitaliseringsdirektoratet tjeneste for reservasjon mot kommunikasjon på nett.

|  |  |
| --- | --- |
| **Funksjonalitet**  | **Teknisk grensesnitt**  |
| Oppslag av en eller flere innbyggere  | Webservice  |
| Oppdatering av digital kontaktinformasjon  | Lenketjeneste  |
| Reservasjon mot kommunikasjon på nett  | Lenketjeneste  |
| Valg av digital postkasse for innbyggere  | Lenketjeneste  |

Teknisk grensesnitt for denne tilleggstjenesten er webservice.

Det finnes også en relatert tjeneste til registeret, utlevering av digital kontaktinformasjon via ID-porten. Dette er en tilleggstjeneste til ID-porten.

**Bruk av digital kontaktinformasjon**
Kontakt- og reservasjonsregisteret kan benyttes i forbindelse med saksbehandling og utføring av forvaltningsoppgaver for øvrig og skal benyttes til varsling etter eForvaltningsforskriften § 8. Dette omfatter blant annet:

* Registeret skal benyttes til å varsle innbygger om at enkeltvedtak er fattet, og om hvor og hvordan vedkommende kan skaffe seg kunnskap om innholdet. Det samme gjelder for:
* 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
* Registeret kan benyttes til varsling av innbyggere om øvrige elektroniske meddelelser fra forvaltningen
* Registeret kan benyttes til generell informasjon til innbyggere knyttet til kundens forvaltningsoppgaver
* Registeret kan benyttes til andre henvendelser fra kunden til innbyggere relatert til saksbehandlingen, som f.eks. påminnelse om avtaler og servicemeldinger

Ved hver utsendelse skal kunden gjøre oppslag i registeret.

Informasjonen fra registeret skal ikke importeres til lokale kontaktregistre hos kunden.

**Identifisering av fødselsnummer**
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.*», se også vedlagte vilkår fra skattedirektoratet.

Kunden må selv vurdere behandlingsgrunnlag etter personopplysningsloven §1, jf. forordningen artikkel 6.

4.1.1.2 Leverandør

Kontakt- og reservasjonsregisteret blir driftet av TietoEVRY Norway AS.

4.1.1.3 Selvbetjening

På [Min profil](https://minside-samarbeid.digdir.no/) på Samarbeidsportalen får kunden tilgang til selvbetjening for Kontakt- og reservasjonsregisteret, og kan opprette og redigere sine tjenester.

*4.1.2 Prinsipper for bruk*

I eForvaltningsforskriften (FOR-2004-06-25-988) kapittel 7 reguleres register over digital kontaktinformasjon og reservasjon med tilhørende infrastruktur. Registeret kan inneholde nærmere definerte opplysninger om innbyggere (privatpersoner og enheter som ikke er registrert i Enhetsregisteret), se § 31. Digdir er behandlingsansvarlig for registeret.

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

Reservasjonen skal registreres i register over digital kontaktinformasjon og reservasjon.

Etter eForvaltningsforskriften § 37 skal alle forvaltningsorganer benytte den kontaktinformasjonen som er registrert i register over digital kontaktinformasjon og reservasjon til å sende varsel om enkeltvedtak mv. etter forskriftens § 8, senest fra 1. januar 2016.

Så snart forvaltningsorganet er koblet til registeret, kan det kommunisere elektronisk med innbyggere uten å innhente samtykke. Kontaktinformasjonen i registeret skal fra samme tid benyttes til å sende varsel etter § 8.

4.2 Finansiering

[Kostnadsmodell for Kontakt- og reservasjonsregisteret](https://samarbeid.digdir.no/kontaktregisteret/kostnadsmodell-kontaktregisteret/577) er tilgjengelig på Samarbeidsportalen.

4.3 Digdirs ansvar

*4.3.1 Tjenestenivå*

Alle krav som er spesifisert i disse spesielle bruksvilkår for Kontakt- og reservasjonsregisteret, skal følges opp slik at tjenester og ytelser blir levert med avtalt og tilfredsstillende kvalitetsnivå.

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

Tilgjengelighet 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 request er mottatt i eksternt API til respons er sendt.

*4.3.2 Vedlikeholdsvindu*

Vedlikeholdsvindu for Kontakt- og reservasjonsregisteret er natt til tirsdag mellom kl. 00:30 - 05:00.

4.4 Behandling av personopplysninger

*4.4.1 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. Loggene oppbevares i 1 år.

*4.4.2 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 overenstemmelse med de krav som følger av personopplysningsloven

# 5. Digital postkasse til innbyggere

5.1 Om Digital postkasse til innbyggere

Digital postkasse til innbyggere er en fellesløsning offentlige virksomheter kan benytte for å sende post digitalt til innbyggere. Den enkelte innbygger velger selv en digital postkasse for å motta post fra offentlig sektor, blant leverandører som har avtale med Digitaliseringsdirektoratet. Innbygger må inngå avtale med postkasseleverandøren.

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. Digital postkasse må ikke oppfattes som betegnelsen på en bestemt teknisk løsning.

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.

*5.1.1 Beskrivelse og funksjonalitet*

5.1.1.1 Funksjonalitet

Digital postkasse omfatter flere komponenter:

**Aksesspunkt**
Aksesspunkt for digital postkasse skal formidle meldinger fra offentlige avsendere til angitt postkasseleverandør eller utskriftstjeneste, og formidle leveringsstatus tilbake til kundens aksesspunkt. Integrasjonspunktet for eFormidling kan benyttes for å integrere kundens systemer til kundens aksesspunkt.

**Kontakt- og reservasjonsregisteret**
Kontakt- og reservasjonsregisteret er et register over innbyggerens digitale kontaktinformasjon og reservasjonsstatus. Registeret er regulert i eForvaltningsforskriften (FOR-2004-06-25-988) kapittel 7 og kan inneholde nærmere definerte opplysninger om innbyggere.

Kontakt- og reservasjonsregisteret er en fellesløsning som må benyttes sammen med digital postkasse til innbyggere, se kapittel for Kontakt- og reservasjonsregisteret. Digdir er behandlingsansvarlig for Kontakt- og reservasjonsregisteret, jf. eForvaltningsforskriften § 30.

**Postkasse**
Postkasseleverandørens hovedoppgaver er å motta meldinger fra aksesspunktet, levere dem i innbyggers digitale postkasse, varsle innbygger om ny post hvis innstillingene tilsier det, tilby innbygger enkel tilgang via web og app og lagre posten på en sikker måte så lenge innbygger selv ønsker. Kunden skal ikke ha direkte integrasjon mot postkasseleverandør. Innbygger kan selv flytte mottatt post dersom han ønsker å bytte postkasse.

**Sending av meldinger**
Digital postkasse er en felles løsning for offentlige virksomheter for å sende brev digitalt til innbyggere. Tjenesten leverer post til innbyggers valgte digitale postkasse. Varsling til innbygger om at posten er tilgjengelig i postkassen, formidles av postkasseleverandøren i henhold til innstillinger. Kunden får kvitteringer for at meldingen er levert til postkassen.

Kunden må selv fastsette tilstrekkelig autentiseringsnivå som kreves ved innlogging for å kunne åpne og lese brev sendt til postkassene. Kunden må avgjøre om innbygger skal varsles etter bestemmelsene i eForvaltningsforskriften.

**Utskrifts- og forsendelsestjeneste**
Tjenesten gjør det mulig for kunden å sende brev gjennom løsningen, selv om kunden ikke har en digital postkasse eller er reservert mot digital kommunikasjon.

Kunden betaler for tilpasning av egne systemer for å ta i bruk utskrifts- og forsendelsestjenesten. I tillegg betaler kunden per brev som går til utskrift.

**Varsling av innbygger**
Varslingsplikten etter eForvaltningsforskriften § 8 påligger kunden.

Kunden kan ved sending av meldinger bestemme at innbygger skal varsles, per SMS eller e-post, om at det er levert/tilgjengeliggjort post i postkassen.

Varsling av innbygger per e-post er kostnadsfritt, SMS er priset særskilt, se prislisten.

**Kvitteringer**
Kunden vil få en kvittering på at meldingen er mottatt av postkasseleverandøren og vil bli gjort tilgjengelig i innbyggers digitale postkasse. Dersom kvittering ikke blir levert, skal kunden kontakte Digitaliseringsdirektoratet.

Det blir sendt egen kvittering med feilmelding dersom varsling av innbygger har feilet. Feilmeldinger sendes også dersom det oppstår en uventet feil som ikke kan håndteres av postkasseleverandør eller utskriftsleverandør innen SLA-krav. Feilmeldinger kategoriseres i to typer:

* Klientfeil – feil i melding sendt fra avsender. Klientfeil håndteres og rettes av avsender.
* Serverfeil – intern feil hos postkasseleverandør eller utskriftsleverandør. Håndteres og rettes av leverandør. Følges opp av Digdir som sentralforvalter.

Kunden kan ved sending av meldinger be om åpningskvittering. Postkassen kan bare sende åpningskvittering hvis innbygger gir samtykke til dette. Åpningskvittering er priset særskilt.

Kvitteringsmeldingene er ytterligere beskrevet på Samarbeidsportalen.

5.1.1.2 Leverandør

Digitaliseringsdirektoratet er sentralforvalter for Digital postkasse til innbyggere, og er avtalepart overfor eksterne leverandører:

* TietoEVRY Norway AS er tjenesteleverandør for et aksesspunkt som kundene kan velge å ta i bruk. Aksesspunktet er ferdig integrert mot eFormidling.
* Posten Norge AS er tjenesteleverandør og leverer aksesspunkt for postkassene og utskriftstjenesten.
* Skatteetaten leverer tjeneste for utskrift og forsendelse.
* e-Boks A/S leverer en av de to postkassene innbygger kan velge.
* Posten Norge AS leverer en av de to postkassene innbygger kan velge.

*5.1.2 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 fra offentlig sektor er gratis for innbygger.
* Pålogging til post fra offentlig sektor skjer ved bruk av ID-porten, som er gratis for innbygger.
* Kunden skal i sin portalløsning (fra sin egen nettjeneste) 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».
* Alle postkasseleverandører som er tilknyttet løsningen skal tilby sikker lagring av meldinger mottatt fra det offentlige, så lenge innbygger ønsker.
* Kunden kan ikke reservere sine tjenester mot noen av postkasseleverandørene.

5.2 Finansiering

[Kostnadsmodellen for Digital postkasse til innbyggere](https://samarbeid.digdir.no/digital-postkasse/kostnadsmodell-digital-postkasse/106) er tilgjengelig på Samarbeidsportalen.

5.3 Digdirs ansvar

*5.3.1 Tjenestenivå*

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

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

Måleperiode er månedlig (per kalendermåned).

Driftsperioden for digital post er 24 timer/7 dager i uken/365 dager i året. Tjenesten er dimensjonert til at det offentlige skal kunne sende 1 melding på 100kb til hver av landets innbyggere i løpet av 24 timer. Kvitteringer vil bli levert innen 1 time. Løsningen har en tilgjengelighet på 99,50 %

5.4 Behandling av personopplysninger

*5.4.1 Digdirs ansvar*

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

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 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.

Digitaliseringsdirektoratet 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 Digitaliseringsdirektoratet å stanse behandlingen av personopplysninger på vegne av kunden. Med mindre annet fremgår av pålegget fra kunden, skal Digitaliseringsdirektoratet gjennomføre sending av digital post som er påbegynt før pålegget ble mottatt. Med mindre kunden pålegger Digitaliseringsdirektoratet 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.

*5.4.2 Kundens ansvar*

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

Etter 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 Digitaliseringsdirektoratet før melding er kommet frem til Posten Norge AS sitt aksesspunkt. Behandling av personopplysninger før dette må reguleres i avtalen mellom kunde og aksesspunktleverandør.

# 6. eSignering

6.1 Om eSignering

eSignering er en felles signeringstjeneste for offentlige virksomheter og en frittstående tjeneste for elektronisk personsignatur. Digitaliseringsdirektoratet er sentralforvalter for eSignering.

*6.1.1 Beskrivelse og funksjonalitet
6.1.1.1 Funksjonalitet*

Tjenesten gjør det mulig for innbyggere å signere dokument fra det offentlige digitalt ved påføring av elektronisk personsignatur. En kopi av ferdig signerte oppdrag sendes via eSignering til innbyggerens digitale postkasse dersom innbygger har dette. Videresendingsfunksjonen kan overstyres dersom mottakeren av signeringsoppdrag ikke signerer som en innbygger. Tjenesten har også varslingsfunksjonalitet for varsling av signatar om dokument som skal signeres. Innbygger blir da varslet pr e-post eller SMS. Kontaktinformasjon som benyttes til varsling blir hentet via eSignering fra Kontakt og reservasjonsregisteret. Varslingsinformasjon kan overstyres i de tilfellene der signatar ikke er en innbygger.

eSignering støtter de mest brukte formatene for digital signatur. Gyldige format er dokumentert på Samarbeidsportalen. eSignering lar kunder opprette signeringsoppdrag via en integrasjonsløsning eller via et web-basert administrasjonsgrensesnitt.

**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 foreligger dokument til signering.

6.1.1.2 Leverandør

eSignering blir driftet og utviklet av Posten Norge AS.

*6.1.2 Prinsipper for bruk*

eSignering skal dekke offentlige virksomheter felles behov for signerings- og valideringstjenester. Tjenesten skal tilby god brukervennlighet, sikkerhet og være skalerbar med tanke på fremtidige behov og bruksvolum.

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

Digitaliseringsdirektoratet er ansvarlig for at eSignering oppfyller lovmessige krav, regelverk og forskrifter. 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.

6.2 Finansiering

[Kostnadsmodell for eSignering](https://samarbeid.digdir.no/esignering/kostnadsmodell-esignering/103) er tilgjengelig på Samarbeidsportalen.

6.3 Digdirs ansvar

*6.3.1 Tjenestenivå*

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

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

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

6.4 Behandling av personopplysninger

*6.4.1 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.

*6.4.2 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.

# 7. eFormidling

7.1 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.

Integrasjonspunktet tilbyr et standardisert programmeringsgrensesnitt som kundens saksbehandlings- og fagsystem(er) kan benytte til å sende og motta meldinger.

Integrasjonspunktet er skjæringspunktet mellom kundens indre nettverk og systemer utenfor kundens nettverk. Integrasjonspunktets lokale del har følgende oppgaver:

* Kryptere sending
* Signere sending
* Validere adresseinformasjon ved oppslag mot autoritative register
* Sende via mottaker sin valgte transportinfrastruktur(er)
* Oppdaterer trafikkloggen i sentral fellestjeneste (pakkesporingstjenesten).

Virksomheter kan utvikle og administrere sitt eget integrasjonspunkt. Virksomheter som har egenutviklet integrasjonspunkt, er pliktig til å levere statuslogg. Format for statuslogg ligger beskrevet på Samarbeidsportalen.

*7.1.1 Beskrivelse og funksjonalitet*

7.1.1.1 Funksjonalitet

Programvarekomponenten integrasjonspunktet installeres lokalt hos kunden. Denne tilbyr et standardisert programmeringsgrensesnitt (API) for integrasjon mellom kundens fagsystemer og meldingsorienterte fellestjenester, for eksempel digitale postkasser. Programvarekomponenten integrasjonspunktet har ansvar for at meldinger er syntaktisk korrekt utformet, og at overføringen skjer på en måte som sikrer meldingens integritet og konfidensialitet. Komponenten vil medføre at kundens løsninger vil kunne fungere med høy tilgjengelighet, men meldingens endelige tilgjengelighet (tiden før den blir levert til mottaker) er avhengig av kanalen den blir formidlet via.

Løsningen består av flere sentrale fellestjenester som understøtter forvaltning, logging og sporing av integrasjonspunktet og meldingene som blir formidlet gjennom dette.

**Meldingstyper**
Integrasjonspunktet er tilrettelagt som en infrastruktur for å sende meldinger. Gyldig innhold i meldingene vil variere avhengig av hva mottakende tjeneste eller virksomhet godtar. Integrasjonspunktet tilbyr tjenester for å kunne validere strukturerte meldingstyper (for eksempel xml) og filtrere gyldige formater på ustrukturerte filer (for eksempel pdf, docx).

**Adressering**
Integrasjonspunktet bruker informasjon fra flere offentlige autoritative kilder til validering av adresser. Kildene er kontakt- og reservasjonsregisteret, ELMA, FIKS og Enhetsregisteret i Brønnøysund. Ansvar for kvaliteten på innholdet i disse registrene reguleres av egne regler og er utenfor denne avtalen.

7.1.1.2 Leverandør

eFormidling blir driftet av TietoEVRY Norway AS.

*7.1.2 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.

7.2 Finansiering

[Kostnadsmodell for eFormidling](https://samarbeid.digdir.no/eformidling/kostnadsmodell-eformidling/111) er tilgjengelig på Samarbeidsportalen.

7.3 Digdirs ansvar

*7.3.1 Tjenestenivå*

Alle krav som er spesifisert i disse spesielle bruksvilkår for integrasjonspunktet, skal følges opp slik at tjenester og ytelser blir levert med avtalt og tilfredsstillende kvalitetsnivå. Digitaliseringsdirektoratet tilbyr integrasjonspunktet som programkode, støttetjenester til integrasjonspunktet gjennom API og support til integrasjonspunktet.

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

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

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. Oppdateringer til det lokale integrasjonspunktet har samme tilgjengelighet som det sentrale integrasjonspunktet.

7.4 Behandling av personopplysninger

*7.4.1 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 avidentifisert. 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.

*7.4.2 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.

#

# 8. Digital post til virksomheter

## 8.1 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.

### 8.1.1 Beskrivelse og funksjonalitet

#### 8.1.1.1 Funksjonalitet

Tjenesten Digital post til virksomheter i Altinn dekker behov for forsendelse, statusoppdatering, varslinger og re-varsling (varsling på nytt om en melding ikke er åpnet). I tillegg til eksisterefunksjonalitet er det for DPV lagt inn 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»
* Mulighet for å lese status på inntil 10.000 meldinger av gangen

**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

**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)](https://www.altinn.no/hjelp/skjema/alle-altinn-roller/postarkiv/) 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.

**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 8.1.1.1.1.1 “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.

**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](https://altinn.github.io/docs/utviklingsguider/digital-post-til-virksomheter/overorndet-funksjonalitet/del-tilgang-til-melding/) av hvordan virksomhetene bør håndtere tilgangsstyringen i slike tilfeller.

**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.

#### 8.1.1.2 Leverandør

DPV driftes av Basefarm og forvaltes av Accenture.

### 8.1.2 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.

###

## 8.2 Finansiering

[Kostnadsmodell for Digital post til virksomheter](https://samarbeid.digdir.no/eformidling/kostnadsmodell-eformidling/111) og varsling er tilgjengelig på Samarbeidsportalen.

###

## 8.3 Digdirs ansvar

### 8.3.1 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.

## 8.4 Behandling av personopplysninger

### 8.4.1 Digdirs ansvar

Digdir er databehandler på vegne av den enkelte kunde ved bruk av tjenesten Digital post ti 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 Personvernnemnda.

### 8.4.2 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.