Spørsmålsorientert veiledning til eForvaltningsforskriften

Oversikt (innholdsfortegnelse)

2.2.2 Hva menes med sikkerhetstjenester og -produkter og hvilke kan forvaltningsorganet benytte?

Spørsmålsorientert veiledning til eForvaltningsforskriften

1. For enkeltpersoner og andre brukere av forvaltningens tjenester

1.1 Om å kommunisere med offentlig forvaltning

1.1.1 Når kan jeg sende e-post eller bruke annen elektronisk kommunikasjon for å kontakte forvaltningen?

Du har ikke noe ubetinget krav på å få henvende deg til forvaltningsorganet ved bruk av elektronisk kommunikasjon. Det kan du bare gjøre når det er lagt til rette for det fra forvaltningsorganets side. Forvaltningsorganet kan for eksempel ha opprettet et eget nettsted for å ta imot henvendelser fra brukerne av forvaltningens tjenester. Se for eksempel et enkelt kontaktskjema som benyttes av Kommunal- og moderniseringsdepartementet. [Lenke til: http://www.regjeringen.no/nb/dep/kmd/dep/kontakt/skjema-kontakt-kommunal--og-regionaldepa.html?id=437520] Flere avanserte tjenester fra ulike forvaltningsorganer er samlet i portalen "Altinn".

Forvaltningsorgan som bruker e-post, skal også ha etablert en felles e-postadresse for organet (for eksempel postmottak@kmd.dep.no). Hvis forvaltningsorganet har etablert en generell elektronisk adresse, og de ikke har stilt noen spesielle krav til den aktuelle typen henvendelse, for eksempel at det skal benyttes et skjema eller tjeneste fra et bestemt nettsted, kan den generelle elektroniske adressen benyttes. Et forvaltningsorgan kan også ha opprettet særlige nettsteder eller tjenester som skal benyttes for bestemte typer henvendelser (for eksempel i forbindelse med lovpålagt innrapportering), mens andre henvendelser kan formidles via forvaltningsorganets generelle elektroniske adresse.

Les mer:

- eForvaltningsforskriften § 3 [lenke til Lovdata[1]]
- arkivforskriften § 3-2 [lenke til lovdata] med kommentarene [Lenke til Veilederen del 3 – Forskrift med noteapparat, § 3]
- Mer om denne delen av eForvaltningsforskriften i en annen del av veilederen som er tilgjengelig her [Lenke til Veilederen del 1, kapittel 3.2]

1.1.2 Hvordan vet jeg at min henvendelse har kommet frem til forvaltningsorganet?

Et forvaltningsorgan som mottar en henvendelse i elektronisk form skal gi deg bekreftelse på at henvendelsen er mottatt, se efvf. § 6. Bekreftelsen bør gis straks henvendelsen er mottatt og bør inneholde et referansenummer, journalnummer eller lignende og angi på hvilket tidspunkt henvendelsen ble mottatt.

Begrunnelsen for kravet er bl.a. å bidra til forutberegnelighet og tillit til tjenestene og å fjerne usikkerhet med hensyn til om forvaltningsorganet har mottatt henvendelsen. I tillegg vil en slik

[1] eForvaltningsforskriften § 3: http://lovdata.no/for/sf/fa/ta-20040625-0988-002.html#3

ordning med bruk av referansenummer og tidspunkt for når henvendelsen ble mottatt, gjøre det lettere for deg å følge opp henvendelsen til forvaltningsorganet.

Det er ikke nødvendig å sende kvittering hvis henvendelsen blir besvart umiddelbart. Det gjøres også unntak fra denne hovedregelen når henvendelsen ikke utløser saksbehandling, for eksempel hvis det gjelder "spam".

Les mer:

- eForvaltningsforskriften § 6 [lenke til Lovdata[2]] med kommentarer [Lenke til Veilederen del 3 – Forskrift med noteapparat, § 6]
- Mer om denne delen av eForvaltningsforskriften i en annen del av veilederen som er tilgjengelig her [Lenke til Veilederen del 1, kapittel 3.6].

1.1.3 Kan jeg sende taushetsbelagte eller personsensitive opplysninger via Internett?

Når personopplysninger, eller andre opplysninger som vil være underlagt taushetsplikt hos forvaltningen, sendes over åpne nett, kan uvedkommende få tilgang til å lese eller endre opplysningene. Du bør derfor ikke sende opplysninger som er taushetsbelagte eller som du ikke ønsker at andre skal se, ved hjelp av vanlig e-post. Forvaltningsorganet har et særlig ansvar for å forebygge slik risiko ved å legge til rette for at det brukes sikre kanaler, og informere om restrisikoen når det tilrettelegges for elektronisk kommunikasjon.

En slik tilrettelegging kan for eksempel være et sikkert elektronisk skjema, en sikker jobbsøkefunksjon på nett eller lignende. Et tegn på at det er satt opp sikker kommunikasjon for deg, er når det ikke lenger står "http", men "https", i nettadressefeltet. Da er det opprettet en kryptert forbindelse med det nettstedet du har koplet deg til. Du vil også se et hengelåsikon på skjermen. For å få bekreftet hvilket nettsted du er koplet til kan du klikke på hengelåsikonet. Enkelte nettlesere viser deg også dette uoppfordret i enden av adressefeltet. Benyttes kryptering er det *forvaltningsorganets krypteringsnøkkel* som benyttes. Forvaltningsorganet skal informere om hvordan dette gjøres. I mange tilfeller vil forvaltningsorganet ha tilrettelagt det slik at det automatisk opprettes en kryptert forbindelse med nettleseren din, når du kommuniserer med forvaltningsorganet på den måten de har lagt til rette for.

Les mer:

- eForvaltningsforskriften § 5 [lenke til Lovdata[3]] med kommentarer [Lenke til Veilederen del 3 – Forskrift med noteapparat, § 5]
- Mer om denne delen av eForvaltningsforskriften i en annen del av veilederen som er tilgjengelig her [Lenke til Veilederen del 1, kapittel 3.5].

[2] eForvaltningsforskriften § 6: http://www.lovdata.no/for/sf/fa/ta-20040625-0988-002.html#6

[3] eForvaltningsforskriften § 5: http://www.lovdata.no/for/sf/fa/ta-20040625-0988-002.html#5

1.1.4 Kan jeg kreve innsyn i elektroniske dokumenter?

Regler om innsynsrett finner vi bl.a. i offentleglova, i forvaltningsloven § 18 og i personopplysningsloven § 18. Det gjøres ingen begrensninger i innsynsretten fordi dokumentene foreligger i elektronisk form. Derimot kan elektronisk lagring av dokumenter bidra til lettere å realisere innsynsretten for publikum. Det er opp til forvaltningsorganet hvordan det legger til rette for innsyn i dokumenter og opplysninger i elektronisk form.

Alt etter hvordan forvaltningsorganet i henhold til sikkerhetsstrategien legger til rette for innsyn i elektroniske dokumenter, vil du kunne:

- Forespørre om innsyn ved bruk av elektronisk kommunikasjon.
- Få oversendt dokumentet ved bruk av elektronisk kommunikasjon
- Få innsyn direkte i elektronisk dokumentregister.
- Få innsyn direkte i det elektroniske dokumentarkivet.

Hva slags innsyn som gis vil selvsagt også styres av hva den du har rett til å se. Hvis du er ”part” i saken, vil du ha større adgang til innsyn i dokumentene enn det ”enhver” kan få etter offentleglova. For å gi partsinnsyn er det nødvendig at forvaltningen sørger for å bringe på det rene identiteten (autentisering) din når du ber om innsyn. Dersom du ber om innsyn etter offentleglova, kan ikke forvaltningsorganet kreve at du identifiserer deg ut over det som er nødvendig for selve innsynet (for eksempel ved at de må ha en e-postadresse å sende dokumentet til).

Les mer:

- eForvaltningsforskriften § 12 [lenke til Lovdata] med kommentarer [Lenke til Veilederen del 3 – Forskrift med noteapparat, § 12]
- Mer om denne delen av eForvaltningsforskriften i en annen del av veilederen som er tilgjengelig her [Lenke til Veilederen del 1, kapittel 3.9].

1.1.5 Må jeg underskrive dokumenter som skal til et forvaltningsorgan når det benyttes elektronisk kommunikasjon?

Det er ikke noe generelt krav om at henvendelser til et forvaltningsorgan skal være underskrevet. Ofte vil det være tilstrekkelig at forvaltningsorganet kan få bekreftet avsenderens identitet (hvem du er). Av og til behøver ikke forvaltningsorganet vite hvem avsenderen er heller, for eksempel hvis det er spørsmål om helt generell veiledning eller hvis du ber om innsyn i dokumenter etter offentleglova.

I de tilfellene forvaltningsorganet har lagt til rette for å motta henvendelser ved hjelp av elektronisk kommunikasjon, og det *er* krav om underskrift, skal forvaltningsorganet gi veiledning om hva du trenger og hvordan du skal gå frem. Det vanlige vil være at man benytter elektroniske signaturer gjennom en portalløsning som for eksempel ”Altinn”.

Les mer:

- eForvaltningsforskriften § 4 [lenke til Lovdata] med kommentarer [Lenke til Veilederen del 3 – Forskrift med noteapparat, § 4]

- Mer om denne delen av eForvaltningsforskriften i en annen del av veilederen som er tilgjengelig her [Lenke til Veilederen del 1, kapittel 3.4].

1.1.6 Er det noe utstyr eller programvare jeg som privatperson må anskaffe for å kunne kommunisere med forvaltningsorganet?

Hvilket utstyr du trenger er litt avhengig av hva du vil kommunisere med forvaltningsorganet om. I mange tilfeller vil en vanlig datamaskin med tilgang til Internett være tilstrekkelig. Hvis du for eksempel skal hente et søknadsskjema eller generell informasjon fra et nettsted, trenger du vanligvis ikke noe spesielt utstyr.

Hvis du derimot skal sende inn søknader, klager eller andre henvendelser til forvaltningen, og forvaltningen har vurdert det slik at du må bekrefte din identitet (hvem du er) når du søker eller klager, må du anskaffe et elektronisk identitetsbevis (e-ID). Det får du ved å henvende deg til en av leverandørene i markedet, eller ved å bruke MinID, se mer informasjon på norge.no: «Ny bruker av offentlige tjenester på nett» [http://eid.difi.no/nb/id-porten]. Forvaltningsorganet avgjør hvilke typer e-ID som gir tilstrekkelig sikkerhet for den aktuelle handlingen.

Les mer:

- eForvaltningsforskriften § 4 [lenke til Lovdata[4]] med kommentarer [Lenke til Veilederen del 3 – Forskrift med noteapparat, § 4]
- Mer om denne delen av eForvaltningsforskriften i en annen del av veilederen som er tilgjengelig her [Lenke til Veilederen del 1, kapittel 3.4].
- Mer om e-ID, se kapittel 1.2.1

1.1.7 Kan forvaltningsorganet kreve at jeg bruker elektronisk kommunikasjon?

Den store hovedregelen er at forvaltningsorganet *ikke* kan *kreve* at du skal bruke elektronisk kommunikasjon ved henvendelse *til* et forvaltningsorgan. Selv om forvaltningsorganet har lagt til rette for det, kan du selv velge om du vil henvende deg til forvaltningsorganet ved bruk av elektronisk kommunikasjon eller ved bruk av tradisjonelle metoder (ordinært brev eller telefon).

Når det gjelder enkeltvedtak eller tilsvarende *fra* forvaltningen, se punkt 1.3.1, er utgangspunktet at forvaltningen kan sende disse elektronisk. Du skal varsles om at vedtaket er fattet, og hvordan du kan få tilgang til innholdet.

Privatpersoner kan reservere seg mot denne typen kommunikasjon. Dette står nærmere omtalt i kapittel 1.3.7.

Les mer:

- eForvaltningsforskriften § 8 (underretning om enkeltvedtak mv) og § 9 (reservasjon) [lenke til Lovdata[5]] med kommentarer [Lenke til Veilederen del 3 – Forskrift med noteapparat, § 8 og § 9]

---

[4] eForvaltningsforskriften § 4 http://www.lovdata.no/for/sf/fa/ta-20040625-0988-002.html#4

- Mer om denne delen av eForvaltningsforskriften i en annen del av veilederen som er tilgjengelig her [Lenke til Veilederen del 1, kapittel 3.7].

1.2 Om elektroniske identitetsbevis (e-ID) og ID-porten

1.2.1 Hva er et elektronisk identitetsbevis eller e-ID?

Begrepet elektronisk identitetsbevis benyttes blant annet i eForvaltningsforskriften § 10. Begrepet forkortes gjerne til e-ID. En e-ID er et elektronisk alternativ til fysiske legitimasjonsbevis, og e-ID-en muliggjør elektronisk identitetskontroll. En e-ID består gjerne av et sett opplysninger som bare innehaveren og utstederen kjenner til eller har kontroll over. En vanlig kombinasjon er at innehaveren bruker et passord og en engangskode som mottas per sms eller fra en engangskodekalkulator.

Les mer:

- Mer om e-ID http://eid.difi.no/nb/id-porten/hva-er-en-elektronisk-id-eid

1.2.2 Hva er elektronisk signatur?

I esignaturloven (lov om elektronisk signatur) er begrepet *elektronisk signatur* definert som "*data i elektronisk form som er knyttet til andre elektroniske data og som brukes som autentiseringsmetode*". I begrepet autentiseringsmetode ligger at datasettet er egnet til å bevise dokumentets opphav og innhold. Bevisstyrken kan variere, blant annet med typen signatur. En PIN-kode kan være en elektronisk signatur. En slik løsning har blant annet Skatteetaten benyttet ved innsendelse av selvangivelse.

Esignaturloven benytter også begrepet avansert elektronisk signatur. Dette er signeringsløsninger som gir relativt sterke bindinger mellom en autentisering og et dokument

Les mer:

- esignaturloven § 3 nr. 1. Esignaturloven gjennomfører EUs direktiv om elektroniske signaturer (Direktiv 1999/93/EF). Direktivet erstattes 1.7.2016 av EU-forordning om e-ID og tillitstjenester (forordning 910/2014).

1.2.3 Hva er ID-porten?

ID-porten er en felles innloggingsløsning til offentlige tjenester på nett. Direktoratet for forvaltning og IKT (Difi) har ansvaret for driften.

Statlige virksomheter skal ta i bruk ID-porten for digitale tjenester som krever innlogging og autentisering jf. Digitaliseringsrundskrivet kapittel 1.2. Mange offentlige virksomheter bruker derfor ID-porten som den tekniske løsningen for autentisering når innbyggerne skal kommunisere med det offentlige. Eksempler på dette er digital postkasse, altinn.no og helsenorge.no.

Les mer:

---

[5] eForvaltningsforskriften § 8 http://www.lovdata.no/for/sf/fa/ta-20040625-0988-002.html#8

- Difis nettsider [http://www.difi.no/digital-forvaltning/felles-it-losninger-fra-difi/id-porten].
- Digitaliseringsrundskrivet kapittel 1.2. [lenke]

1.2.4 Må jeg anskaffe en e-ID?

Om du må anskaffe et elektronisk identitetsbevis (e-ID) er avhengig av hva du vil kommunisere med forvaltningsorganet om. I mange tilfeller vil en vanlig datamaskin med tilgang til Internett være tilstrekkelig. Hvis du for eksempel skal hente et søknadsskjema eller generell informasjon fra et nettsted, trenger du vanligvis ikke noe spesielt utstyr eller noen elektronisk signatur.

Hvis du derimot skal sende inn søknader, klager eller andre henvendelser til forvaltningen, kan det hende du må anskaffe en e-ID. Hvis forvaltningsorganet har lagt til rette for bruk av elektronisk kommunikasjon, og det er nødvendig å bruke e-ID, skal forvaltningsorganet informere om det.

Forvaltningen vurderer hvilke sikkerhetsløsninger som er nødvendig for å kunne kommunisere med dem. Når forvaltningen stiller krav til bruk av slike sikkerhetstjenester og -produkter skal det være dokumentert i forvaltningsorganets sikkerhetsstrategi. En slik strategi må forvaltningsorganet utarbeide før de tar i bruk elektronisk kommunikasjon. Det er det enkelte forvaltningsorgans begrunnede behov for å bruke slike tjenester som skal styre bruken av for eksempel elektroniske signaturer.

Les mer:

- eForvaltningsforskriften § 4 [lenke til Lovdata] med kommentarer [Lenke til Veilederen del 3 – Forskrift med noteapparat, § 4]
- Mer om denne delen av eForvaltningsforskriften i en annen del av veilederen som er tilgjengelig her [Lenke til Veilederen del 1, kapittel 3.4].

1.2.5 Hvordan skaffer jeg meg en e-ID?

Elektronisk identitetsbevis (e-ID) for bruk mot offentlige tjenester kan du skaffe deg hos de leverandørene som støttes av ID-porten. Se mer informasjon på norge.no; «Ny bruker av offentlige tjenester på nett» [http://eid.difi.no/nb/id-porten].

Et forvaltningsorgan som krever at du benytter e-ID, skal informere om hva du trenger og hvor du kan få tak i det.

Les mer:

- eForvaltningsforskriften § 4 [lenke til Lovdata[6]] med kommentarer [Lenke til Veilederen del 3 – Forskrift med noteapparat, § 4]

[6] eForvaltningsforskriften § 4
http://www.npt.no/portal/page?_pageid=145,62509&_dad=web&_schema=PORTAL

- Mer om denne delen av eForvaltningsforskriften i en annen del av veilederen som er tilgjengelig her [Lenke til Veilederen del 1, kapittel 3.4]

1.3 Om digital postkasse, kontakt- og reservasjonsregisteret

1.3.1 Hva er digital postkasse?

Når forvaltningen ønsker å sende et enkeltvedtak, eller tilsvarende, med elektronisk kommunikasjon må det benyttes et «egnet informasjonssystem» ihht. eForvaltningsforskriften § 8.

Digital postkasse til innbyggere er et slikt egnet informasjonssystem, som både stat og kommune kan benytte. Forvaltningen kan gjennom løsningen sende enkeltvedtak og andre meldinger til innbyggeren, inkludert meldinger med taushetsbelagte opplysninger og annen beskyttelsesverdig informasjon. En forutsetning for bruk av løsningen er at innbyggeren har valgt seg en digital postkasse hos en av de private leverandørene. Det er frivillig for innbygger å ha en digital postkasse.

Det er Difi som forvalter fellesløsningen digital postkasse til innbygger. Alle statlige forvaltningsorganer som sender post på papir til innbyggere skal ta løsningen i bruk, jf. Digitaliseringsrundskrivet pkt. 1.2

I tillegg til enkeltvedtak gjelder tilsvarende 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.

I denne veilederen brukes «enkeltvedtak, eller tilsvarende» for å vise at også disse meldingene er inkludert.

Les mer:

- eForvaltningsforskriften § 8 (underretning om enkeltvedtak mv) [lenke til Lovdata[7]] med kommentarer [Lenke til Veilederen del 3 – Forskrift med noteapparat, § 8]
- Digitaliseringsrundskrivet kapittel 1.2.

1.3.2 Hvordan skaffer jeg meg en digital postkasse?

Opprettelse av digital postkasse gjøres hos en av tilbyderne av slike postkasser.
For veiledning, se Norge.no http://www.norge.no/nb/velgpostkasse.

[7] eForvaltningsforskriften § 8 http://www.lovdata.no/for/sf/fa/ta-20040625-0988-002.html#8

1.3.3 Hva kan jeg motta fra forvaltningen i min digitale postkasse?

Det er opp til forvaltningsorganet å vurdere hvilken informasjon de vil sende til din digitale postkasse. Løsningen er egnet for å sende enkeltvedtak og andre meldinger, også innhold med taushetsbelagt og annen beskyttelsesverdig informasjon.

Alle statlige forvaltningsorganer som sender post på papir til innbyggere skal ta løsningen i bruk, jf. Digitaliseringsrundskrivet pkt. 1.2. Løsningen kan også benyttes av kommuner og fylkeskommuner. Det vil gradvis bli flere offentlige virksomheter som benytter løsningen.

For å lese brev fra offentlige avsendere benyttes ID-porten til å logge inn i postkassen.

1.3.4 Hvordan vet jeg at det er kommet post i min digitale postkasse?

Når enkeltvedtak, eller tilsvarende, sendes elektronisk skal du få et varsel om at enkeltvedtak er fattet og om hvor og hvordan du kan skaffe deg kunnskap om innholdet. Dersom enkeltvedtaket eller tilsvarende ikke åpnes innen en uke etter at det ble gjort tilgjengelig, skal det sendes et nytt varsel.

Senest fra 1. januar 2016 skal forvaltningsorganer når de sender enkeltvedtak, eller tilsvarende, digitalt, bruke den kontaktinformasjonen (e-postadresse og/eller mobilnummer) som er registrert i kontakt- og reservasjonsregisteret for å sende varsel.

Les mer:

- eForvaltningsforskriften § 8 [lenke til Lovdata].
- Digitaliseringsrundskrivet kapittel 1.2.

1.3.5 Hva er kontakt- og reservasjonsregisteret?

Kontakt- og informasjonsregisteret er et felles register for offentlig sektor som inneholder innbyggeres digitale kontaktinformasjon og opplysninger om innbyggeren har reservert seg mot digital kommunikasjon med offentlig sektor. Difi er behandlingsansvarlig for registeret.

Registeret omfatter kun privatpersoner og enheter som ikke er registret i Enhetsregisteret. Kontaktinformasjon til enheter som er registrert i Enhetsregisteret lagres ikke i register over digital kontaktinformasjon og reservasjon.

Informasjonen kan benyttes i forbindelse med saksbehandling og utføring av forvaltningens oppgaver, og skal benyttes ved varsling om at enkeltvedtak, eller tilsvarende, er fattet.

Formålet med registeret er å ha et felles og godt oppdatert register som det offentlige skal benytte for å kunne kommunisere digitalt med innbyggerne og samtidig ivareta dem som har reservert seg mot digital kommunikasjon med offentlig sektor. Innbyggerne registrerer seg med e-postadresse og/eller mobilnummer i registeret og har rett til å endre eller slette registeropplysningene om seg selv.

1.3.6 Hvilke opplysninger står i register over digital kontaktinformasjon og reservasjon?

Registeret inneholder per desember 2014 følgende opplysninger:

- Fødselsnummer eller D-nummer
- e-postadresse og/eller mobilnummer den enkelte selv har registrert
- Opplysninger om den registrertes eventuelle reservasjon mot elektronisk kommunikasjon
- Eventuell adresse til innbyggers valgte digitale postkasse
- Andre opplysninger som er nødvendig for forvaltningens elektroniske kommunikasjon i forbindelse med saksbehandling og utføring av forvaltningsoppgaver

Dette er opplysninger som kan registreres uten samtykke. Det er i tillegg lov til å registrere navn og den registrertes fullmaktsforhold i det samme registeret uten samtykke. Dette er opplysninger som per desember 2014 ikke inngår i registeret.

Les mer:

- eForvaltningsforskriften kapittel 7 og § 38 [lenke til Lovdata].

1.3.7 Hva innebærer reservasjonsretten? Hva reserverer jeg meg mot?

Privatpersoner kan reservere seg mot å få enkeltvedtak eller tilsvarende tilsendt elektronisk. Innbygger reserverer seg via norge.no eller per telefon 800 30 300. Når man har reservert seg mot digital kommunikasjon med offentlig sektor gjelder det generelt for stat og kommune. Forvaltningen vil da sende enkeltvedtak eller tilsvarende med ordinær post på papir.

Det er ikke en generell adgang til å reservere seg mot å få all informasjon og generelle servicemeldinger elektronisk fra forvaltningen. F.eks. kan kommunen sende beskjed om stengning av vann per SMS også til personer som har reservert seg.

Reservasjonsretten gjelder kun for privatpersoner. Næringsdrivende og andre enheter som er registrert i enhetsregisteret, har ikke adgang til å reservere seg mot elektronisk kommunikasjon fra forvaltningen.

Les mer:

- eForvaltningsforskriften § 9 [lenke].

1.3.8 Hva er forskjellen på å slette seg fra kontakt- og reservasjonsregisteret og å reservere seg mot digital kommunikasjon med offentlig sektor?

Innbyggere kan reservere seg mot å få enkeltvedtak og tilsvarende elektronisk fra forvaltningen, se kapittel 1.3.7. Slik reservasjon ikke til hinder for at forvaltningen sender servicemeldinger og generell informasjon til innbyggeren, eller at den tar kontakt med vedkommende elektronisk eller per telefon i forbindelse med saksbehandling eller andre forvaltningsoppgaver.

Dersom du sletter deg fra kontaktregisteret, vil enkeltvedtak og tilsvarende bli sendt deg på papir. Du kan heller ikke motta annen type informasjon eller servicemeldinger på sms eller e-post. Dersom du sletter deg fra kontaktregisteret, kan du heller ikke bruke MinID til å logge inn på offentlige tjenester på nett.

Når man ikke er oppført i kontakt- og reservasjonsregisteret (fordi man aldri har vært registrert eller fordi man har slettet seg) har forvaltningen ikke kontaktinformasjon for å varsle om enkeltvedtak eller tilsvarende som sendes elektronisk, se omtale i pkt. 1.3.4. Det er da ikke behov for å reservere seg.

Les mer:

- eForvaltningsforskriften kapittel 7, og § 38 [lenke].

2. For forvaltningsorganene og deres ansatte

2.1 Om elektronisk kommunikasjon med forvaltningens brukere

2.1.1 Hva og hvordan kan forvaltningsorganet kommunisere digitalt med sine brukere?

Forvaltningen kan velge hvordan de ønsker å kommunisere digitalt så lenge sikkerheten i kommunikasjonsformen er ivaretatt. Forvaltningen kan kommunisere per e-post, etablere egne nettløsninger eller portaler, eller benytte fellesløsninger, som Altinn eller digital postkasse avhengig av hva forvaltningen finner hensiktsmessig, og så lenge kommunikasjonen skjer på en betryggende måte.

Enkeltvedtak og andre viktige meldinger skal som utgangspunkt gjøres tilgjengelig i egnet informasjonssystem. Dette gjelder følgende meldingstyper:

- 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.

I denne veilederen brukes «enkeltvedtak, eller tilsvarende» for å vise at også disse meldingene er inkludert.

Hvis mottakeren er privatperson som har registrert seg med digital postkasse (se punkt 1.3.1 ovenfor), er statlige forvaltningsorganer i utgangspunktet pålagt å sende digital post til denne postkassen. Dette fremgår av digitaliseringsrundskrivet punkt 1.2.[8]

Forvaltningsorgan skal koble seg til register over digital kontaktinformasjon og reservasjon og ta dette i bruk innen 1. januar 2016. Så snart registeret er tatt i bruk, er det ikke nødvendig å innhente samtykke for å kommunisere digitalt med privatpersoner og enheter som ikke er registrert i Enhetsregisteret.

Før forvaltningsorganet kommuniserer digitalt med privatpersoner, må organet undersøke om vedkommende har reservert seg mot digital kommunikasjon. Dette gjøres ved oppslag i kontakt- og reservasjonsregisteret.

[8] http://www.regjeringen.no/nb/dep/kmd/dok/rundskriv/2014/Digitaliseringsrundskrivet.html?id=766322

Forvaltningen skal sørge for at varsel om at enkeltvedtak er fattet blir sendt parten og om hvor og hvordan vedkommende kan skaffe seg kunnskap om innholdet. Tilsvarende gjelder for den type meldinger som er omtalt over. Er mottaker en privatperson er det en varslingsadresse i kontakt- og reservasjonsregisteret som skal benyttes. Er mottakeren næringsdrivende skal en oppdatert elektronisk adresse som enheten har oppgitt benyttes til varsling. Dersom brevet ikke åpnes innen en uke etter at det ble gjort tilgjengelig, sendes det nytt varsel.

Les mer:

- eForvaltningsforskriften §§ 8, 9 og 37
- Digitaliseringsrundskrivet punkt 1.2.

2.1.2 Må forvaltningsorganet bruke register over digital kontaktinformasjon og reservasjon?

Alle forvaltningsorganer som kommuniserer elektronisk med innbyggere skal være koblet til registeret og benytte seg av varslingsadressene i dette registeret innen 1. januar 2016.

Registeret inneholder kun informasjon om privatpersoner og enheter som ikke er registrert i Enhetsregisteret. Registeret kan derfor kun benyttes til kommunikasjons med innbyggere, ikke til i kommunikasjon med næringslivet.

Etter forskriften bør den enkelte som er registrert i registeret minst to ganger årlig oppfordres til å oppdatere eller bekrefte at opplysningene som er registrert om vedkommende er korrekte. Dette ivaretas av ID-porten i forbindelse med innlogging til offentlig tjenester på nett. Hver nittiende dag må man oppdatere/bekrefte sine kontaktopplysninger før innlogging. Dersom opplysningen ikke har blitt oppdatert eller bekreftet på 18 måneder, kan ikke forvaltningsorganet benytte opplysningene til varsling.

Les mer:

- eForvaltningsforskriften §§ 31, 32 og 37.
- Digitaliseringsrundskrivet punkt 1.2.

2.1.3 Kan forvaltningsorganet sende enkeltvedtak med e-post?

Når forvaltningen ønsker å sende et enkeltvedtak, eller tilsvarende, med elektronisk kommunikasjon er utgangspunktet at det må benyttes et «egnet informasjonssystem» ihht. eForvaltningsforskriften § 8. (For eksempel Digital postkasse til innbyggere, Altinn eller tjenester hos den enkelte virksomhet.). Det vil si at man som regel ikke har adgang til å sende enkeltvedtak eller tilsvarende med e-post.

I enkelte tilfeller kan det likevel være adgang til å sende ut enkeltvedtak eller tilsvarende på vanlig e-post. Dette vil imidlertid bero på at parten ber om det, at det ikke er hensiktsmessig å kommunisere via egnet informasjonssystem, at det er forsvarlig, og at annet regelverk på området ikke er til hinder. Alle disse vilkårene må være oppfylt for at man skal kunne sende enkeltvedtak eller tilsvarende med e-post.

Dersom parten ønsker bruk av en forsendelsesmåte som forvaltningsorganet ellers ikke ville kunne benytte, vil det påhvile forvaltningen et særlig ansvar for å sikre at situasjonen er slik at det

likevel fremstår som forsvarlig og at parten har forstått og akseptert restrisikoen, jf. den tilsvarende veiledningsplikten i § 5 annet ledd for kommunikasjon til organet.

Forvaltningsorganet må sikre at bare rette vedkommende får tilgang til vedtaket (autentisering). Dessuten må underretning gis på en slik måte at forvaltningsorganet kan registrere når parten faktisk skaffer seg tilgang til vedtaket. Den som skal motta vedtaket skal få varsel) om at et vedtak er fattet (om vedtaket sendes på e-post, anses varslingsplikten oppfylt), og om hvordan vedkommende kan få tilgang til vedtaket (laste det ned). Hvis vedkommende ikke har skaffet seg tilgang til vedtaket innen en uke, skal det sendes nytt varsel på e-post og/eller SMS.

Les mer:

- eForvaltningsforskriften § 8 [lenke til Lovdata] med kommentarer [Lenke til Veilederen del 3 – Forskrift med noteapparat, § 8]
- Mer om denne delen av eForvaltningsforskriften i en annen del av veilederen som er tilgjengelig her [Lenke til Veilederen del 1, kapittel 3.7].

2.1.4 Må forvaltningsorganet ved utsending av enkeltvedtak varsle mottaker både på e-post og i sms?

Nei, forvaltningen velger om de vil varsle per e-post eller sms. Dersom forvaltningsorganet har ønske om å benytte en bestemt kanal, for eksempel e-post, men mottaker ikke har oppgitt den aktuelle digitale kontaktadressen, kan denne kommunikasjonsformen ikke benyttes

For privatpersoner og enheter som ikke er registrert i enhetsregisteret er det opplysningene i kontakt- og reservasjonsregisteret som brukes. Om innbygger der *kun* har registrert enten e-postadresse eller mobilnummer, er det denne adressen som skal benyttes.

Er mottakeren næringsdrivende må varslingsadressen være oppdatert og stamme fra enheten.

Les mer:

- eForvaltningsforskriften § 8 tredje ledd. [lenke til Lovdata].

2.1.5 Hva er konsekvensen hvis forvaltningens brukere ikke leser et enkeltvedtak eller tilsvarende som det er gitt underretning om?

Informasjonssystemet som benyttes skal registrere tidspunktet for når mottaker har skaffet seg tilgang til enkeltvedtak eller lignende. Dette er i stor grad en teknisk funksjonalitet som følger med på om mottaker har åpnet enkeltvedtak eller lignende. Hvis det ikke blir åpnet innen en uke, skal det sendes nytt varsel. Bakgrunnen for denne reglen er å forhindre at mottaker lider et rettstap. Når mottaker er varslet to ganger, bør mottaker ha blitt tilstrekkelig oppfordret til å gjøre seg kjent med enkeltvedtaket eller tilsvarende, og ytterligere varsling er ikke nødvendig.

Klagefrist løper fra første varsel ble sendt. Skulle det vise seg at parten, til tross for dobbelt varsling, likevel ikke blir oppmerksom på enkeltvedtak eller tilsvarende, slik at en frist blir oversittet, må tilfellet håndteres som om parten hadde oversett, eller hevder ikke å ha mottatt, et papirbasert brev, herunder om det kan gis oppreisning for fristoversittelse etter forvaltningsloven § 31. Det skal i den sammenheng legges vekt på om parten kan lastes for å ha oversittet fristen.

Les mer:

- eForvaltningsforskriften § 8 og § 11.

2.1.6 Kan forvaltningsorganet "underskrive" sine avgjørelser og vedtak med elektronisk signatur?

Det er ikke vanskelig å tenke seg at forvaltningsorganets saksbehandlere, på samme måte som enhver som henvender seg med bruk av elektronisk kommunikasjon til forvaltningsorganet, kan benytte elektronisk signatur.

Det er imidlertid *forvaltningsorganets kompetanse* til å fatte nærmere bestemte avgjørelser og vedtak som er viktig for den enkelte. Derved er det viktigere å få visshet om at avsenderen virkelig er *forvaltningsorganet*, enn å kunne få bekreftet hvem i forvaltningsorganet som er saksbehandler (selv om det av og til kan være hensiktsmessig å vite hvem som er saksbehandler).

Som en konsekvens av dette kan forvaltningsorganet som sådant "signere" avgjørelser og vedtak som fattes av organet. Forvaltningsorganet kan benytte en bestemt type elektronisk identitetsbevis som kalles "virksomhetssertifikat" [lenke til eForvaltningsforskriften § 16] for å identifisere forvaltningsorganet.

Hvilke personer i organet som er autorisert til å benytte en slik signatur vil følge av de fullmakter organet har gitt sine ansatte. Dette vil ikke være noe annerledes enn andre typer fullmakter gitt til enkeltpersoner eller lagt til en bestemt stilling eller rolle i organet. Det mest vanlige er at virksomhetssertifikater er knyttet til signaturfremstillingsdata som er lagret sentralt. Aktivering av signaturfremstillingsdata, som påfører signaturen, vil være gjenstand for rollebasert tilgangskontroll, og saksflyt- eller arkivsystemet vil registrere hvem som aktiverte dataene (og altså utløste påføring av signaturen). Er det flere i forvaltningsorganet som har fullmakt til å benytte virksomhetssertifikat som er lagret lokalt eller på individuelle smartkort e.l., bør de utstyres med hvert sitt sertifikat. Dette gjør det lettere å spore tilbake hvilke(n) person(er) som har disponert på organets vegne når dette ikke ivaretas sentralt i løsningen.

Les mer:

- Reglene om virksomhetssertifikater i eForvaltningsforskriften § 16 [lenke til Lovdata] med kommentarer [Lenke til Veilederen del 3 – Forskrift med noteapparat, § 16]
- Mer om denne delen av eForvaltningsforskriften i en annen del av veilederen som er tilgjengelig her [Lenke til Veilederen del 1, kapittel 4.2].

2.1.7 Hva skal forvaltningsorganet gjøre når det mottar en signert melding?

Hvordan forvaltningsorganet skal behandle en signert melding som organet mottar, avhenger av hva slags melding det dreier seg om, hvilke krav som er stilt til den aktuelle meldingen og til signaturen og hvilken type signatur det er snakk om.

Hvis det ikke er stilt noen krav om at meldingen skal signeres, og man egentlig ikke har behov for å vite hvem avsenderen er, for eksempel fordi det kun dreier seg om et generelt spørsmål, som ikke er relatert til en bestemt sak, kan man se helt bort fra signaturen. Da kan henvendelsen

besvares uten at man vurderer signaturen nærmere. Det er da heller ikke særlige krav til arkivering av signaturen.

Hvis meldingen er av en slik art at det er av betydning for den videre behandlingen om man kan stole på signaturen, eller det følger av regelverket at det skal benyttes en "avansert elektronisk signatur" eller lignende, er det flere ting man må ta hensyn til.

Når man mottar et dokument med en elektronisk signatur, kan systemet foreta en teknisk kontroll av at signaturen lar seg verifisere med det sertifikatet som hører til meldingen, og at ikke meldingen er endret. Hvis systemet ikke "kjenner igjen" den sertifikattypen som er benyttet, kan det hende du få varsel om at systemet ikke har "tillit til" sertifikatet. Dette behøver ikke bety at det er noe galt med sertifikatet, men kan for eksempel skyldes at det er første gang et sertifikat av denne typen er benyttet. Forvaltningsorganet, eller den som håndterer sertifikatet på vegne av organet, må da vurdere om den sertifikattypen som er benyttet er anvendelig for det aktuelle formålet. Hvis det ikke lar seg gjøre å få bekreftet at sertifikatet er anvendelig for det aktuelle formålet, må den signerte meldingen avvises og avsenderen må få melding om dette og årsaken til avvisningen. Reglene om behandling av meldinger som ikke tilfredsstiller aktuelle krav står i eForvaltningsforskriften § 7, jf. § 27 siste ledd [lenker til Lovdata]. Du kan se kommentarene til denne bestemmelsen her [Lenke til Veilederen del 3 – Forskrift med noteapparat, § 7].

I forbindelse med arkivering av en melding som er signert med "avansert elektronisk signatur", må det av og til innhentes opplysninger i tillegg til de som følger med meldingen. Hvis forvaltningsorganet benytter elektronisk arkiv, og gir innsyn i arkivert materiale i elektronisk form, må man også ta hensyn til reglene om hvordan signerte elektroniske meldinger skal utleveres. Reglene om innsyn og utlevering står i eForvaltningsforskriften § 12 [lenke til Lovdata]. Du kan se kommentarene til denne bestemmelsen her [Lenke til Veilederen del 3 – Forskrift med noteapparat, § 12] og lese mer om denne delen av eForvaltningsforskriften i en annen del av veilederen som er tilgjengelig her [Lenke til Veilederen del 1, kapittel 3.9].

Les mer:

- eForvaltningsforskriften § 27 og § 28 [lenke til Lovdata[9]] med kommentarer til § 27 her og § 28 her [Lenke til Veilederen del 3 – Forskrift med noteapparat, hhv § 27 og § 28]
- Mer om denne delen av eForvaltningsforskriften i en annen del av veilederen som er tilgjengelig her [Lenke til Veilederen del 1, hhv kapittel 4.3 og 4.4].

2.2 Om sikkerhetsmål, sikkerhetsstrategi, sikkerhetstjenester, sikkerhetsprodukter og internkontroll

2.2.1 Hva er en sikkerhetsstrategi?

Forvaltningsorganet har plikt til å utarbeide sikkerhetsmål og sikkerhetsstrategi. Sikkerhetsmål skal beskrive overordnede formål med informasjonsbehandlingen og overordnede prinsipper for arbeidet og ikt-bruken. Sikkerhetsstrategien bør inneholde retningslinjer for hvordan sikkerhetsarbeidet skal gjennomføres (internkontrollen) og retningslinjer for relevante områder.

[9] eForvaltningsforskriften §§ 25, 26 http://www.lovdata.no/for/sf/fa/ta-20040625-0988-006.html#25

Det er virksomhetens kompleksitet, risiko og behov som bør avgjøre omfang, innretning og detaljeringsnivå på sikkerhetsmål og sikkerhetsstrategi.

Sikkerhetsstrategien skal ikke bare danne grunnlag for valg av sikkerhetstjenester og det nærmere nivået på sikkerheten, men skal også danne grunnlag for eventuelt å velge *bort* sikkerhetstiltak der de ut fra nærmere vurderinger ikke anses nødvendige. Ofte tas elektroniske løsninger i bruk uten nærmere sikkerhetstenkning; for eksempel skytjenester og sosiale medier. Dette er det ikke adgang til. Forskriftene krever at dette skal være en bevisst og gjennomtenkt handling, med basis i sikkerhetsstrategien. Alle steder hvor forskriften gir adgang til å anvende sikkerhetstjenester og -produkter, skal eventuelle krav være basert på forvaltningsorganets sikkerhetsstrategi.

Sikkerhetsstrategien og internkontrollen for øvrig vil ha betydning for tilliten til forvaltningsorganenes tekniske løsninger og tilliten til et forvaltningsorgans evne til å ivareta sikkerhetsbehovene i et helhetlig og organisasjonsmessig forsvarlig perspektiv. Sikkerhetsmål og -strategi anses som viktige virkemidler for at det enkelte forvaltningsorgan skal klare å gjennomføre dette på en trygg og effektiv måte, som grunnlag for at borgere og næringsliv kan ha tillit til forvaltningen. Sikkerhetstenkningen skal være en integrert del av virksomhetens øvrige planarbeid (virksomhetsstrategi, inkludert strategi for IKT og informasjonssikkerhet), slik at styring av videre valg og bruk skjer ut fra en helhetlig tenkning.

Enhver bruk av elektronisk signatur, kryptering og sertifikater i et forvaltningsorgan, bør være basert på og nærmere beskrevet i sikkerhetsstrategien, se efvf. § 15 fjerde ledd som gir anvisning på en rekke spesifikke temaer som er relevante for anvendelsen av eForvaltningsforskriften og som bør være adressert i sikkerhetsstrategien.

Les mer:

- eForvaltningsforskriften § 15 [lenke til Lovdata] med kommentarer her [Lenke til Veilederen del 3 – Forskrift med noteapparat, § 15]
- Mer om denne delen av eForvaltningsforskriften i en annen del av veilederen som er tilgjengelig her [Lenke til Veilederen del 1, hhv kapittel 3.3 og 4.1].

2.2.2 Hva menes med sikkerhetstjenester og -produkter og hvilke kan forvaltningsorganet benytte?

Sikkerhetstjenester og -produkter er tjenester som blant annet skal sikre autentisering, integritet, konfidensialitet og ikke-benekting. Eksempler på dette er elektroniske signaturer og kryptering.

I henhold til efvf § 4, er det opp til forvaltningsorganet selv å velge hvilke sikkerhetstjenester og -produkter de skal benytte. Valg av løsninger skal være forankret i forvaltningsorganets sikkerhetsstrategi, jf. efvf § 15.

I forbindelse med tiltak for å fremme bruk av elektroniske tjenester og for å koordinere forvaltningens bruk av sikkerhetstjenester, er forvaltningsorganets valgfrihet likevel begrenset. Det stilles i Digitaliseringsrundskrivet krav om at statlige virksomheter tar i bruk ID-porten for digitale tjenester som krever innlogging og autentisering. i tillegg skal alle statlige etater som ønsker å ta i bruk PKI for autentisering og elektronisk signatur benytte "Kravspesifikasjon for PKI i offentlig sektor" som er en forvaltningsstandard [lenke til http://www.odin.dep.no/filarkiv/234033/Kravspek_PKI_v102.pdf]. De samme løsninger

anbefales for kommunene. Se brev fra Moderniseringsdepartementet til samtlige statsetater 7. juni 2005 og brev til samtlige statsetater fra Fornyings- og administrasjonsdepartementet 20. september 2006, vedrørende "Felles sikkerhetsinfrastruktur for elektronisk kommunikasjon med offentlig sektor", på s. 3.

I kravspesifikasjonen er det definert tre (3) ulike sikkerhetsnivåer med tilhørende krav til sikkerhetstjenester. De tre sikkerhetsnivåene er: "*Person-Standard*", "*Person-Høyt*", "*Virksomhet*". Dette forenkler vurderingene for forvaltningsorganene når de skal utarbeide sin sikkerhetsstrategi og så velge sikkerhetsnivå.

Det er også stilt krav om at sertifikattjenester som skal benyttes ved kommunikasjon med og i forvaltningen skal være omfattet av den såkalte selvdeklareringsordningen. Ordningen administreres av Post- og teletilsynet.[10] Tjenester som har levert slik selvdeklarasjon, og som tilsynsorganet ikke har funnet grunn til å gripe inn mot, kan forvaltningsorganene benytte. Se eForvaltningsforskriften § 36 [lenke til Lovdata[11]]. Tilsynet vedlikeholder en liste over tjenester og produkter som er omfattet av ordningen.

Selvdeklareringsordningen er forankret i esignaturloven § 16a[12]. Denne bestemmelsen danner rammen for etablering av frivillige sertifiserings-, godkjennings- eller selvdeklareringsordninger. Slike ordninger gjør det enklere for brukerne å orientere seg blant de sikkerhetstjenester og -produkter som er tilgjengelige i markedet, og kan bidra til å etablere tillit til deres pålitelighet.

Les mer:

- Reglene om bruk av sikkerhetstjenester og -produkter står bl.a. i eForvaltningsforskriften § 4 og § 36 [lenke til Lovdata[13]] med kommentarer til § 4 og § 36 her [Lenke til Veilederen del 3 – Forskrift med noteapparat, hhv § 4, § 15 og § 36]
- Mer om disse delene av eForvaltningsforskriften i en annen del av veilederen som er tilgjengelig her [Lenke til Veilederen del 1, hhv kapittel 3.4 og 4.8].
- Se også kravspesifikasjon for PKI i offentlig sektor [lenke].

[10] Post- og teletilsynets nettsider finner du på http://www.npt.no.

[11] eForvaltningsforskriften § 27 http://www.lovdata.no/for/sf/fa/ta-20040625-0988-007.html#27

[12] esignaturloven §16a http://www.lovdata.no/all/tl-20010615-081-004.html#16a

[13] eForvaltningsforskriften http://www.lovdata.no/for/sf/fa/fa-20040625-0988.html