HØRINGSNOTAT

Digital kommunikasjon som hovedregel

Forskrift om endringer i forskrift 35. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

Sendt ut: 11. juni 2013
Høringsfrist: 13. september 2013

Innhold

1. Innledning ... 4

2. Bakgrunn ... 6

2.1 Regjeringens arbeid for digitalisering ... 6

2.2 Den norske befolkningens bruk av elektronisk kommunikasjon ... 6

2.3 Gjeldende rett ... 7

2.3.1 Prop. 116 L (2012-2013) ... 8

2.4 Elektronisk kommunikasjon i Danmark og Sverige ... 9

3. Fra samtykke til reservasjon ... 10

3.1 Fokus på de digitalt aktive ... 10

3.2 Hvem skal kunne reservere seg mot elektronisk kommunikasjon? ... 11

3.3 Hva skal man kunne reservere seg mot? ... 12

3.3.1 Reservasjon mot digital kommunikasjon fra enkeltvirksomheter, enkeltsektorer eller lignende ... 12

3.3.2 Samtykke avgitt til enkeltvirksomheter ... 13

4. Løsning for digital post fra forvaltningen og digitale postkasser ... 14

4.1 Formålet med å regulere løsning for digital post fra forvaltningen i forskrift ... 14

4.2 Løsning for digital post fra forvaltningen - konseptet ... 14

4.3 Ansvarsforhold ... 16

4.3.1 Gjeldende rett ... 16

4.3.2 Forholdet til personopplysningsloven § 3 annet ledd ... 16

4.3.3 Departementets vurderinger og forslag ... 17

4.4 Nedre aldersgrense for å kunne ha digital postkasse for mottak av digital post fra det offentlige ... 20

4.5 Tildeling av digital postkasse til innbygger ... 20

4.6 Digitale postkasser og reservasjonsretten ... 21

4.7 Varsel om ny post i den digitale postkassen ... 21

4.8 Bruk av mottakers digitale postkasse ... 22

4.9 Taushetsplikt ... 23

4.10 Lagringstid – herunder forholdet til arkivloven ... 23

4.10.1 Lagringstid ... 23

4.10.2 Forholdet til arkivloven ... 23

4.11 Bytte av postkasseleverandør og avvikling av en markedsbasert digital postkasse – flytting av innholdet ... 24

5. Digital kontaktinformasjon og opplysning om reservasjon ... 25
5.1 Behovet for et register over digital kontaktinformasjon og reservasjon ... 25
5.2 Regulering av register over digital kontaktinformasjon og reservasjon ... 25
5.3 Hvem skal register over digital kontaktinformasjon og reservasjon inneholde opplysninger om? ... 26
5.4 Registrering og oppdatering av digital kontaktinformasjon ... 27
5.5 Registrering av reservasjonsstatus ... 28
5.6 Bruk av opplysninger i register over digital kontaktinformasjon og reservasjon ... 28
5.7 Bruk av lokale registre over digital kontaktinformasjon ... 29
5.8 Behandlingsansvar for register over digital kontaktinformasjon og reservasjon ... 30
5.9 Taushetsplikt ... 31

6. Andre endringer i eForvaltningsforskriften ... 32
6.1 Når klagefristen begynner å løpe ... 32
6.1.1 Endring av eForvaltningsforskriften § 8 fra 1. januar 2013 og gjeldende rett ... 32
6.1.2 Departementets vurdering og forslag ... 32
6.2 Når klage er rettidig fremsatt ... 33
6.3 Ekstra elektronisk varsling ... 33
6.3.1 Endring av eForvaltningsforskriften § 8 fra 1. januar 2013 ... 33
6.3.2 Departementets vurdering og forslag ... 33
6.4 Endring av eForvaltningsforskriften § 13 – sikkerhetsmål og sikkerhetsstrategi ... 34
6.4.1 Bakgrunn ... 34
6.4.2 Departementets vurdering og forslag ... 34

7. Overgangsbestemmelser ... 36

8. Personvern og informasjonssikkerhet ... 37
8.1 Omtale av personvern i Prop. 116 L (2012-2013) ... 37
8.2 Ivaretakelse av personvern i løsning for digital post fra forvaltningen ... 37
8.3 Ivaretakelse av informasjonssikkerhet i løsning for digital post fra forvaltningen ... 38

9. Økonomiske og administrative konsekvenser ... 40

10. Merknader til de enkelte bestemmelsene ... 41

11. Utkast til forskrift om endringer i eForvaltningsforskriften ... 49

VEDLEGG ... 57
1. Kryptografisk beskyttelse av digital post ... 57

1. Innledning

Fornyings-, administrasjons- og kirkedepartementet (departementet) sender med dette endringer i forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) på høring.

Prop. 116 L (2012-2013) ble fremmet for Stortinget 12. april 2013. Proposisjonen foreslo endringer i lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven). Stortinget vedtok lovendringene 3. juni 2013, jf. Innst. 342 L (2012-2013) og Lovvedtak 72 (2012-2013). Forslagene i dette høringsnotatet er i hovedsak oppfølging av endringene i forvaltningsloven.

Forslagene omtalt i høringsnotatet kapitlene 3 og 6 gjelder digital kommunikasjon fra forvaltningen generelt, uavhengig av i hvilke tekniske løsninger kommunikasjonen skjer. Det vil for eksempel si at forslagene gjelder uavhengig av om den digitale kommunikasjonen skjer via Altinn, løsning for digital post fra forvaltningen, eller Lånekassens løsning for kommunikasjon med sine kunder. Omtalen av løsning for digital post fra forvaltningen i kapittel 4 og forslag til nytt kapittel 7 i eForvaltningsforskriften gjelder bare denne løsningen. Omtalen av register over digital kontaktinformasjon og reservasjon i høringsnotatet kapittel 5 og forslag til nytt kapittel 8 i eForvaltningsforskriften gjelder det omtalte registeret.

Elektronisk kommunikasjon fra forvaltningen til næringslivet berøres i noen grad i høringsnotatet. Forslaget om at samtykkekravet skal fjernes, gjelder også forvaltningens elektroniske kommunikasjon til næringslivet. Reguleringen av løsning for digital post fra forvaltningen omfatter imidlertid ikke digital post fra forvaltningen til næringslivet. Forvaltningens elektroniske kommunikasjon med næringslivet skjer pr. i dag i stor utstrekning via Altinn.

Samferdselsdepartementet har startet en revisjon av lov 29. november 1996 nr. 73 om formidling av landsdekkende postsendinger (postloven). Revisjonen skal inkludere regulering av digital post. Når det gjelder forholdet mellom de endringene i eForvaltningsforskriften som foreslås i dette høringsnotatet, og fremtidig regulering av digital post i postloven, er departementet åpne for at den regelverksstrukturen som er etablert i og med hjemmel i forvaltningsloven blir vurdert, dersom det blir aktuelt å lovregulere elektronisk postutveksling generelt.

Begrepene *elektronisk kommunikasjon* og *digital kommunikasjon* er brukt om hverandre i høringsnotatet, men meningsinnholdet er det samme. Bakgrunnen for dette er at begrepet som pr. i dag brukes i praksis er *digital kommunikasjon*. Regelverket, herunder forvaltningsloven, bruker imidlertid begrepet *elektronisk kommunikasjon*. I relevans til de forhold forvaltningsloven og eForvaltningsforskriften regulerer er det, slik departementet ser det, ingen tilsiktet forskjell mellom begrepene. Departementet bruker derfor de to begrepene om det samme.

Flere saksfelt innen forvaltningen er unntatt fra forvaltningslovens virkeområde. Departementet mener det er hensiktsmessig å ha en oversiktig regulering av digital kommunikasjon med og i forvaltningen, uavhengig av om forvaltningsområdet reguleres av forvaltningsloven eller ikke. Departementet ser derfor på hvordan en gjennomgang av regelverk, og eventuelle endringer som følge av en slik gjennomgang, best kan gjøres.

Departementet tar også sikte på å gjøre en språklig og pedagogisk gjennomgang av eForvaltningsforskriften mens dette høringsnotatet er på høring. Det kan derfor være at de foreslåtte endringene blir innarbeidet i en ”ny” versjon av forskriften. De språklige og/eller pedagogiske endringene vil ikke innebære noen materielle endringer, og vil derfor ikke måtte sendes på høring.

2. Bakgrunn

2.1 Regjeringens arbeid for digitalisering

Slik det framgår av Meld. St. nr. 23 (2012-2013*) Digital agenda for Norge – IKT for vekst og verdiskaping* som ble lagt fram 22. mars 2013, ønsker regjeringen å øke farten i digitaliseringen av forvaltningen og også at forvaltningens kommunikasjon som hovedregel skal skje elektronisk. Tekniske løsninger som skal etableres for å oppnå dette, er under planlegging av Difi. Mange offentlige virksomheter arbeider med digitalisering av sine offentlige tjenester. I tillegg har Direktoratet for forvaltning og IKT (Difi) felles løsninger som forvaltningen kan benytte til digital kommunikasjon, under etablering. Enkelte målsetninger er skissert av regjeringen i digitaliseringsprogrammet *På nett med innbyggerne*, som ble lagt fram i april 2012, jf. Programmets kapittel 3.3:

> *"Regjeringen tar sikte på å tilby innbyggere og næringsliv en digital postkasse hvor de kan motta digital post fra staten på en sikker måte. Den digitale postkassen vil i motsetning til vanlig e-post tilfredsstille kravene til sikkerhet. Regjeringen tar sikte på at det skal legges til rette for en toveis digital kommunikasjon mellom innbyggere og statlige virksomheter i fremtiden. Det tas sikte på at kommuner også skal kunne bruke den digitale postkassen, men dette krever samordning på kommunal side. I den digitale postkassen vil brukerne få tilgang til alle vedtak og meldinger fra det offentlige og ha oversikt over all sin digitale kommunikasjon med forvaltningen. Brukerne varsles om nye brev i postkassen på sms eller e-post."*

Løsningen for elektronisk post fra det offentlige skal ha gode systemer og rutiner for å ivareta konfidensialitet, integritet og tilgjengelighet. Dette innebærer at posten bare skal være tilgjengelig for mottakeren, at meldingen er korrekt og fullstendig og at den er tilgjengelig til rett tid.

2.2 Den norske befolkningens bruk av elektronisk kommunikasjon

En undersøkelse av nordmenns holdning til å motta post fra forvaltningen i en sikker digital postkasse, ble gjennomført av Norstat i mars 2013 på oppdrag fra Direktoratet for forvaltning og IKT (Difi). Undersøkelsen viser blant annet at 65 prosent av de spurte stiller seg positive til en sikker digital postkasse. 19 prosent stilte seg nøytrale og 17 prosent var negative. Til sammen er 84 prosent positive eller nøytrale til å motta offentlige brev i en digital postkasse. Dette er en positiv utvikling fra en sammenlignbar undersøkelse vinteren 2011. Da svarte 40 prosent at de foretrekker å motta brev fra stat og kommune elektronisk, mens 46 % svarte at de ikke ønsket dette. Svarene fra 2011 ble innhentet i en undersøkelse om nordmenns holdning til offentlige tjenester på internett og elektronisk ID, gjennomført av Opinion på oppdrag av Difi.

I undersøkelsen gjennomført i mars 2013 ble innbyggerne også spurt om de viktigste årsakene til at de ønsket å ta i bruk en sikker digital postkasse. De viktigste årsakene som ble angitt, var:

- bedre oversikt over brev fra det offentlige
- mindre papir i hjemmet
- tilgang til brev hvor og når som helst
- bedre for miljøet
- mer fornuftig pengebruk i det offentlige

Innbyggerne ble også spurt om de ville reservere seg mot å ta i bruk en sikker digital postkasse og heller motta brev på papir. 31 prosent svarte at de ville reservere seg. De viktigste grunnene som ble angitt for dette, var:

- at papir er enklere å forholde seg til og mer oversiktlig
- frykt for dårlig sikkerhet
- ønske om å arkivere manuelt
- usikkerhet om hvem som har ansvaret dersom noe skulle komme på avveie
- lav datakunnskap
- usikkerhet om hvem som skal spørres ved behov for hjelp.

Norge har en befolkning som i stor grad benytter seg av elektroniske løsninger. Det er registrert over 2,9 millioner brukere av MinID i ID-porten. To av tre søknader om pensjon sendes på nett. Tall fra Statistisk sentralbyrås undersøkelse *IKT-bruk i husholdningene, 2012, 2. kvartal viser dessuten (undersøkelsen omfatter norske innbyggere fra og med 16 år til og med 74 år):*

- 93 prosent av norske husholdninger i 2012 har tilgang til internett i hjemmet (tallet gjelder for husholdninger der minst én er under 75 år).
- 86 prosent av den norske befolkningen bruker internett hver dag.
- Tilgang til og bruk av internett øker mest blant de eldste gruppene i befolkningen.
- 86 prosent av den norske befolkningen bruker nettbank.
- Åtte av ti innbyggere har vært i kontakt med offentlige myndigheter via internett det siste året. Blant de i aldersgruppen 65-74 år er tallet syv av ti.

Selv om enkelte undersøkelser viser at ikke alle innbyggere er like klare for å ta i bruk løsninger for elektronisk kommunikasjon, er det grunn til å si at Norge samlet sett har en digitalt moden befolkning. Tall for bruk av nettbank indikerer for øvrig at innføring av gode tekniske løsninger medfører at bruken øker.

2.3 Gjeldende rett

Forvaltningsloven ble endret ved lov 21. desember 2001 nr. 117 for å legge til rette for elektronisk kommunikasjon på forvaltningsrettens område. Loven har likevel ingen omfattende regulering av elektronisk kommunikasjon, men hjemler i stedet – sammen med lov 15. juni 2001 nr. 81 om elektronisk signatur – utfyllende regler fastsatt i eForvaltningsforskriften.

Et forvaltningsorgan kan bare formidle forhåndsvarsel og underretning om et enkeltvedtak elektronisk dersom mottakeren har gitt sitt uttrykkelige samtykke til dette. Dette følger av forvaltningsloven § 16 og § 27 og er utdypet i eForvaltningsforskriften § 8.

Uttrykkelig samtykke må også innhentes i forkant for *"andre meldinger som har betydning for mottakerens rettsstilling, for behandlingen av saken eller for meldinger som det av andre grunner er av særlig betydning å sikre at vedkommende mottar",* jf. eForvaltningsforskriften § 8 nr. 6.

Når det gjelder den enkeltes anledning til å henvende seg elektronisk til et forvaltningsorgan, er dette i all hovedsak regulert i eForvaltningsforskriften. Bare enkelte fragmenter framgår av forvaltningsloven – slik som muligheten til å framsette en klage elektronisk, jf.

Forvaltningsloven § 32 fjerde ledd. Den praktiske hovedregelen framgår av eForvaltningsforskriften § 3 nr. 1:

> *«Enhver som henvender seg til et forvaltningsorgan kan benytte elektronisk kommunikasjon når det skjer i henhold til den form og fremgangsmåte og ved bruk av den elektroniske adressen som forvaltningsorganet har anvist for den aktuelle type henvendelse.»*

I tillegg finnes det en rekke bestemmelser om elektronisk kommunikasjon mellom forvaltningen og publikum i særlovgivningen.

Lov 14. april 2000 nr 31 om behandling av personopplysninger (personopplysningsloven) § 2 definert personopplysninger som *"opplysninger og vurderinger som kan knyttes til en enkeltperson"*. Eksempler på personopplysninger er navn, fødselsdato, yrke, telefonnummer og e-postadresse.

"[B]ehandling av personopplysninger" er et vidt begrep, og omfatter etter definisjonen i personopplysningsloven "enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller kombinasjoner av slike bruksmåter". Personopplysningsloven §§ 8, 9 og 11 oppstiller visse grunnkrav til behandling av personopplysninger. Disse kravene må oppfylles for at behandlingen skal være lovlig.

2.3.1 Prop. 116 L (2012-2013) og Innst. 342 L (2012-2013)

Forslagene i Prop. 116 L (2012-2013) ble vedtatt i Stortinget 3. juni i år, jf. Innst. 342 L (2012-2013) og Lovvedtak 72 (2012-2013). Fra proposisjonen siteres fra kapittel 1 *Proposisjonens hovedinnhold*:

> *"Forslaget tar sikte på å styrke forvaltningens adgang til å kommunisere elektronisk gjennom å oppheve dagens krav om først å måtte innhente et samtykke fra den enkelte mottaker. I stedet vil forvaltningen som hovedregel ha lov til å kommunisere elektronisk. Forvaltningsloven skal imidlertid åpne for at privatpersoner kan reservere seg mot elektronisk kommunikasjon og i stedet motta tradisjonell post fra forvaltningen.*
>
> *Videre foreslås det å presisere og utvide den forskriftskompetansen Kongen har etter forvaltningsloven for så vidt gjelder elektronisk kommunikasjon. Kongen skal kunne gi forskrift om registrering av kontaktinformasjon for privatpersoner mv. og deres fullmaktsforhold og om adgang for privatpersoner mv. til å reservere seg mot elektronisk kommunikasjon og den registrering dette forutsetter. Det foreslås presisert at Kongen kan gi regler om hvordan elektronisk kommunikasjon kan skje. Sammen med de fullmaktsbestemmelsene som foreslås videreført, vil dette gi grunnlag for å gi nærmere regler om en sikker løsning for digital post fra det offentlige som ledd i forvaltningens elektroniske kommunikasjon med den enkelte.*
>
> *Det foreslås videre en bestemmelse om at den enkelte kan kommunisere elektronisk med forvaltningsorganer dersom disse har lagt til rette for dette og det skjer på den anviste måten. Reguleringen av dette finnes i dag hovedsakelig i forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)."*

Fra Innst. 342 L (2012-2013) siteres fra *Komiteens merknader*:

> *"Komiteen er av den oppfatning at det er viktig at offentlige organer i utstrakt grad tar i bruk teknologi og de muligheter som denne teknologien representerer både for det offentlige selv og for den enkelte bruker og borger. Ved å ta i bruk moderne teknologiske løsninger vil offentlige organer bli lettere tilgjengelige for borgerne, og en vil på sikt kunne få en offentlig sektor som tilnærmet vil være tilgjengelig for befolkningen 24 timer i døgnet. Det vil også bli langt raskere å få svar på søknader, spørsmål, skatteoppgjør o.l.*
>
> *Komiteen har merket seg at privatpersoner selv fortsatt skal kunne velge om vedkommende ønsker elektronisk kommunikasjon eller ikke. Den som velger å ikke reservere seg, har dermed en klar oppfordring til å innrette seg slik at elektroniske henvendelser ikke overses. Komiteen har på den bakgrunn merket seg at regjeringen presiserer at denne valgfriheten skal være reell og at reservasjonsordningen skal utformes slik at personer som ikke mestrer eller har tilgang til nødvendige teknologiske løsninger, ikke må reservere seg gjennom bruk av slike verktøy. Komiteen vil presisere viktigheten av at gjennomføringen av reservasjonen gjennomføres på en brukervennlig måte slik at alle får et reelt valg til å kunne reservere seg. Komiteen presiserer at det fortsatt er mange innbyggere som fortsatt ikke bruker teknologiske verktøy, har sperrer mot å benytte slike eller fortsatt føler størst trygghet med å få offentlig korrespondanse på papir. Komiteen har for øvrig ikke ytterligere merknader og slutter seg til forslaget"*

2.4 Elektronisk kommunikasjon i Danmark og Sverige

Danmark har ingen omfattende regulering av elektronisk kommunikasjon sammenliknbar med den Norge har gjennom forvaltningsloven og eForvaltningsforskriften. Etter lov nr. 528 af 11/06/2012 om Offentlig Digital Post får imidlertid innbyggere og virksomheter en plikt til å motta henvendelser fra det offentlige i sin elektroniske postkasse, kalt Offentlig Digital Post. Privatpersoners tilknytning til ordningen skal skje i november 2014, mens det for virksomheter skal skje i løpet av 2013. I mellomtiden er det frivillig for den enkelte å registrere seg for bruk av systemet. Rettsvirkningene av å motta elektronisk post skal være som for tradisjonell papirpost. Adressater som ikke er i stand til å motta henvendelser fra det offentlige elektronisk, kan søke om fritak.

Heller ikke Sverige har noen omfattende regulering av elektronisk kommunikasjon sammenliknbar med den Norge har. De reglene som finnes, er i stedet spredt i særlovgivningen. Det er opp til forvaltningen å avgjøre om bruk av elektronisk kommunikasjon er passende og forsvarlig i det enkelte tilfellet.

Det svenske Skatteverket har etablert et system der den enkelte ved bruk av elektronisk ID får tilgang til en sikker digital postkasse. Skatteverket skal også opprette et register over dem som slutter seg til infrastrukturen – både over enkeltpersoner som ønsker å motta henvendelser elektronisk, og over leverandører av elektroniske tjenester for postforsendelse og elektroniske postkasser. I første fase vil postkassetjenesten tilbys av Skatteverket, men etter hvert skal det også åpnes for private postkasseleverandører.

3. Fra samtykke til reservasjon

Kravet til samtykke til elektronisk kommunikasjon i forvaltningsloven er foreslått erstattet med en rett til å reservere seg, jf forslaget i Prop. 116 L (2012-2013). Nedenfor følger omtale av hvordan departementet foreslår at denne endringen reguleres i eForvaltningsforskriften.

3.1 Fokus på de digitalt aktive

Departementets utgangspunkt er at forvaltningen skal kunne kommuniserer digitalt med alle innbyggere som ikke aktivt har reservert seg. Det er imidlertid en begrensning knyttet til dette utgangspunktet.

Digital kommunikasjon til innbyggerne må sees i sammenheng med digital kontaktinformasjon. Mottaker av digitale meddelelser fra forvaltningen skal få varsel om hvor meddelelsen kan finnes. Dette forutsetter at det finnes oppdatert digital kontaktinformasjon til mottaker. Se nærmere i kapittel 5.4 for omtale av hvordan registreringen og oppdatering av digital kontaktinformasjon skal foregå.

Kravet om at den forvaltningen skal kommunisere digital med, har oppdatert digital kontaktinformasjon, medfører at det er flere enn de som aktivt har reservert seg som forvaltningen ikke kan kommunisere med digitalt. Endringen fra et krav om samtykke til en reservasjonsrett får på bakgrunn av dette et fokus på det departementet mener er de digitalt aktive i befolkningen. Departementet legger til grunn at innbyggere som har oppgitt sin digitale kontaktinformasjon til forvaltningen, til en viss grad er digitalt aktive. Det er heller ikke usannsynlig at de som er digitalt aktive, ønsker bruk av digital kommunikasjon.

I Digitaliseringsprogrammet[1] står det:

> *"Det vil kunne gjøres unntak for innbyggere som av særskilte grunner ikke kan forventes å kunne benytte seg av reservasjonsretten, for eksempel av helsemessige grunner."*

Departementet mener innbyggere som av ulike grunner ikke kan benytte seg av reservasjonsretten, er ivaretatt ved at en viss grad av aktivitet fra innbyggers side er påkrevd for at forvaltningen skal kunne kommunisere digitalt med vedkommende. Det vil si at en mottaker som ikke har oppgitt digital kontaktinformasjon til forvaltningen ikke vil motta meddelelser elektronisk. De gruppene i befolkningen som eventuelt ikke kan benytte seg av reservasjonsretten har, med stor sannsynlighet, ikke oppgitt digital kontaktinformasjon til forvaltningen. Forvaltningen vil derfor i praksis være forhindret fra å kommunisere digitalt med disse.

Departementet er opptatt av at reservasjonsretten skal være reell. Det vises også til Innst. 342 L (2012-2013), hvor Justiskomiteen uttaler:

> *"Komiteen har merket seg at privatpersoner selv fortsatt skal kunne velge om vedkommende ønsker elektronisk kommunikasjon eller ikke. Den som velger å ikke reservere seg, har dermed en klar oppfordring til å innrette seg slik at elektroniske henvendelser ikke overses. Komiteen har på den bakgrunn merket seg at regjeringen presiserer at denne valgfriheten skal være reell og at reservasjonsordningen skal utformes slik at personer som ikke mestrer eller har tilgang til nødvendige teknologiske*

[1] Under punkt 3.8 på side 28.

løsninger, ikke må reservere seg gjennom bruk av slike verktøy. Komiteen vil presisere viktigheten av at gjennomføringen av reservasjonen gjennomføres på en brukervennlig måte slik at alle får et reelt valg til å kunne reservere seg. Komiteen presiserer at det fortsatt er mange innbyggere som fortsatt ikke bruker teknologiske verktøy, har sperrer mot å benytte slike eller fortsatt føler størst trygghet med å få offentlig korrespondanse på papir."

3.2 Hvem skal kunne reservere seg mot elektronisk kommunikasjon?

Prop. 116 L (2012-2013) står det følgende om hvem som skal kunne reservere seg mot elektronisk kommunikasjon på side 10 første spalte:

> *"Med hensyn til reservasjonsadgangen foreslås det at forskriftskompetansen er begrenset til å gi regler om adgangen for privatpersoner mv. til å reservere seg mot elektronisk kommunikasjon og om registrering av reservasjonene. Dette har naturlig sammenheng med at det er for privatpersoner mv. det etter forvaltningsloven skal kunne opprettes register for elektronisk kontaktinformasjon."*

Departementet foreslår, i tråd med forslaget i lovproposisjonen, at de som skal kunne reservere seg mot elektronisk kommunikasjon er privatpersoner og enheter som ikke er registrert i Enhetsregisteret.

Enkeltpersonforetak står i en særstilling sammenlignet med andre former for foretak, i den forstand at det er nær sammenheng mellom privatpersonen og foretaket ettersom næringsvirksomheten ikke er organisert som en egen juridisk person. Det er allikevel ikke tradisjon for å regulere enkeltpersonforetak vesentlig annerledes enn andre typer foretak, når det gjelder på hvilken måte det offentlige kan henvende seg til næringslivet. Departementets forslag innebærer derfor at enkeltpersonforetak, på lik linje med andre enheter registrert i Enhetsregisteret, ikke vil kunne reservere seg mot elektronisk kommunikasjon fra det offentlige.

Det ligger til avsendervirksomheten å vurdere om den aktuelle henvendelsen skal sendes vedkommende som privatperson eller som enkeltpersonforetak. Dersom det er tvil om personen opptrer i rollen som privatperson eller næringsdrivende, kan det vurderes om henvendelsen bør sendes i flere kanaler.

Frivillige organisasjoner som ønsker det kan registrere seg i Frivillighetsregisteret. Registrering i Frivillighetsregisteret er en forutsetning for å kunne delta i Grasrotandelen[2] og også for å kunne få momskompensasjon[3]. Enkelte offentlige og private tilskuddsordninger forutsetter også registrering i Frivillighetsregisteret.

Frivillige organisasjoner som vil registrere seg i Frivillighetsregisteret må også være registrert i Enhetsregisteret. For frivillige organisasjoner innebærer departementets forslag derfor at de som registrerer seg i Frivillighetsregisteret, og da også Enhetsregisteret, ikke vil kunne reservere seg mot digital kommunikasjon fra det offentlige.

---

[2] En ordning som gjør det mulig for spillere hos Norsk Tipping å gi en andel på 5 prosent av innsatsbeløpet direkte til en lokal frivillig organisasjon.

[3] Det vil si at de kan søke om å få kompensasjon for moms de har betalt ved kjøp av varer og tjenester forutsatt at øvrige vilkår for søknad er oppfylt.

Hvis en forening ikke er registrert i Enhetsregisteret, og derfor ikke har et organisasjonsnummer, må det være en privatperson som står ansvarlig. Det betyr i praksis en med fødselsnummer eller d-nummer.

Det vises for øvrig til omtalen av hvem det skal kunne registreres opplysninger om i register over digital kontaktinformasjon og reservasjon i kapittel 5.3 nedenfor.

Departementets forslag til bestemmelse fremgår av utkastet til forskrift § 8 nr (2) og § 28.

3.3 Hva skal man kunne reservere seg mot?

Departementet mener at reservasjonsretten må speile de tilfeller der det i dag er krav om samtykke. Det vil si at det ikke innføres en rett til å reservere seg mot all elektronisk kommunikasjon fra forvaltningen. I så fall ville det for enkelte typer elektronisk kommunikasjon blitt en snevrere adgang til å kommunisere elektronisk enn etter dagens regelverk. Det vil ikke være i samsvar med målsettingene i regjeringens digitaliseringsprogram.

I dag er det krav om samtykke for elektronisk kommunikasjon av vedtak og forhåndsvarsel om vedtak etter forvaltningsloven §§ 16 og 27. Dette kravet er i Prop. 116 L (2012-2013) forslått fjernet. I tillegg sier eForvaltningsforskriften § 8 nr (1) og (6) følgende:

> *"(1) Underretning om enkeltvedtak kan skje ved bruk av elektronisk kommunikasjon dersom parten uttrykkelig har godtatt dette og oppgitt den elektroniske adresse forvaltningsorganet skal benytte for å sende varsel etter nr. (2) nedenfor.*
> *[...]*
> *(6) Det som er sagt om underretning om enkeltvedtak i nr. (1)–(5) ovenfor, gjelder tilsvarende ved forhåndsvarsel etter forvaltningsloven § 16 og for andre meldinger som har betydning for mottakerens rettsstilling, for behandlingen av saken eller for meldinger som det av andre grunner er av særlig betydning å sikre at vedkommende mottar."*

Departementet foreslår at det inntas en bestemmelse i eForvaltningsforskriften § 8 som fastslår at forvaltningen kan henvende seg elektronisk til andre. Videre foreslås det at eForvaltningsforskriften endres slik at elektronisk kommunikasjon av enkeltvedtak kan skje med mindre mottaker har reservert seg mot dette. Det vil da følge av eForvaltningsforskriften § 8 nr (6) (foreslått endret til nr (8)) at tilsvarende gjelder for forhåndsvarsel etter forvaltningsloven § 16 og andre meldinger som har betydning for mottakers rettsstilling, for behandling av saken eller for meldinger som det av andre grunner er av særlig betydning å sikre at vedkommende mottar.

Departementet mener at de formuleringene som foreslås ikke gjør at det innføres en reservasjonsrett mot elektronisk høring av forskriftsendringer.

Når det gjelder reservasjon mot å ha en digital postkasse, vises det til omtale av dette i kapittel 4.6.

3.3.1 Reservasjon mot digital kommunikasjon fra enkeltvirksomheter, enkeltsektorer eller lignende

Det er et spørsmål om en mottaker skal kunne velge å reservere seg mot nevnte former for elektronisk kommunikasjon fra enkeltvirksomheter, enkeltsektorer eller lignende.

Det å etablere virksomhets- eller sektorspesifikke reservasjoner er komplekst, og krever god oversikt over den enkelte sektor eller virksomhet, jf Difi-notat 2012:4 *Etablering av en løsning for reservasjon mot digital post*[4]. Difi mente i nevnte notat at en eventuell innføring av virksomhetsspesifikke eller sektorspesifikke reservasjonsordninger er noe som bør gjøres i den enkelte virksomhet eller sektor.

Det kan imidlertid være nyttig med lokale reservasjonsløsninger som supplement til en generell reservasjonsrett. Departementets vurdering er at det kan tillates lokale reservasjonsløsninger som styres, utvikles og vedlikeholdes av den enkelte virksomhet eller sektor. Det er den enkelte virksomhet eller sektor som må bestemme om de skal innføre en lokal reservasjonsrett for sine tjenester. Kompleksiteten i organiseringen av offentlig sektor og deres tjenestetilbud tilsier imidlertid at lokale reservasjonsløsninger må utvikles og vedlikeholdes av de virksomhetene som reservasjonen omfatter. For at reservasjonsretten skal være reell, må det være klart hvilke virksomheter og hvilke tjenester som omfattes av en reservasjon.

Departementet mener at det ikke er nødvendig å gi regler om at det kan innføres virksomhetsspesifikk reservasjon. Muligheten til å kunne reservere seg mot digital kommunikasjon fra enkeltvirksomheter, enkeltsektorer eller lignende er derfor ikke reflektert i utkastet til forskrift.

3.3.2 Samtykker avgitt til enkeltvirksomheter

Det er et spørsmål om en mottaker skal kunne velge å reservere seg mot elektronisk kommunikasjon generelt, men likevel kunne avgi et samtykke til enkeltvirksomheter, enkeltsektorer eller lignende som overstyrer reservasjonen.

Lokale samtykker som overstyrer en reservasjon går imot prinsippene i endringen av regelverket, som nettopp snur prinsippet fra et krav om samtykke til en rett til å reservere seg mot elektronisk kommunikasjon. Departementet mener derfor at det ikke bør legges opp til permanente løsninger hvor samtykker avgitt til enkeltvirksomheter, enkeltsektorer eller lignende kan overstyre en reservasjon. Det vises imidlertid til kapittel 7 nedenfor, hvor det foreslås at det i en periode skal være mulig å benytte elektronisk kommunikasjon basert på tidligere samtykker, også for de innbyggerne som har reservert seg. Når overgangsperioden er over, vil da en reservasjon overstyre allerede avgitte samtykke.

[4] http://www.difi.no/artikkel/2013/02/etablering-av-en-losning-for-reservasjon-mot-digital-post-difi-notat-2012-4

4. Løsning for digital post fra forvaltningen og digitale postkasser

4.1 Formålet med å regulere løsning for digital post fra forvaltningen i forskrift

Personopplysningsloven krever at all behandling av personopplysninger skal ha et behandlingsgrunnlag. Personopplysningsloven § 8 oppstiller de ulike behandlingsgrunnlagene. I tillegg krever personopplysningsloven § 9 at flere vilkår er oppfylt dersom det er sensitive personopplysninger som skal behandles.

Når det gjelder løsning for digital post fra forvaltningen, er det tre behandlingsgrunnlag som utpeker seg som relevante. Disse er samtykke fra den opplysningene gjelder, lovgrunnlag eller at behandlingen av personopplysninger er nødvendig for å utøve offentlig myndighet, jf personopplysningsloven § 8 e).

Innføring av digital kommunikasjon som hovedregel og forslaget i Prop. 116 L (2012-2013) om å snu fra et krav om samtykke til en rett til reservasjon, innebærer at samtykke ikke er et aktuelt behandlingsgrunnlag . Departementet mener også at ettersom det er snakk om å etablere en sentral, nasjonal løsning for digital post fra forvaltning til innbygger er det ryddig å regulere behandlingsgrunnlaget for personopplysningene i forskrift med hjemmel i lov, fremfor et av nødvendighetskriteriene i pol § 8.

Rammene (sikkerhetskravene og øvrige plikter) for behandlingen av personopplysninger i løsning for digital post fra forvaltningen vil som sådan kunne fastsettes privatrettslig gjennom databehandleravtalen mellom behandlingsansvarlig og databehandler. En slik løsning åpner for en fleksibilitet når det gjelder tilpasninger av avtalen basert på avsendervirksomhetens behov. Departementet kan imidlertid ikke se at det er ønskelig med en slik fleksibilitet. Dersom ulike avsendervirksomheter skal inngå databehandleravtaler med ulikt innhold vil dette kunne bli uhåndterlig å administrere. Ettersom det er ønskelig at alle avsendervirksomheter så langt som mulig skal stille de samme kravene til løsningen som sådan, er det etter departementets vurdering ryddigst at sentrale hensyn og krav reguleres i forskrift.

De bestemmelsene som foreslås når det gjelder løsning for digital post fra forvaltningen, vil ikke regulere alle sider ved løsningen. Bestemmelsen vil ikke gi et fullstendig bilde av funksjonalitet i løsningen, fordi ikke alle sider ved løsningen har behov for rettslig regulering. Videre vil allerede eksisterende regelverk regulere ulike sider ved løsningen. Slike regler er ikke nødvendigvis gjentatt i utkastet til endringer i eForvaltningsforskriften. Dette gjelder for eksempel generelle regler om behandling av personopplysninger i personopplysningsloven, regler om informasjonssikkerhet i personopplysningsforskriften og generelle regler om forsvarlig saksbehandling. Egne bestemmelser om dette er derfor ikke foreslått gjentatt i eForvaltningsforskriften.

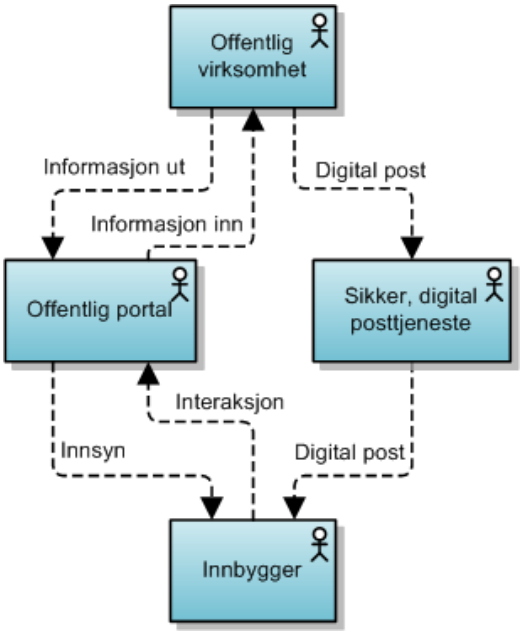
4.2 Løsning for digital post fra forvaltningen - konseptet

Løsning for digital post fra forvaltningen vil formidle digital post fra forvaltningen til innbyggere. Det er Altinn som formidler digital post fra forvaltningen til næringslivet i dag..

Selv om ikke løsningsarkitekturen for digital post fra forvaltningen som sådan skal reguleres i forskrift, mener departementet at det er viktig at høringsinstansene har et bilde av hvordan løsningen er planlagt for å kunne ta stilling til det forslaget til regelverk som foreslås.

Nedenfor følger derfor en kort beskrivelse av løsningen for sikker digital post fra forvaltningen slik den på nåværende tidspunkt er planlagt.

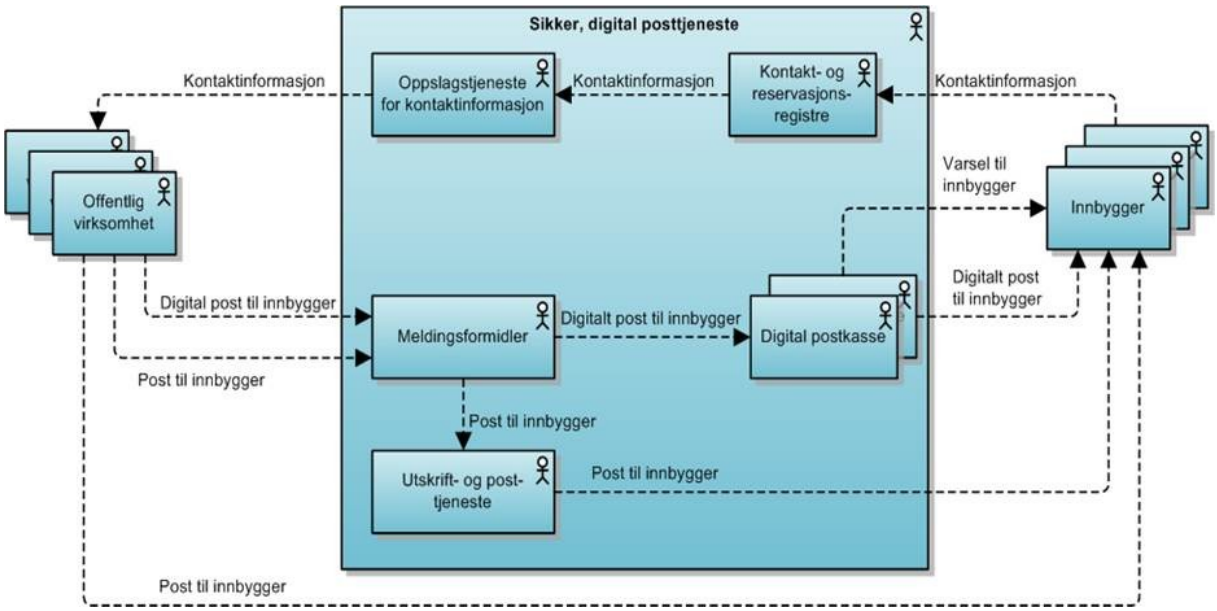
Figur 1 nedenfor viser hvordan løsning for digital post fra forvaltningen vil være et supplement til andre løsninger for elektronisk kommunikasjon mellom forvaltningen og innbyggere. eForvaltningsforskriftens bestemmelser gjelder, innenfor forvaltningslovens virkeområde, for all elektronisk kommunikasjon i figur 1. Bestemmelsene som foreslås i nytt kapittel 7 i utkastet til forskrift vil gjelde elektronisk kommunikasjon til høyre i figur 1, som illustrerer løsning for digital post fra forvaltningen



Figur 1

Løsningen består av fem sentrale deler, se figur 2:

- *Oppslagstjeneste for kontaktinformasjon*: Forvaltningens grensesnitt mot register over digital kontaktinformasjon og reservasjon.
- *Kontakt- og reservasjonsregistre*: registre for innbyggernes kontaktinformasjon til den digitale dialogen med forvaltningen. Registrene holder rede på innbyggernes valg knyttet til dialog med og postgang fra forvaltningen. Forvaltningen har tilgang til innbyggers kontaktinformasjon via oppslagstjeneste for kontaktinformasjon.
- *Meldingsformidler*: Forvaltningens grensesnitt mot posttjenesten. Har ansvaret for å formidle post til innbygger, enten som digitale brev til innbyggers selvvalgte digitale postkasse eller som papirbrev til innbyggers postadresse.
- *Digital postkasse*: Innbyggernes grensesnitt mot posttjenesten. Har ansvaret for å gjøre tilgjengelig og oppbevare innbyggers digitale brev fra forvaltningen.
- *Utskrift- og posttjeneste*: Sender papirbrev til innbygger som ikke kan eller ønsker å motta digitale brev.



Figur 2

4.3 Ansvarsforhold

4.3.1 Gjeldende rett

Behandlingsansvarlig er i personopplysningsloven § 2 nr 4 definerer som:

> *"den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes".*

Den behandlingsansvarlige har, jf. personopplysningsloven, ansvaret for at personopplysningslovens bestemmelser etterleves i forbindelse med behandling av personopplysninger, herunder beskrivelse av formålet med behandlingen, behandlingsgrunnlag, meldeplikt, informasjonsplikter, retting og sletting av opplysninger og krav til internkontroll og ivaretakelse av informasjonssikkerhet. Den behandlingsansvarlige har bestemmelsesrett med hensyn til hvilke virkemidler som benyttes og formålet med behandlingen.

Databehandler er i personopplysningsloven § 2 nr 5 definert som:

> *"databehandler: den som behandler personopplysninger på vegne av den behandlingsansvarlige".*

Databehandler har, jf. personopplysningsloven § 15, kun adgang til å behandle opplysninger innen de rammer den behandlingsansvarlige har satt i databehandleravtalen. Databehandlers selvstendige ansvar etter loven er begrenset til å ivareta krav om tilfredsstillende informasjonssikkerhet, jf personopplysningsloven § 13 og personopplysningsforskriften § 2-15 tredje ledd.

4.3.2 Forholdet til personopplysningsloven § 3 annet ledd

Personopplysningsloven § 3 annet ledd lyder:

> *"Loven gjelder ikke behandling av personopplysninger som den enkelte foretar for rent personlige eller andre private formål."*

Det kan diskuteres om den behandlingen av personopplysninger som mottaker gjør i sin digitale postkasse er *"for rent personlige eller andre private formål"*, og dermed er utenfor virkeområdet i personopplysningsloven. I så fall vil ikke personopplysningslovens regler om behandlingsgrunnlag og behandlingsansvar m.v. gjelde etter at digital post er gjort tilgjengelig for mottaker i den digitale postkassen.

De regler som er foreslått i dette høringsnotatet mener departementet er formålstjenlige uavhengig av om mottakers behandling av personopplysninger er utenfor eller innenfor personopplysningslovens virkeområde. Departementet har derfor kommet til at det ikke er behov for at det, for dette høringsnotatets formål, tas stilling til ovenfor nevnte problemstilling.

4.3.3 Departementets vurderinger og forslag

Meldinger som sendes fra forvaltningsorganer til innbyggere i løsning for digital post fra forvaltningen vil stort sett alltid inneholde personopplysninger. Det vil fremgå hvilke virksomheter som sender hvilket innhold til hvilke innbyggere. Det følger derfor av personopplysningsloven, jf omtale av gjeldende rett ovenfor, at det er knyttet ulike former for ansvar til behandlingen av slike meldinger.

Avsendervirksomhetene vil være behandlingsansvarlige for all behandling av personopplysninger som skjer i avsendervirksomheten. Dette vil ikke bli nærmere omtalt her.

Departementet foreslår bestemmelser som angir de ulike aktørenes ansvar etter at avsendervirksomheten har sendt post fra egne systemer til løsning for digital post fra forvaltningen. Det foreslås også bestemmelser om taushetsplikt og bestemmelser om behandling av trafikkdata. Departementet har i forskriftsteksten valgt å fokusere på hvilke oppgaver og ansvar den enkelte aktør har i meldingsformidlingen, men har ikke eksplisitt knyttet dette til personopplysningslovens begreper *behandlingsansvarlig* og *databehandler*. For å klargjøre forholdet til begrepene i personopplysningsloven, vil departementet allikevel knytte noen kommentarer til dette nedenfor. Ettersom departmentet ikke forslår sanksjonsbestemmelser i eForvaltningsforskriften knyttet til brudd på forskriftens bestemmelser, vil sanksjonbestemmelsene i personopplysningsloven og –forskriften gjelde for brudde på for eksempel bestemmelser om informasjonssikkerhet. Hvem som anses å være behandlingsansvarlig og databehandler har derfor betydning.

Forholdet til begrepene behandlingsansvarlig og databehandler i personopplysningsloven

Departementet vil knytte enkelte kommentarer til hvordan ansvaret for de ulike elementene ovenfor relaterer seg til begrepene *behandlingsansvarlig* og *databehandler* i personopplysningsloven.

Departementet er av den oppfatning at avsendervirksomheten etter gjeldende rett som utgangspunkt er behandlingsansvarlig fra en melding sendes til meldingen er mottatt i mottakers digitale postkasse. Etter gjeldende rett vil, slik departementet ser det, både sentralforvalter og postkasseleverandør være databehandlere på vegne av avsendervirksomheten. Postkasseleverandøren vil være databehandler for avsendervirksomheten i et kort tidsrom fra meldingen er mottatt hos postkasseleverandøren og til meldingen er lagt i mottakers digitale postkasse. Både sentralforvalter og postkasseleverandøren som databehandler vil imidlertid ha et selvstendig ansvar for overholdelse av informasjonssikkerhetsbestemmelser, jf. personopplysningsloven § 13 og personopplysningsforskriften § 2-15 tredje ledd.

Postkasseleverandøren vil i tillegg ha et selvstendig behandlingsansvar for behandlingen av personopplysninger som denne foretar. Det vises for øvrig til punkt 4.3.2 ovenfor.

Hvor bør ansvaret plasseres?
Departementet er opptatt av at behandlingen av personopplysningene i løsningen har en klar rettslig regulering, at ansvarsforholdene er klare og at opplysningene behandles med tilfredsstillende sikkerhet. Departementet har identifisert følgende ansvarsområder som relevante for en rettslig regulering knyttet til løsning for digital post fra forvaltningen:

- Sikkerhetstiltak
- Taushetsplikt
- Presisering av tilgangsregime
- Råderett
- Internkontroll

Departementet vil i det videre vurdere hvilke av aktørene – som har en rolle i løsning for digital post fra forvaltningen – som det er mest naturlig at ansvaret for de enkelte områdene nevnt ovenfor legges til. Vurderingene knytter seg blant annet til hvilken reell påvirkning de ulike aktørene vil ha når det gjelder løsningen og de virkemidler som benyttes.

Når det gjelder formålspresisering vil få eller ingen av aktørene ha direkte innflytelse på denne, ettersom formålet vil følge av behandlingsformålet til avsendervirksomheten. Når det gjelder råderett over opplysningene i mottakers postkasse, forslås dette regulert i eForvaltningsforskriften. Det er ikke foreslått egne bestemmelser om internkontroll i eForvaltningsforskriften, og de generelle reglene i personopplysningsloven vil derfor gjelde. Det vil si at omtalen nedenfor hovedsaklig omhandler sikkerhetstiltak og tilgangsregime.

Avsendervirksomhetene
Avsendervirksomhet er i utkastet til forskrift definert som *offentlig virksomhet som har inngått avtale med sentralforvalter av løsning for digital post fra forvaltningen,* jf utkastet til forskrift § 2 nr 4.

Det er bare avsendervirksomhetene som kan vurdere om løsningen for digital post fra forvaltningen er egnet for å formidle avsendervirksomhetens meldinger med tilhørende personopplysninger. Vurderingene vil blant annet være knyttet til meldingens innhold, krav til forsvarlig saksbehandling og øvrige risikovurderinger.

Det vil være stor variasjon både i sikkerhetsbehov og trusselbilde for forvaltningens digitale post til innbyggerne. Løsningen skal være egnet til å dekke sikkerhetsbehovene for de fleste typer digital post. Det er allikevel avsendervirkomhetens ansvar å vurdere om løsningen er egnet i det enkelte tilfelle. For opplysninger som krever særskilte beskyttelsestiltak etter for eksempel sikkerhetsloven, vil trolig ikke løsning for digital post fra forvaltningen være egnet.

Departementet vil knytte noen merknader til forsendelse av enkelte typer opplysninger. Dokumentet med opplysninger gradert etter sikkerhetsloven skal håndteres etter sikkerhetslovens forskrift om informasjonssikkerhet. For dokumenter med opplysninger som er gradert etter beskyttelsesinstruksen gjelder et knippe av reglene i nevnte forskrift «så langt det passer», jf. beskyttelsesinstruksen § 12. Det er ikke nå lagt opp til at løsning for digital post fra forvaltningen skal etterleve kravene i nevnte forskrift. Hvorvidt dette senere vil bli

gjort vil være avhengig av en kost-nyttevurdering. Systemet er således ikke egnet for forsendelse av graderte dokumenter.

Trusselutsatte personer har gjerne en bostedsadresse som er gradert FORTROLIG eller STRENGT FORTROLIG, jf. folkeregisterforskriften § 9-5. Dokumenter som inneholder en slik gradert bostedsadresse kan ikke sendes gjennom systemet.

For forsendelse av dokumenter uten graderte opplysninger, vil det bero på en konkret vurdering av beskyttelsesbehovene for de aktuelle opplysninger, sikkerhetsnivået i tjenesten og det aktuelle trusselbildet om løsningen er egnet eller ikke.

Det må være avsendervirksomheten som er ansvarlig for ovenfor nevnte vurderinger. Sentralforvalter og postkasseleverandørene vil ikke ha mulighet til å foreta vurderinger av innholdet i de meldinger som sendes via løsningen.

Avsendervirksomheten vil i praksis ha begrenset innflytelse på hvordan løsning for digital post fra forvaltningen utformes og hvilke virkemidler som brukes i løsningen for å ivareta informasjonssikkerheten. Departementet har derfor valgt å tydeliggjøre i forskriften at det i hovedsak er sentralforvalter som er ansvarlig for informasjonssikkerheten i løsning for digital post fra forvaltningen. Det er også tydeliggjort at postkasseleverandøren er ansvarlig for informasjonssikkerheten i de digitale postkassene.

Sentralforvalter av løsning for digital post fra forvaltningen
Departementet forslår at sentralforvalter utpekes av departementet, jf utkastet til forskrift § 2 nr. 2. Sentralforvalter er gitt viktige oppgaver og ansvar i forskriften, og det er derfor viktig at denne rollen tildeles en enhet som er kapabel til å forvalte løsningen på en god måte. Departementet foreslår at Direktoratet for forvaltning og IKT (Difi) er sentralforvalter av løsningen fra forskriftens ikrafttredelse.

Når det gjelder sikkerhetstiltak og tiltak for å overholde taushetsplikt, vil sentralforvalteren – gjennom arbeidet med kravspesifikasjon, kontraktsinngåelser og oppfølging av disse avtaleforholdene – ha reell bestemmelsesrett over hvordan opplysningene i løsning for digital post fra det offentlige skal behandles. Det vil i praksis si at sentralforvalter vil være den aktøren som har størst reell påvirkningsmulighet når det gjelder sikkerhetstiltak i de komponenter og den infrastruktur som utgjør løsningen. Departementet mener derfor at det er naturlig at sentralforvalter har ansvaret for informasjonssikkerheten i løsning for digital post fra forvaltningen.

Postkasseleverandørene
Postkasseleverandør er i utkastet til forskrift definert som *leverandør av digitale postkasser som har inngått avtale med sentralforvalter av løsning for digital post fra forvaltningen,* jf utkastet til forskrift § 2 nr. 4.

Postkasseleverandørene har størst oversikt over sikkerhetsrisiko og størst reell påvirkningsmulighet når det gjelder sikkerhetstiltak knyttet til den digitale posten etter at den er mottatt i de digitale postkassene. Av den grunn er det naturlig at postkasseleverandøren er ansvarlig for informasjonssikkerheten i de digitale postkassene. Det er også naturlig at det er postkasseleverandøren som er ansvarlig for at bestemmelsene om tilgang til de digitale postkassene overholdes. Kravene til informasjonssikkerhet og tilgangskontroll må imidlertid stilles gjennom regelverk og avtaler mellom sentralforvalter og postkasseleverandør.

Departementet foreslår etter dette at det inntas bestemmelser i forskriften §§ 31, 32 og 33 som regulerer ansvarsforhold knyttet til løsning for digital post fra forvaltningen. Videre foreslår departementet at det i § 32 og § 33 inntas en beskrivelse av hvordan ansvaret for ulike deler av informasjonssikkerheten skal ivaretas.

For omtale av behandlingsansvaret for register over digital kontaktinformasjon og reservasjon vises det til punkt 5.8 nedenfor.

4.4 Nedre aldersgrense for å kunne ha digital postkasse for mottak av digital post fra det offentlige

Fra 15-16-års alder utløses en rekke rettigheter som medfører at det er hensiktsmessig med digital kommunikasjon og digital post.

- Fra 15-årsalderen har man rett til vanlig lønnet arbeid, man kan velge trossamfunn og utdanningsløp selv og klage på egenhånd til barnevernet.15 år er også den kriminelle lavalder.
- 16-år er definert som en myndighetsalder i helsesektoren, bl.a. når det gjelder selvbestemt abort. Man har fra 16 år også rett til å søke lån og stipend til utdanning, ta førerkort for lett motorsykkel og moped og man har stemmerett ved lokalvalg i forsøkskommuner.

Per i dag er det krav om elektronisk ID på høyeste sikkerhetsnivå (e-ID på nivå 4) for å opprette digital postkasse. Buypass og BankID opererer med aldersgrense på 15 år for å utstede e-ID, men noen banker har 18-årsgrense for dette.

Leverandører av digitale postkasser i markedet har etablert 15-års aldersgrense, og Danmark har også satt 15 år som aldersgrense for digital post.

Departementet mener at det kan forventes størst bruk av løsning for digital post til forvaltningen av personer over 15 år. Det vil stilles krav om at postkasseleverandørene tilbyr tjenesten for personer over 15 år.

Før den enkelte fyller 15 år, vil foresatte i de aller fleste sammenhenger være rette adressat. Det er imidlertid avsendervirksomheten som må avgjøre om den digitale posten skal adresseres til barnet eller foreldre/foresatte, på samme måte som de gjør når henvendelser sendes pr papirpost.

Departementet mener at en aldersgrense for opprettelse av digital postkasse ikke er et forhold som det er nødvendig å forskriftsfeste, og har derfor ikke foreslått noen bestemmelse som regulerer dette.

4.5 Tildeling av digital postkasse til innbygger

Det er en målsetning at digital kommunikasjon skal være utgangspunktet og hovedregelen når forvaltningen kommuniserer med innbyggere og næringsliv, jf kapittel 3 ovenfor. Innbyggere skal imidlertid ha rett til å reservere seg. Reservasjonsretten gjelder etter departementets mening også det å ha en digital postkasse. Det vil si at innbyggere i utgangspunktet skal ha en digital postkasse, med mindre de har reservert seg mot dette.

Det er ulike måter den enkelte innbygger kan få sin digitale postkasse på. En mulighet er at innbyggere som ikke har reservert seg, og som har registrert digital kontaktinformasjon, får tildelt en digital postkasse fra sentralforvalter. Et annet alternativ er at den enkelte innbygger selv aktivt må opprette sin digitale postkasse.

Departementet ønsker høringsinstansenes syn på om regelverket bør gi mulighet for at innbyggere som ikke selv oppretter sin digitale postkasse, på et senere tidspunkt skal kunne tildeles en digital postkasse. Departementet ber derfor spesielt om høringsinstansenes tilbakemelding på dette punktet.

En overgang fra et krav om samtykke til en rett til å reservere seg mot elektronisk kommunikasjon, herunder det å ha en digital postkasse, innebærer som et utgangspunkt at alle som ikke har reservert seg skal ha en digital postkasse, jf ovenfor. Det er imidlertid en realitet at det vil ta tid før alle forvaltningsorganer er tilknyttet løsning for digital post fra forvaltningen. Det vil derfor også ta tid før innbygger kan motta all post fra forvaltningen digitalt. Departementet mener at det bør være en balanse mellom de krav som stilles til forvaltningsorganene om å sende digital post, mottakers berettigede forventning om at forvaltningen sender digital post, og det at mottaker tildeles en digital postkasse. I en innledende fase vil det etter departementets vurdering være riktig å informere og oppmuntre innbyggerne til å ta løsningen i bruk fremfor å benytte virkemidler som automatisk tildeling av postkasser. Departementet mener derfor at innbygger uansett ikke skal tildeles digital postkasse før innføringen av løsningen har kommet et stykke på vei. I startfasen vil innbygger derfor selv måtte opprette sin digitale postkasse.

Departementet ser at det også kan være andre hensyn som taler imot automatisk tildeling av digital postkasse til innbygger. Man risikerer at innbygger ikke har et bevisst forhold til digital post og digitale postkasser. Dette kan føre til at innbygger ikke forholder seg til sin digitale post og risikoen for å lide rettstap kan øke. Det vil også kunne påføre forvaltningen merarbeid om det rutinemessig sendes ut digital post til innbyggere som faktisk ikke benytter sin digitale postkasse.

For det tilfelle at det skal innføres en ordning hvor innbygger tildeles en digital postkasse, er det inntatt forslag til en bestemmelse om dette i utkastet til forskrift § 29, samt overgangsbestemmelsen § 47.

4.6 Digitale postkasser og reservasjonsretten

Det vises til omtalen av innføring av en rett til å reservere seg mot elektronisk kommunikasjon under punkt 3 ovenfor. Der er forslaget at det for de områdene hvor det i Prop. L 116 (2012-2013) er foreslått å fjerne kravet til samtykke, innføres en rett til å reservere seg mot elektronisk kommunikasjon. I tillegg mener departementet at innbygger skal kunne reservere seg mot å ha en digital postkasse. Det vises i den forbindelse til utkastet til forskrift § 28.

Det er et spørsmål om en mottaker som har en digital postkasse skal kunne velge å reservere seg mot å få digital post i den digitale postkassen fra enkeltvirksomheter, enkeltsektorer eller lignende. Det vises i den forbindelse til omtalen av reservasjon mot digital kommunikasjon fra enkeltvirksomheter, enkeltsektorer eller lignende under punkt 3.3.1 ovenfor.

4.7 Varsel om ny post i den digitale postkassen

I digitaliseringsprogrammet står følgende i kapittel 2 *Strategiske valg for fremtiden, Regjeringens program for fremtidens digitale forvaltning bygger på følgende prinsipper*:

*”**Innbyggere og bedrifter skal få varsling på sms og e-post***
Innbyggere og bedrifter skal kunne registrere sine ønsker for hvordan de foretrekker å bli kontaktet av forvaltningen. Kontaktinformasjon som e-post og mobiltelefonnummer skal brukes til å varsle når det kommer post i den digitale postkassen og til å sende enkel, ikke-sensitiv informasjon, slik som påminnelse om avtaler og frister. Kontaktinformasjonen skal samles på ett sted. På den måten slipper brukerne å oppgi e-postadresse og mobiltelefonnummer flere ganger til ulike deler av forvaltningen.”

Departementet foreslår at mottaker skal varsles når det kommer ny post i den digitale postkassen. Mottaker kan imidlertid velge å ikke bli varslet. Dersom forvaltningen sender enkeltvedtak m.v. til mottakers digitale postkasse, kan mottaker ikke velge å ikke bli varslet, jf § 8 nr 4 og § 30 nr (2).

Ved varsling skal den varslingsadresse som mottaker har registrert i register over digital kontaktinformasjon og reservasjon benyttes. Se imidlertid forslag til overgangsregler i utkastet § 47.

Departementet foreslår en bestemmelse om varsling av mottaker i utkastet til forskrift § 30.

4.8 Bruk av mottakers digitale postkasse

Det er i utgangspunktet kun mottaker av digital post som skal ha tilgang til sin digitale postkasse. Mottaker kan gi fullmakt til andre som denne ønsker skal ha tilgang. Dette forutsetter at fullmakter kan registreres. På kort sikt vil fullmakter måtte registreres hos den enkelte postkasseleverandør. På lenger sikt er målet at fullmakter skal registreres i register over digital kontaktinformasjon og reservasjon.

Departementet vil knytte noen merknader til digital post til personer med vergemål. Det er utfordringer knyttet til hvordan man skal sikre korrekt adressering til personer med vergemål. Folkeregisteret gir opplysninger om hvor papirpost kan sendes, men verken folkeregisteret eller kontaktregisteret er i dag tilrettelagt for å gjøre oppslag fra den som har verge, til vergen. Slike løsninger må trolig på plass før man kan etablere et digitalt førstevalg for personer med verge. Her kan det være aktuelt å finne løsninger i samarbeid med Statens sivilrettsforvaltning som sentral vergemålsmyndighet.

Verken postkasseleverandør eller avsender skal i utgangspunktet ha tilgang til mottakers digitale postkasse. Det er imidlertid enkelte begrensninger til dette utgangspunktet.

Teknisk personell vil for eksempel i enkelte tilfeller ha behov for å gjøre postkassen utilgjengelig for mottakeren på grunn av systemoppdateringer, retting av feil ved løsningen og lignende. Dette vil imidlertid normalt ikke kreve tilgang til selve innholdet i de digitale brevene.

Det kan oppstå tilfeller der det kan være hensiktsmessig at andre enn mottaker selv har tilgang til den digitale postkassen. Dette kan for eksempel være der det er sendt en melding fra avsendervirksomheten som inneholder virus og denne meldingen er lagret i mottakers postkasse. Det kan også tenkes tilfeller der avsendervirksomheten sender feil brev til feil mottaker. Skal avsendervirksomheten da kunne trekke brevet tilbake fra mottakers digitale postkasse?

Ved tilfeller av virus eller andre trusler mot informasjonssikkerheten, mener departementet at dette bør håndteres av postkasseleverandørene. Det er de som er ansvarlig for informasjonssikkerheten i de digitale postkassene. Departementet ser derfor ikke behov for at avsendervirksomheten skal kunne trekke tilbake meldinger som er lagret i mottakers digitale postkasse i slike tilfeller. Avsender har uansett plikt til å undersøke så langt som mulig at meldinger de sender er uten virus eller annen skadelig programvare.

Departementet mener at det er viktig å fastholde prinsippet om at den digitale postkassen er mottakers postkasse og at mottaker skal ha full råderett over denne. For tilfeller der avsendervirksomheten har sendt feil brev til feil mottaker, mener departementet imidlertid at det kan være aktuelt å tillate at meldinger trekkes tilbake av avsender dersom mottaker ikke har åpnet meldingen. Departementet har imidlertid ikke foreslått en bestemmelse knyttet til dette og ber spesielt om høringsinstansenes syn.

Dersom eier av postkassen dør, kan arvingene få tilgang på innholdet i postkassen ved framvisning av skifteattest.

Dersom mottaker ønsker å bytte postkasseleverandør eller sier opp avtalen med postkasseleverandøren, skal mottaker kunne overføre post til ny leverandør eller eget utstyr ved hjelp av funksjonalitet stilt til rådighet i løsningen. Mottaker har dermed frasatt seg råderett over sin tidligere digitale postkassen og postkasseleverandøren kan slette innholdet etter en gitt tidsfrist. Se mer om dette under punkt 4.11 nedenfor.

Departementet foreslår bestemmelser i utkast til forskrift § 35 som regulerer bruk av mottakers digitale postkasse.

4.9 Taushetsplikt

Det er viktig at personopplysningenes konfidensialitet blir ivaretatt på en tilfredsstillende måte i løsning for digital post fra forvaltningen. Det vises også til omtalen av ivaretakelse av personvern og informasjonssikkerhet i kap 8 nedenfor.

Departementet foreslår at det inntas en bestemmelse i eForvaltningsforskriften utkastet § 34 om taushetsplikt for de som behandler personopplysninger i løsning for digital post fra forvaltningen, og som ikke omfattes av forvaltningslovens regler om taushetsplikt, jf forvaltningsloven §§ 13 følgende.

4.10 Lagringstid – herunder forholdet til arkivloven

4.10.1 Lagringstid

Departementet mener at det er mottaker som etter eget ønske skal kunne slette mottatte meldinger, eller la disse bli liggende lagret i postkassen. Avsender eller postkasseleverandøren skal ikke på eget initiativ kunne slette mottakers meldinger. Dersom mottaker skal ha denne muligheten, kan det ikke være noen begrensninger i lagringstid.

Departementet foreslår at det inntas en bestemmelse om lagringstid i forskriften § 35 nr (3).

4.10.2 Forholdet til arkivloven

Når det gjelder forholdet til arkivloven, viser departementet til høringsuttalelse fra Riksarkivet i forbindelse med høring av Difi-rapport 2011:7 *En felles meldingsboks,* hvor det står:

«Rapporten stadfester at dokumenter forvaltninger sender til og mottar fra meldingsboksen er omfattet av arkivloven og skal arkiveres i forvaltningens egne arkivsystemer. Opplysningene og dokumentene i meldingsboksen er dermed kopier av ditto i forvaltningens egne arkiv, og er ikke omfattet av arkivloven. Det er dermed ikke grunnlag for at Riksarkivaren skal stille krav til håndteringen av meldingsboksen»

4.11 Bytte av postkasseleverandør og avvikling av en markedsbasert digital postkasse – flytting av innholdet

Departementet mener at mottaker fritt skal kunne bytte leverandør og ta med seg sin post. Noen ulemper vil det imidlertid kunne innebære for mottaker å flytte sin digitale post fra en postkasseleverandør til en annen. Organiseringen av postkassene og tilknyttet funksjonalitet vil være ulik mellom de forskjellige leverandørene. Selv om den digitale posten vil kunne flyttes mellom leverandører, vil den strukturen som brukeren har bygget opp etter all sannsynlighet gå tapt ved flytting.

Løsningen kan ha funksjonalitet for å eksportere innholdet i en postkasse på et generisk format og kunne importere tilsvarende. Funksjonalitet for å flytte digital post kan også implementeres ved at postkasseleverandøren det flyttes fra i slike tilfeller opptrer som avsender, og sender digital post til den nye postkasseleverandøren. Denne funksjonaliteten vil også kunne benyttes for flytting dersom en postkasseleverandør av ulike grunner legger ned virksomheten eller postkasseleverandøren etter utløpet av kontraktstiden ikke lenger har et avtaleforhold med sentralforvalter.

Departementet har inntatt forslag til regulering av ovenfor nevnte i utkastet til forskrift §§ 36 og 37.

5. Digital kontaktinformasjon og opplysning om reservasjon

5.1 Behovet for et register over digital kontaktinformasjon og reservasjon

I digitaliseringsprogrammet står følgende i kapittel 2 *Strategiske valg for fremtiden, Regjeringens program for fremtidens digitale forvaltning bygger på følgende prinsipper*:

> *"**Innbyggere og bedrifter skal få varsling på sms og e-post***
> *Innbyggere og bedrifter skal kunne registrere sine ønsker for hvordan de foretrekker å bli kontaktet av forvaltningen. Kontaktinformasjon som e-post og mobiltelefonnummer skal brukes til å varsle når det kommer post i den digitale postkassen og til å sende enkel, ikke-sensitiv informasjon, slik som påminnelse om avtaler og frister. Kontaktinformasjonen skal samles på ett sted. På den måten slipper brukerne å oppgi e-postadresse og mobiltelefonnummer flere ganger til ulike deler av forvaltningen."*

Videre står det følgende under punkt 3.4 i digitaliseringsprogrammet:

> *"**Det etableres en felles ordning for kontaktinformasjon og reservasjon mot digital post***
> *Regjeringen tar sikte på å etablere en felles ordning for at innbyggerne skal kunne reservere seg mot å motta digital post fra staten og fra de kommunene som velger å sende post digitalt. Alle statlige virksomheter skal sjekke eventuelle reservasjoner før de sender ut digital post. Brukere skal enkelt kunne registrere og endre hvorvidt man ønsker digital reservasjon, samt hvilket mobilnummer og e-postadresse de ønsker å bli varslet på. Brukerens mobilnummer og e-post kan også brukes til å sende enkel, ikke-sensitiv informasjon, for eksempel påminning om avtaler, frister og lignende. Det skal tilrettelegges for at også kommuner kan bruke kontaktinformasjonen."*

I punkt 3.5 i digitaliseringsprogrammet står det:

> *"**Felles offentlige registre skal understøtte den digitale forvaltningen***
> *[...]*
> *Regjeringen vil vurdere om innbyggernes digitale kontaktinformasjon på sikt skal inngå i folkeregisteret."*

I tråd med målsetningene i digitaliseringsprogrammet sitert ovenfor, er det et mål å etablere en sentral løsning for digital kontaktinformasjon som alle offentlige virksomheter kan benytte. Registeret skal blant annet inneholde informasjon om mottakers foretrukne e-postadresse, mobilnummer og valgte digitale postkasse.

Det vises også til kapittel 4.2 ovenfor når det gjelder register over digital kontaktinformasjon og reservasjons betydning for, og plassering i, løsning for digital post fra forvaltningen.

5.2 Regulering av register over digital kontaktinformasjon og reservasjon

Ettersom det er en målsetning at digital kommunikasjon fra forvaltningen ikke skal måtte baseres på samtykke fra mottaker, er det nødvendig med et annet behandlingsgrunnlag etter personopplysningsloven for digitale kontaktopplysninger og reservasjonsstatus. Departementet foreslår derfor at det gis regler i eForvaltningsforskriften som sikrer et slikt behandlingsgrunnlag. Det vises for øvrig til departementets vurderinger under punkt 4.1 ovenfor.

Begrepet ”oppslagstjeneste” brukt i figur 2 i kapittel 4.2 ovenfor, viser til avsendervirksomhetenes kontaktpunkt mot bakenforliggende registre, herunder register over digital kontaktinformasjon og reservasjon. Hjemlene i forslaget til forskriftsendringer som nå er på høring omfatter også en slik oppslagstjeneste, jf ”med tilhørende infrastruktur” i utkastet til forskrift § 39.

5.3 Hvem skal register over digital kontaktinformasjon og reservasjon inneholde opplysninger om?

I Prop. 116 L (2012-2013) står det følgende om hvem som skal kunne stå registrert i register over digital kontaktinformasjon:

> *”Når det gjelder register over kontaktinformasjon, foreslår departementet at forskriftskompetansen er begrenset til å regulere dette for privatpersoner mv. Med det siktes det i utgangspunktet til enheter som ikke er registrert i Enhetsregisteret. Enkelte detaljspørsmål om hvem som hører hjemme i registeret etter forvaltningsloven, berøres imidlertid i merknaden til forvaltningsloven § 15 a bokstav b i punkt 5 nedenfor. Registrering av elektronisk kontaktinformasjon for enheter registrert i Enhetsregisteret er i dag regulert i enhetsregisterloven § 6 andre ledd.”*
> *[…]*
> *”Hjemmelen er begrenset til å gi regler om et register for «privatpersoner mv.». Med privatpersoner siktes det i utgangspunktet til rettssubjekter som ikke er registrert i Enhetsregisteret. Det framgår i dag av enhetsregisterloven § 6 andre ledd at det kan inntas elektronisk kontaktinformasjon i Enhetsregisteret for enheter som er registrert der. Også eventuelt ytterligere regulering av registrering av elektronisk kontaktinformasjon for enheter registrert i Enhetsregisteret bør gjøres i enhetsregisterregelverket. Utvidelsen «mv.» er tatt med for å gi rom for at også andre enn privatpersoner i noen grad skal kunne omfattes av registeret opprettet etter forvaltningsloven, for eksempel fordi en finner reguleringen etter forvaltningsloven – med tilhørende reservasjonsmulighet, jf. bokstav c – mer egnet for enkelte av de enhetene som kan være registrert i Enhetsregisteret, jf. enhetsregisterloven § 4. Den nærmere reguleringen av dette hører til forskriftsarbeidet.*
>
> *Enkeltpersonforetak vil i stor utstrekning være registrert i Enhetsregisteret. Registrering av elektronisk kontaktinformasjon for foretaket må skje i samsvar med enhetsregisterregelverket. Som privatperson vil innehaveren høre hjemme i registeret opprettet etter forvaltningsloven.”*

Departementet foreslår, i tråd med forslaget i lovproposisjonen, at de som det skal kunne registreres opplysninger om i register over digital kontaktinformasjon og reservasjon, er privatpersoner og enheter som ikke er registrert i Enhetsregisteret.

Det vises til omtalen av enkeltpersonforetak i kapittel 3.2 ovenfor. Når det gjelder enkeltpersonforetak foreslår departementet at den digitale kontaktinformasjon som gjelder vedkommendes næringsvirksomhet registreres i Enhetsregisteret, og den private digitale kontaktinformasjonen registreres i register over digital kontaktinformasjon og reservasjon. Dette kan være den samme digitale kontaktinformasjon dersom innehaver av enkeltpersonforetaket ønsker det.

Det vises til omtalen av frivillige organisasjoner i kapittel 3.2 ovenfor. For frivillige organisasjoner innebærer departementets forslag at disse kan stå registrert i register over digital kontaktinformasjon dersom de ikke er registrert i Enhetsregisteret.

Det er imidlertid ennå ikke lagt opp til at andre enn personer med fødselsnummer eller d-nummer skal kunne være registrert i register over digital kontaktinformasjon og reservasjon. Hjemmelen gir allikevel mulighet til å registrere andre som ikke er registrert i Enhetsregisteret den dagen en slik løsning er på plass.

Departementets forslag til bestemmelse fremgår av utkastet til forskrift § 40.

5.4 Registrering og oppdatering av digital kontaktinformasjon

Flere virksomheter har i dag lokale registre med elektronisk kontaktinformasjon. Det største eksisterende registeret over digital kontaktinformasjon er kontaktregisteret til ID-porten. Her er e-postadressen og mobilnummeret til nærmere 2,8 millioner innbyggere registrert. Andre virksomheter med store kontaktregistre er Skatteetaten, Lånekassen og NAV.

I Prop. 116 L (2012-2013) står det følgende på side 13 andre spalte:

> *"Til ikrafttredelses- og overgangsbestemmelsen:*
>
> *Det åpnes uttrykkelig for at det kan bestemmes at en under etableringen av et register etter § 15 a henter inn personopplysninger fra kontaktregisteret tilknyttet ID-porten. I og med at det i lovvedtaket åpnes særskilt for slik gjenbruk, vil ikke forholdet til personopplysningsloven § 11 c om gjenbruk av personopplysninger aktualiseres, jf. personopplysningsloven § 5 om lovens virkeområde."*

Selve ikrafttredelses- og overgangsbestemmelsen andre punktum lyder:

> *"Kongen kan gi nærmere overgangsregler, herunder om adgang for register som opprettes etter forvaltningsloven § 15 a til å innhente personopplysninger fra kontaktregisteret tilknyttet ID-porten."*

Departementet foreslår at registeret i en oppstartsfase baseres på informasjon i kontaktregisteret til ID-porten. For å sikre tilstrekkelig kvalitet på de digitale kontaktopplysningene som skal inngå i register over digital kontaktinformasjon og reservasjon, foreslår departementet at det er kontaktinformasjon som er oppdatert eller bekreftet riktig ett år før overføringen skjer som flyttes over. Innbyggerne blir varslet om dette.

Det er utviklet en egen tjeneste der innbygger selv kan oppdatere sin kontaktinformasjon. Innbyggerne vil videre få mulighet til å oppdatere sin kontaktinformasjon i det sentrale registeret hver gang de logger seg på en offentlig elektronisk tjeneste. Slik vil kontaktinformasjonen bli oppdatert etter hvert som innbyggerne er i kontakt med det offentlige. I tillegg vil det bli sendt ut oppfordring om å oppdatere sin digitale kontaktinformasjon til innbyggere som ikke de seneste seks måneder har oppdatert eller bekreftet opplysningene i forbindelse med sin bruk av en offentlig elektronisk tjeneste.

Det legges også opp til at offentlige etater sender ut en henvendelse til alle som er registrert i deres eksisterende lokale kontaktregistre. Mottaker vil da bli informert om det sentrale registeret over digital kontaktinformasjon og bli bedt om å oppdatere eller bekrefte sin digitale kontaktinformasjon i det sentrale kontaktregisteret. En slik henvendelse sendes også ut til de som er registeret i ID-portens kontaktregister.

Det er viktig at den digitale kontaktinformasjonen er så oppdatert som mulig. Man kunne derfor tenkt seg at det stilles krav om at innbyggers digitale kontaktinformasjon i register over digital kontaktinformasjon og reservasjon skal være oppdatert eller bekreftet at er riktig for eksempel årlig, for at denne skal kunne brukes til varsling om digital post. Dersom dette ikke skjer, vil det innebære at innbygger i praksis er forhindret fra å motta digital post fra forvaltningen.

På den annen side, skal det innføres en rett for innbygger til å reservere seg. Dersom innbygger ikke reserverer seg, vil man til en viss grad kunne forutsette at innbygger ønsker digital post fra forvaltningen. Innbygger får da også et ansvar for å holde sin digitale kontaktinformasjon oppdatert, slik at varsel og annen kommunikasjon fra forvaltningen blir sendt riktig. Det kan i den forbindelse trekkes en parallell til innbyggers plikt til å holde sin folkeregistrerte postadresse oppdatert i det sentrale folkeregisteret. Justiskomiteen uttalte i forbindelse med behandlingen av endringer i forvaltningsloven § 15a at *"[d]en som velger å ikke reservere seg, har dermed en klar oppfordring til å innrette seg slik at elektroniske henvendelser ikke overses."*

Departementet synes det er hensyn som taler i begge retninger på dette punkt. Departementet foreslår at det som utgangspunkt er slik at dersom innbygger ikke har reservert seg, må hun sørge for at den digitale kontaktinformasjonen er oppdatert. Det kan imidlertid ta noe tid før det er naturlig for innbyggerne å forholde seg til en løsning for digital post fra forvaltningen. Departementet foreslår derfor en overgangsbestemmelse som sier at digital kontaktinformasjon som ikke er oppdatert eller bekreftet riktig de siste 12 månedene, ikke kan brukes til varsling, se utkastet til forskrift § 47. Det vil i praksis si at forvaltningen som et utgangspunkt er forhindret fra å kommunisere digitalt med vedkommende.

Hjemmel til å overføre kontaktinformasjon fra dagens kontaktregister tilknyttet ID-porten er forslått regulert i utkastet til forskrift § 48.

5.5 Registrering av reservasjonsstatus

Reservasjonsretten innebærer at reservasjonsstatus til den enkelte mottaker må kunne registreres. Reservasjonsstatus er en personopplysning etter personopplysningsloven og trenger et behandlingsgrunnlag. Ettersom det er ønskelig at behandlingsgrunnlaget er et annet enn samtykke, trengs det hjemmel i forskrift til å registrere reservasjonsstatus.

Departementet foreslår at en hjemmel til å registrere reservasjonsstatus inntas i utkastet til forskrift § 40.

5.6 Bruk av opplysninger i register over digital kontaktinformasjon og reservasjon

Informasjonen i kontaktregisteret skal kunne benyttes for å varsle innbyggerne om alle former for elektroniske henvendelser fra forvaltningen. Enten en digital henvendelse er tilgjengelig for mottaker i den digitale postkassen eller via et *"egnet informasjonssystem"*, jf eForvaltningsforskriften § 8 nr (4), skal forvaltningen kunne bruke informasjonen i kontaktregisteret for å varsle om dette.

Informasjonen skal også kunne benyttes til andre henvendelser fra det offentlige til innbyggerne, som påminnelse om avtaler, servicemeldinger (for eksempel varsel om stenging av vann og lignende) eller andre henvendelser i forbindelse med forvaltningsorganets

saksbehandling. I tillegg kan man se for seg at informasjonen benyttes til preutfylling av data i skjemaer og dialogtjenester.

Det er også departementets vurdering at mottakers digitale kontaktinformasjon (for eksempel mobiltelefonnummer) skal kunne benyttes til å kontakte mottaker pr telefon, jf sitat fra digitaliseringsprogrammet ovenfor under punkt 5.1., hvor det fremgår at kontaktinformasjonen skal samles på ett sted og at brukerne på den måten *"slipper å oppgi e-postadresse og mobiltelefonnummer flere ganger til ulike deler av forvaltningen"*.

Det er ingen felles definisjon for hva elektronisk kommunikasjon omfatter i norsk lovverk. Forvaltningsloven inneholder ingen slik definisjon. I forarbeidene til forvaltningsloven § 15 a (Ot.prp. nr. 108 (2000-2001)) er det inntatt en definisjon av elektronisk kommunikasjon:

> *"Elektronisk kommunikasjon: Dette er det overordnede begrepet for hele prosjektet. Elektronisk kommunikasjon skal forstås vidt og vil omfatte all elektronisk samhandling som for eksempel elektronisk avtaleslutning, elektronisk rapportering, elektronisk markedsføring, elektronisk betaling og elektronisk levering, samt elektronisk saksbehandling, inkludert underretning av vedtak. Kommunikasjonen kan være mellom næringsdrivende, mellom private, i forvaltningen eller mellom disse gruppene."*

Lov 4. juli 2003 nr 83 om elektronisk kommunikasjon (ekomloven) definerer for sitt formål elektronisk kommunikasjon klart snevrere enn definisjonen i Ot.prp. nr. 108 (2000-2001):

> *"elektronisk kommunikasjon: overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler i fritt rom eller kabel i et system for signaltransport."*

eForvaltningsforskriften § 3 første ledd bokstav c definerer elektronisk kommunikasjon. Ingressen og bokstav c lyder:

> *"Enhver som henvender seg til et forvaltningsorgan kan benytte elektronisk kommunikasjon, når det skjer i henhold til den form og fremgangsmåte og ved bruk av den elektroniske adressen, som forvaltningsorganet har anvist for den aktuelle type henvendelse.*
> […]
> *c) Med elektronisk kommunikasjon menes bruk av for eksempel Internett, eller liknende kommunikasjonssystem, og bruk av talestyrte eller andre automatiske telefontjenester, men ikke bruk av taletelefon eller annen muntlig kommunikasjon."*

Denne definisjonen er etter departementets oppfatning kun inntatt for å presisere § 3, og av den grunn er telefoni utelatt.

Departementet mener at det ikke er i strid med formålet i eForvaltningsforskriften å tillate at personopplysninger i register over digital kontaktinformasjon brukes til å kontakte innbygger pr telefon så lenge bruken er innenfor det formålet som er foreslått for bruk av opplysningene i utkastet til forskrift § 38: *"i forbindelse med saksbehandling og utføring av forvaltningsoppgaver for øvrig"*.

5.7 Bruk av lokale registre over digital kontaktinformasjon

På sikt er det tenkt at det sentrale registeret for digital kontaktinformasjon skal bli den sentrale kilden for innbyggeres digitale kontaktinformasjon. På samme måte som forvaltningen henter informasjon fra det sentrale folkeregisteret og Enhetsregisteret skal forvaltningen hente innbyggeres digital kontaktinformasjon fra dette registeret.

Departementet mener at det som utgangspunkt ikke skal benyttes lokale kontaktregistre som inneholder den samme informasjonen som finnes i en sentral løsning.

Departementet presiserer at det med lokale kontaktregistre ikke menes eventuelle kopier av det sentrale kontaktregisteret som forvaltningsorganet har fått utlevert til bruk i sin saksbehandling. Med lokale kontaktregistre menes registre som forvaltningsorganet selv forvalter. Departementet mener at forvaltningsorganer skal kunne få kopier av register over digital kontaktinformasjon og reservasjon uten at dette er i strid med verken formålet med registeret eller begrunnelsen for den sentrale løsningen som sådan. Det vises til utkastet til forskrift § 38 nr (3).

Forvaltningen bør forholde seg til kontaktregisteret som de forholder seg til det sentrale folkeregisteret, et sted hvor man får tilgang til oppdatert og kvalitetssikret informasjon på utvalgte områder. Hensikten med et felles sentralt register for digital kontaktinformasjon er at innbyggerne skal ha ett sted å oppdatere informasjonen. Samling av innbyggeres digitale kontaktinformasjon ett sted vil sannsynligvis også øke kvaliteten på opplysningene. Det er dermed naturlig at offentlige virksomheter gjenbruker denne informasjonen, og ikke har egne registre med den samme informasjonen. Forvaltningsorganer bør kun ha lokale registre over digital kontaktinformasjon der de har behov for flere opplysninger enn de som finnes i register over digital kontaktinformasjon og reservasjon.

Forvaltningsorganer som kobler seg opp mot løsning for digital post fra det offentlige, vil måtte koble seg til det sentrale registeret over digital kontaktinformasjon, blant annet for å kunne sjekke om mottaker har reservert og hvilken digital postkasse mottaker har valgt. I den forbindelse vil det være lite hensiktsmessig for et forvaltningsorgan å opprettholde et lokalt register over digital kontaktinformasjon, med mindre det lokale registeret inneholder elementer som det sentrale registeret ikke inneholder.

Før register over digital kontaktinformasjon og reservasjon er oppdatert med opplysninger fra andre registre, og har fått tilstrekkelig kvalitet, bør det legges opp til at forvaltningen kan benytte sine eksisterende lokale registre med digital kontaktinformasjon. Det er et mål at disse skal fases ut over tid.

Departementet foreslår at det i forskrift fastsettes at kontaktopplysninger i register over digital kontaktinformasjon og reservasjon skal benyttes for varsel om digital post fra forvaltningen, se utkastet til forskrift § 8 nr (3) og § 30 nr (3). Det foreslår imidlertid at bestemmelsene ikke trer i kraft før 1. juli 2016, jf forslaget til overgangsbestemmelse, utkastet § 47.

5.8 Behandlingsansvar for register over digital kontaktinformasjon og reservasjon

Difi skal forvalte register over digital kontaktinformasjon og reservasjon. Det er derfor naturlig at Difi er behandlingsansvarlig for behandlingen av personopplysninger i registeret. Det er Difi som har reell påvirkning når det gjelder registerløsningen og de virkemidler som benyttes for blant annet å ivareta informasjonssikkerheten, herunder tilgangsstyringen. Behandlingsansvaret inkluderer oppslagstjenesten, se kapitlene 4.2 og 5.2 ovenfor, som en nødvendig del av infrastrukturen for registeret.

Departementet foreslår at det i utkastet til forskrift § 39 fastslås at Difi er behandlingsansvarlig for register over digital kontaktinformasjon og reservasjon.

5.9 Taushetsplikt

Det er viktig at personopplysningenes konfidensialitet blir ivaretatt på en tilfredsstillende måte i register over digital kontaktinformasjon og reservasjon. Det vises til omtalen av ivaretakelse av personvern og informasjonssikkerhet i kapittel 8 nedenfor.

Departementet foreslår derfor at det inntas en bestemmelse i eForvaltningsforskriften, se utkastet § 44 om taushetsplikt for de som behandler personopplysninger i registrene, og som ikke omfattes av forvaltningslovens regler om taushetsplikt, jf forvaltningsloven §§ 13 følgende.

6. Andre endringer i eForvaltningsforskriften

6.1 Når klagefristen begynner å løpe

6.1.1 Endring av eForvaltningsforskriften § 8 fra 1. januar 2013 og gjeldende rett

eForvaltningsforskriften § 8 ble endret med virkning fra 1. januar 2013. Fra høringsbrevet til departementet siteres følgende:

> *"Etter forvaltningsloven § 29 begynner klagefristen å løpe når vedtaket er kommet frem til parten. For elektronisk post vil dette bety at et enkeltvedtak skal anses for å være "kommet frem" til mottakeren når det er havnet i dennes elektroniske postkasse, og eventuell klagefrist begynner dermed å løpe.*
> *[...]*
> *Ordlyden i eForvf § 8 (6) er i dag: "Underretning om enkeltvedtak anses å ha kommet frem på det tidspunktet parten skaffet seg tilgang til vedtaket fra forvaltningsorganets informasjonssystem." Denne regelen har sammenheng med 7-dagersregelen i § 8 (7) ved at "skaffet seg tilgang til vedtaket" utløste at klagefristen begynte å løpe. For de tilfeller hvor man ikke skaffet seg tilgang innen en uke, ble vedtaket sendt ut på papir. Fvl § 29 legges til grunn for klagefristen, uavhengig av om vedtaket formidles elektronisk eller i papirpost. Regelen i eForvf § 8 (6) blir derfor overflødig, og foreslås opphevet."*

For beregning av frister ved klage i forbindelse med varsel om vedtak og enkeltvedtak, gjelder reglene i forvaltningsloven § 29, på samme måte som ved papirbasert kommunikasjon. Forvaltningsloven § 29 første ledd første punktum lyder:

> *"Fristen for å klage er 3 uker fra det tidspunkt underretning om vedtaket er kommet frem til vedkommende part."*

Klagefrist regnes fra avsendelsestidspunkt fra forvaltningsorganet. Tidspunktet kan utledes fra forvaltningsorganets elektronisk logg. Som ved papirbasert kommunikasjon kan det være hensiktsmessig å legge til et par dager på grunn av evt. uforutsette omstendigheter. Dette bør imidlertid ikke være nødvendig, da elektronisk loggføring ansees mer pålitelig enn manuelt formidlet papirpost mht fremkommelighet.

6.1.2 Departementets vurdering og forslag

Departementet mener at det som et utgangspunkt ikke skal gjelde andre regler for elektronisk kommunikasjon enn for tradisjonell papirbasert kommunikasjon.

Det er naturlig å knytte skjæringspunktet for når klagefrister mv begynner å løpe til tidspunktet når vedtaket er tilgjengelig i den digitale postkassen eller tilgjengelig fra annet egnet informasjonssystem, og varsel om dette er sendt til mottakeren i henhold til de opplysninger som er registrert i register over digital kontaktinformasjon og reservasjon.

Begrepet *"kommet frem"* i forvaltningsloven § 29 vil etter dette følgelig være å forstå slik at et vedtak er kommet frem når det er gjort tilgjengelig i vedkommendes digitale postkasse eller annet egnet informasjonssystem. Parten har da mulighet til å tilegne seg innholdet av vedtaket. Dette gjelder uavhengig av et eventuelt gjentatt varsel som foreslått i ny § 8 nr (7).

Departementet foreslår at det inntas en bestemmelse i eForvaltningsforskriften § 8 nr (10) som tydeliggjør når klagefristen begynner å løpe når enkeltvedtak formidles elektronisk.

6.2 Når klage er rettidig fremsatt

I Prop. 116 L (2012-2013) er det foreslått å endre forvaltningsloven § 30 første punktum slik at bestemmelsen ikke omhandler fristavbrudd når klage fremsettes elektronisk:

> *"Reguleringen i § 30 første punktum om hva som er en rettidig klage ved elektronisk kommunikasjon, foreslås også opphevet. Det hører til forskriftsarbeidet å vurdere hvordan fristregler i forvaltningsloven og annen lovgivning skal anvendes ved elektronisk kommunikasjon, og denne reguleringen bør i størst mulig grad være samlet i eForvaltningsforskriften."*

Regelen i forvaltningsloven § 30 første punktum om at en klage er rettidig framsatt dersom den er *"kommet fram til den elektroniske adressen som forvaltningsorganet har oppgitt for mottak av elektroniske klager",* er foreslått opphevet. Tilsvarende bestemmelse foreslås i eForvaltningsforskriften, se utkastet til forskrift § 9 nr (3).

6.3 Ekstra elektronisk varsling

6.3.1 Endring av eForvaltningsforskriften § 8 fra 1. januar 2013

Den såkalte syvdagersregelen i eForvaltningsforskriften § 8 nr (7) ble opphevet med virkning fra 1. januar 2013. Videre ble § 8 nr (6), (8) og (9) opphevet, og nr (2) endret, som en følge av at syvdagersregelen ble opphevet.

6.3.2 Departementets vurdering og forslag

Syvdagersregelen ble i sin tid innført for å forhindre at mottaker av for eksempel enkeltvedtak skulle lide rettstap når enkeltvedtaket ble formidlet til vedkommende ved bruk av elektronisk kommunikasjon. Ettersom kravet til samtykke for elektronisk kommunikasjon i forvaltningsloven er fjernet, og erstattet med en rett til å reservere seg, er det relevant å vurdere om det er behov for andre mekanismer som skal hindre at parten lider rettstap. Vedkommende forvaltningen kommuniserer elektronisk med skal varsles elektronisk når nye meddelelser er tilgjengelig for mottaker, jf. omtale i kapittel 4.7 ovenfor og merknader til § 8 nr (3) og § 30. Departementet har vurdert å innføre et krav om ekstra elektronisk varsling dersom meldingen ikke er åpnet innen et visst antall dager. Alternativt kan man la det være opp til avsendervirksomheten å vurdere om viktigheten av det som skal kommuniseres til mottaker er av en slik karakter at ekstra varsling er nødvendig eller ønskelig.

Ettersom innbygger ikke lenger skal trenge å samtykke til elektronisk kommunikasjon fra forvaltningen, kan det være at innbygger ikke har et like bevisst forhold til at forvaltningen henvender seg via elektroniske løsninger. Enkeltvedtak og andre meldinger som har betydning for mottakers rettsstilling er særlig viktige for mottaker, og det er et spørsmål om det bør finnes mekanismer som søker å ivareta innbyggernes rettssikkerhet når forvaltningen skal sende slike meddelelser elektronisk til mottaker.

Departementet mener at vurderingen av om det skal stilles krav til ekstra elektronisk varsling, kan ses i sammenheng med hvilke krav som stilles til hvor ofte den digitale kontaktinformasjonen skal være oppdatert eller bekreftet riktig. Videre vil det være, når det gjelder løsning for digital post fra forvaltningen, en sammenheng mellom et eventuelt krav om ekstra elektronisk varsel, og om innbygger skal tildeles en digital postkasse, eller om innbygger selv skal opprette denne.

På den annen side kan man si at det forvaltningsorgan som skal formidle enkeltvedtak og lignende elektronisk til mottaker, er nærmest til å vurdere om vedtakets innhold er av en slik art at ekstra varsling er nødvendig i det enkelte tilfellet. Det kan være stor variasjon i hvilke konsekvenser et vedtak har for mottaker.

Når det gjelder digital post til næringslivet, som ikke vil få en reservasjonsrett, kan det være ekstra viktig å bli varslet en ekstra gang.

Departementet ønsker ikke å konkludere på dette punktet nå, og ber spesielt om høringsinstansenes tilbakemelding. For det tilfellet at man ønsker en bestemmelse om ekstra elektronisk varsel, er det inntatt utkast til en bestemmelse i §§ 8 nr (7) og 30 nr (2).

6.4 Endring av eForvaltningsforskriften § 13 – sikkerhetsmål og sikkerhetsstrategi

6.4.1 Bakgrunn

eForvaltningsforskriften § 13 krever at forvaltningsorgan som benytter elektronisk kommunikasjon, skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Denne sikkerhetsstrategien skal danne grunnlaget for forvaltningsorganets beslutninger om innføring og bruk av sikkerhetstjenester og -produkter på en helhetlig, planlagt, systematisk og dokumentert måte. Sikkerhetsstrategien skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks. Sikkerhetsstrategien skal være utarbeidet i henhold til anerkjente prinsipper for informasjonssystemers sikkerhet.

Det har vist seg å være vanskelig for forvaltningsorganer å få full oversikt over alle praktiske konsekvensen av eForvaltningsforskriften § 13. Dette har også gjort det krevende for mange virksomheter å etterleve den på en god måte.

Direktoratet for forvaltning og IKT (Difi) har i referansekatalogen for IT-standarder i offentlig sektor versjon nr. 3.1 (publisert 30.10.2012) anbefalt ISO27001som forvaltningsstandard for styringssystem for informasjonssikkerhet. I arbeidet med å implementere relevante kontroller, anbefaler Difi at virksomhetene følger strukturen i ISO27001 appendiks A og innholdsmessig støtter seg på ISO/IEC 27002.

Dersom en virksomhet allerede har et operativt styringssystem på andre områder (f.eks. i relasjon til ISO 9001, ISO 14001 eller HMS), vil det i de fleste tilfeller være mest hensiktsmessig å oppfylle ISO27001-kravene innenfor rammene av det eksisterende styringssystemet.

Difi presiserer at selv om det å følge anviste standarder på området bidrar til økt sikkerhet, gir det ikke en automatisk tilfredsstillelse av alle krav i gjeldende regelverk. Anvendelsesområdet for anbefalingen er sikker offentlig behandling av beskyttelsesverdig informasjon. Dette er utdypet i kap. 2.16 i ovennevnte referansekatalog.

6.4.2 Departementets vurdering og forslag

Departementet har vist til de nye anbefalte forvaltningsstandardene fra Difi i det nye Digitaliseringsrundskrivet P-10/2012 (utsendt 31.10.2012). Rundskrivet gjelder for departementene, statens ordinære forvaltningsorganer, forvaltningsorganer med særskilte fullmakter og forvaltningsbedrifter.

Under pkt 1.7 *Informasjonssikkerhet* i rundskrivet heter det:

> *"Virksomheten skal ha en internkontroll på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. (Jf. Difis referansekatalog versjon 3.1, pkt. 2.16 Styringssystem for informasjonssikkerhet. I forbindelse med Nasjonal strategi for informasjonssikkerhet vil det også bli vurdert å stille krav til statlige virksomheter om bruk av standarder for informasjonssikkerhet.). Denne internkontrollen kan med fordel være en integrert del av virksomhetens helhetlige styringssystem for kontinuerlig forbedring av virksomhetens arbeidsprosesser, måloppnåelse, informasjonssikkerhet, HMS, miljøledelse, samfunnsansvar m.v."*

På denne måten knyttes det en sammenheng mellom begrepene internkontroll, styringssystem for informasjonssikkerhet og virksomhetens helhetlige styringssystem. Med bruken av begrepet "internkontroll" og "basert på", gir departementet også et handlingsrom for bruken av forvaltningsstandarden fra Difi ut fra virksomhetens egenart, samt risiko og vesentlighet. Dette i samsvar med de overordnede føringene for internkontroll i økonomiregelverket i staten. Samtidig poengterer departementet at det kan være aktuelt å stille ytterligere krav til statlige virksomheter om bruk av standarder

Departementet tydeliggjør også at målet ikke er å få et eget selvstendig system, men å implementere standardens krav til styring av informasjonssikkerhet. Departementets presisering av at denne internkontrollen med fordel kan være en integrert del av virksomhetenes helhetlige styringssystem, anses også som et viktig signal for å få virksomhetene til å ta de riktige vurderingene før de starter implementeringen.

På bakgrunn av Difis anbefalinger omtalt ovenfor, mener departementet det er behov at forskriftsteksten og teksten i Digitaliseringsrundskrivet samsvarer, samtidig som kapitteloverskriften foreslås endret for å bedre dekke innholdet i bestemmelsen. Departementet foreslår derfor at teksten i eForvaltningsforskriften § 13 endres som foreslått i kapittel 11 nedenfor.

7. Overgangsbestemmelser

Forslagene til endringer i eForvaltningsforskriften medfører at forvaltningen fra endringenes ikrafttredelse ikke lenger trenger samtykke for å kommunisere elektronisk med mottaker. Fra samme tidspunkt innføres en rett for mottaker til å reservere seg mot elektronisk kommunikasjon i enkelte tilfeller. Dersom mottakers rett til reservasjon skal bli reell, må avsendervirksomheten være i stand til å sjekke om mottaker har reservert seg. Dette forutsetter at avsendervirksomheten er koblet opp mot register over digital kontaktinformasjon og reservasjon. Alternativt må avsendervirksomheten ha innhentet utrykkelig samtykke og nødvendig kontaktinformasjon fra mottaker.

Difi arbeider ut fra en målsetning om at en pilotering av løsning for digital post fra forvaltningen skal starte medio 2014. Departementet ser derfor for seg at de foreslåtte endringene i forvaltningsloven og eForvaltningsforskriften skal tre i kraft fra 1. januar 2014. Det er på det rene at ikke alle enheter i forvaltningen vil være koblet opp mot register over digital kontaktinformasjon og reservasjon fra dette tidspunktet. Det er derfor behov for overgangsbestemmelser.

Departementet foreslår at de forvaltningsorganer som ikke er koblet opp mot register over digital kontaktinformasjon og reservasjon, fortsatt må innhente samtykke for å kommunisere elektronisk med mottaker, i samsvar med dagens regelverk. Det vil også si at de samtykker mottaker pr i dag har avgitt til forvaltningsorganer for bruk av elektronisk kommunikasjon vil gjelde selv om mottaker har reservert seg i register over digital kontaktinformasjon og reservasjon. Mottaker kan etter vanlige regler trekke avgitte samtykker tilbake.

Departementet foreslår overgangsbestemmelser knyttet til de paragrafene i forskriften som krever at det er den digitale kontaktinformasjonen i register over digital kontaktinformasjon og reservasjon som benyttes til varsling av mottaker. Ettersom ikke alle forvaltningsorganer er koblet opp mot dette registeret i en overgangsperiode, vil forvaltningsorganer måtte kunne benytte annen digital kontaktinformasjon til mottaker.

Det vises for øvrig til omtalen av tildeling av digitale postkasser under kapittel 4.5 og omtale i kapittel 5.4 om oppdatering av digital kontaktinformasjon, med tilhørende forslag til overgangsbestemmelser.

Departementet foreslår at det gis overgangsbestemmelser i utkast til forskrift § 47. Bestemmelsene som krever at avsendervirksomheten bruker mottakers kontantinformasjon registrert i register over digital kontaktinformasjon og reservasjon til varsling, foreslås tre i kraft fra 1. januar 2016. Dette gir tid for alle forvaltningsorganer til å koble seg til register over digital kontaktinformasjon og reservasjon. Øvrige overgangsbestemmelser foreslås det at gjelder til 1. juli 2016.

8. Personvern og informasjonssikkerhet

8.1 Omtale av personvern i Prop. 116 L (2012-2013)

"Et sentralt element i personvernet er den enkeltes rett til og reelle mulighet for å bestemme over bruk av egne personopplysninger. Personverninteresser må veies mot andre interesser, som for eksempel rettssikkerhetshensyn, økonomiske hensyn og effektiv utnyttelse av samfunnets ressurser. Når det gjelder lovregulering av en hovedregel om elektronisk kommunikasjon mellom forvaltning og innbygger, mener departementet at en avveining mellom personverninteresser og samfunnets interesser for øvrig taler for å fremme forslaget slik det foreligger i denne proposisjonen. Det hører til forskriftsarbeidet å vurdere nærmere hvordan hensynet til personvern og informasjonssikkerhet skal ivaretas ved den nærmere utformingen av løsningene."

8.2 Ivaretakelse av personvern i løsning for digital post fra forvaltningen

Endringen av forvaltningsloven (Prop. 116 L (2012-2013)) innebærer at forvaltningen som hovedregel skal kommunisere digitalt med innbyggere og næringsliv. Derfor er det desto viktigere at forvaltningen garanterer for at innbyggernes personvern ivaretas tilstrekkelig i kommunikasjonsprosessene.

Personopplysningslovens regler er generelle og gjør seg gjeldende for løsning for digital post fra forvaltningen, med mindre annet er spesifisert. I personopplysningsloven § 11 er det oppstilt noen generelle grunnkrav til behandling av personopplysninger som gjør seg gjeldende for all behandling av personopplysninger. Denne bestemmelsen gjør seg gjeldende for den behandling av personopplysninger som skjer i løsning for digital post fra det offentlige. Bestemmelsen sier at personopplysninger kun skal behandles til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet, og at senere bruk til formål som er uforenlig med det opprinnelige krever samtykke fra den registrerte. Videre skal personopplysningene være tilstrekkelige og relevante for formålet, de skal være korrekte og oppdaterte, og de skal ikke lagres lenger enn det som er nødvendig ut fra formålet med behandlingen.

Regjeringen mener det bør fastsettes et prinsipielt mål om innebygget personvern i alle sektorer, jf Meld. St. 11 (2012-2013) *Personvern – utsikter og utfordringar*. Innebygget personvern innebærer at personvernhensyn skal være en naturlig del av alle ledd i utviklingen og bruken av informasjonsteknologi. Det innebærer også, på et overordnet plan, at personvern skal være en naturlig del av alle systemer og løsninger som innbyggerne møter i hverdagen. Personvern spiller en viktig rolle i både planleggings-, lovgivnings- og utviklingsstadiet av prosjekter som det foreliggende.

Et tema som aktualiseres ved innføringen av offentlige digitale postkasser for innbyggerne, er overvåkning. Digital kommunikasjon åpner for helt andre tekniske muligheter til å overvåke både kommunikasjon og bevegelser hos mottaker enn de man har i det tradisjonelle postsystemet. Nye tekniske muligheter til overvåkning fordrer at forvaltningen har en helt klar formening om hvilken grad av overvåkning som er nødvendig for å gjennomføre kommunikasjonen, og hvordan hensynet til administrasjon og effektivitet bør veies mot hensynet til innbyggernes personvern og rett til ikke å bli overvåket i sine handlinger. Bruk av

personopplysninger til nye formål, eller formål som er uforenlige med det opprinnelige, krever samtykke fra den enkelte innbygger, dersom annet lovlig grunnlag ikke finnes.

En viktig side av personvernet er informasjon. For å kunne øve full kontroll over bruken av egne personopplysninger må innbyggeren være klar over at, hvordan, og hvorfor deres personopplysninger behandles. Gode informasjonsprosesser kan også bidra til økt tillit hos innbyggeren til forvaltningen. Ved innføring av løsning for digital post fra det offentlige er det derfor svært viktig at innbyggerne informeres om endringene og om løsningen på tilstrekkelig vis.

Det bør i en oppstartsfase gjennomføres informasjonskampanjer rettet mot sentrale befolkningsgrupper i forskjellige fora. Til selve løsningen bør det utarbeides klare og lett tilgjengelige personvernpolicyer, som blant annet forklarer hvilke rutiner for behandling av personopplysninger som innføres, hvilke rettigheter innbyggerne har og hvordan de kan praktisere disse. Innbyggerne bør videre få godt tilrettelagt informasjon om betydningen av tekniske innstillinger for deres personvern. Det vil stilles krav til postkasseleverandører om at de mest personvernvennlige tekniske løsningene settes som standardinnstillinger der det er nødvendig med forhåndsdefinerte innstillinger. Slik kan man bedre sikre at innbyggerne er informerte før de eventuelt godtar mindre personvernvennlige innstillinger.

En særlig viktig del av informasjonsarbeidet gjelder innbyggernes rett til å reservere seg mot digital kommunikasjon fra forvaltningen. Reservasjonsretten følger av utkast til forskrift om endringer i eForvaltningsforskriften § 8. Tilrettelagt informasjon om reservasjon bør gis ved innbyggerens første møte med løsningen. Det er svært viktig at denne informasjonen både er tilrettelagt, lett forståelig og lett tilgjengelig for innbyggeren, både ved første møte og ved senere tidspunkt. Godt tilrettelagte og enkle brukergrensesnitt er viktig i denne sammenheng.

8.3 Ivaretakelse av informasjonssikkerhet i løsning for digital post fra forvaltningen

Sentralt for ivaretakelse av informasjonssikkerhet i systemer hvor det behandles personopplysninger, er hensyn til konfidensialitet, integritet og tilgjengelighet. Hensynet til konfidensialitet tilsier at det skal vernes mot uautorisert innsyn i personopplysninger, og hensynet til integritet tilsier at det skal vernes mot uautorisert endring av personopplysninger. Tilgjengelighetshensynet innebærer at relevant informasjon skal være tilgjengelig ved behov, og til rett tid. Se også omtale av konfidensialitet og integritet i vedlegg til dette høringsnotatet om kryptografisk beskyttelse av digital post.

Personopplysningsloven § 13 og personopplysningsforskriften kapittel 2 oppstiller generelle krav til informasjonssikkerheten i systemer hvor det behandles personopplysninger. Disse reglene gjelder også for løsning for digital post fra forvaltningen. Hensynene til konfidensialitet, integritet og tilgjengelighet skal ivaretas gjennom systematiske og dokumenterte sikkerhetstiltak hos den behandlingsansvarlige og dennes databehandler(e).

I tillegg til reglene i personopplysningsloven, gjelder også regjeringens nasjonale strategi for informasjonssikkerhet for løsning for digital post fra det offentlige. Denne er et uttrykk for regjeringens overordnede prioriteringer på informasjonssikkerhetsområdet.

Sentralt for ivaretakelsen av god informasjonssikkerhet i løsning for digital post fra forvaltningen er at det foreligger klare ansvarsforhold og roller, slik at det aldri er tvil om hvem som har det primære ansvaret for informasjonssikkerhet på de forskjellige stadiene i

kommunikasjonsprosessen. Dette er klargjort for løsning for digital post ved at det i forskriften er inntatt en egen bestemmelse om ansvaret for informasjonssikkerheten i løsningen.

Et av de viktigste sikkerhetstiltakene i løsning for digital post fra forvaltningen, er kryptering av meldinger. Krypteringen skal skje allerede hos avsendervirksomheten, og sted for dekryptering vil avhenge av hvilket sertifikat postkasseleverandøren stiller til rådighet for innbyggeren. I utgangspunktet er det ønskelig at dekryptering skal skje hos mottaker, men i første omgang vil dekryptering trolig skje hos postkasseleverandøren, jf også vedlegg til dette høringsnotatet om kryptografisk beskyttelse av digital post. God tilgangsstyring, både hos avsendervirksomhetene og hos mottaker, er derfor nødvendig å sikre. På mottakersiden sikres dette blant annet ved at kontaktinformasjon er oppdatert og riktig, og ved at tilfredsstillende autentiseringsnivå implementeres for tilgang til postkassene. De konkrete kravene til informasjonssikkerhet i løsning for digital post fra det offentlige er spesifisert i konkurransegrunnlaget fra Direktoratet for forvaltning og IKT.

Det er viktig at den behandlingsansvarlige og dennes databehandlere har et bevisst forhold til informasjonssikkerhet, blant annet ved at det utarbeides strategier for ivaretakelse av informasjonssikkerhet i løsningen, basert på gode risikoanalyser. Det er også viktig at interne rutiner fastsettes som støtter opp under informasjonssikkerhetstiltakene.

Fordi den enkelte innbygger skal ha råderett over innholdet i sin digitale postkasse så snart dette er levert ham eller henne, vil den enkelte også kunne ha en viss påvirkning på sikkerhets- og personvernnivået i sin egen postkasse. Det kan ikke forventes at alle innbyggerne har kjennskap til hvilke konsekvenser deres egne handlinger i postkassen kan få for informasjonssikkerheten og personvernet. Derfor er det viktig at dette kommuniseres til innbyggerne på en god og konstruktiv måte, slik at de er best mulig rustet til å ta riktige valg som ivaretar informasjonssikkerheten og personvernet i postkassene.

9. Økonomiske og administrative konsekvenser

Økt bruk av elektronisk kommunikasjon fra forvaltningens side vil innebære en samfunnsøkonomisk gevinst. Gevinsten knytter seg ikke minst til økt effektivitet og til besparelser i portoutgifter. For innbyggere og næringsliv antas de økonomiske konsekvensene å være ubetydelige. Privatpersoner mv. som ikke opplever det som en fordel å motta henvendelser fra forvaltningen elektronisk, vil for øvrig kunne reservere seg. Innføring av elektronisk kommunikasjon som forvaltningens hovedregel vil innebære administrative forenklinger i form av blant annet redusert håndtering av fysiske dokumenter.

Difi har estimert at den samfunnsøkonomiske gevinsten ved etablering og bruk av digitale postkasser hvor innbyggere og næringsliv kan motta elektronisk post fra forvaltningen på en sikker måte, over 10 år vil være mellom 2,5 og 2,8 milliarder kroner i netto nåverdi sammenlignet med at det ikke etableres en felles løsning for elektronisk post fra det offentlige. Det er beregnet at volum og besparelser fordeler seg relativt likt mellom post til innbyggere og post til næringslivet. Det er imidlertid stor usikkerhet knyttet både til volumet av elektronisk post og til utviklingen av dette over tid, og det hefter derfor usikkerhet ved beregningen. Utvikling av volumet vil være avhengig av hvor raskt forvaltningen og dens brukere tar i bruk sikker digital post. For at digitale postkasser skal få fotfeste hos forvaltningens brukere, er det blant annet viktig at sluttbrukerne opplever at postboksen er enkel å bruke og at de har tillit til sikkerheten. Dette og andre forutsetninger for beregningene ovenfor er beskrevet nærmere i Difi-rapport 2012:10 *Sikker digital post for det offentlige*[5].

Når det gjelder kostnadene for forvaltningsorganer ved å knytte seg til løsningen, ble det gjort estimater i forbindelse med samfunnsøkonomisk analyse. Det ble da lagt til grunn ett grensesnitt mot løsning for digital post fra forvaltningen. Det vil også være behov for et grensesnitt til register over digital kontaktinformasjon og reservasjon. I den samfunnsøkonomiske analysen ble tilknytningskostnaden til løsning for digital post fra forvaltningen estimert til kr. 65 000,- (middelanslag) per avsendervirksomhet. Disse kostnadene vil imidlertid kunne variere mellom virksomhetene.

Enkelte forslag, for eksempel et eventuelt krav om ekstra elektronisk varsel jf. punkt 6.3, vil kunne innebære kostnader for avsendervirksomhetene i forvaltningen. Slike eventuelle kostnader må dekkes av den enkelte virksomhet.

[5] http://www.difi.no/filearchive/rapport-2012-10-sikker-digital-post-med-vedlegg-w.pdf

10. Merknader til de enkelte bestemmelsene

Kapittel 2. Alminnelige krav ved bruk av elektronisk kommunikasjon med forvaltningen

Til § 2 *Begreper*
Til første ledd nr 1 – *Løsning for digital post fra forvaltningen*:
Med *løsning for digital post fra forvaltningen* menes forvaltningens distribusjonskanal for digital post fra avsendervirksomhet til innbyggers digitale postkasse. Begrepet omfatter også det som omtales som meldingsformidleren i figur 2 i kapittel 4.2 ovenfor.

Begrepet omfatter ikke de digitale postkassene hos postkasseleverandøren. Dette gjenspeiles blant annet i utkastet §§ 33 og 34, som blant annet beskriver henholdsvis sentralforvalters og postkasseleverandørens ansvar for informasjonssikkerhet. Dette medfører også at mottaker kan behandle opplysninger i sin postkasse for andre formål enn de som er beskrevet for *løsning for digital post fra forvaltningen*.

Til første ledd nr 2 – *Sentralforvalter av løsning for digital post fra forvaltningen*
Departementet forslår at sentralforvalter utpekes av departementet. Sentralforvalter er gitt viktige oppgaver og ansvar i forskriften, og det er derfor viktig at denne rollen tildeles en enhet som er kapabel til å forvalte løsningen på en god måte. Departementet foreslår at Direktoratet for forvaltning og IKT (Difi) er sentralforvalter av løsningen fra forskriftens ikrafttredelse.

Til første ledd nr3 – *Avsendervirksomhet*
Det er bare de offentlige virksomhetene som har inngått avtale med sentralforvalter som kan benytte løsning for digital post fra forvaltningen.

Til første ledd nr4 – *Postkasseleverandør*
Postkasseleverandørene vil inngå avtaler med sentralforvalter etter konkurranse i henhold til lov og forskrift om offentlige anskaffelser.

Til første ledd nr 6 – *Mottaker*:
Departementet foreslår at bare privatpersoner og enheter som ikke er registrert i Enhetsregisteret skal kunne være mottaker av digital post i løsning for digital post fra forvaltningen. Dette har nær sammenheng med hvem som skal kunne reservere seg mot elektronisk kommunikasjon fra forvaltningen, og hvem som skal kunne være registrert i register over digital kontaktinformasjon og reservasjon.

Frivillige organisasjoner som vil registrere seg i Frivillighetsregisteret må også være registrert i Enhetsregisteret. Disse er da ikke omfattet av begrepet *mottaker*.

Til § 3 *Bruk av elektronisk kommunikasjon ved henvendelser til et forvaltningsorgan*
Endringen er foretatt for å avstemme ordlyden med de endringer som er foreslått i Prop. 116 L (2012-2013), og innebærer ingen endring av gjeldende rett.

Til § 8 *Underretning om enkeltvedtak og enkelte andre meddelelser fra forvaltningsorgan*

Til nr. 1

Departementet foreslår at eForvaltningsforskriften § 8 nr (1) endres slik at hovedregelen om at forvaltningen kan benytte elektronisk kommunikasjon når det henvender seg til andre, fremgår av § 8.

Til nr. 2

Andre ledd presiserer at det en en rett til å reservere seg mot elektronisk kommunikasjon av enkeltvedtak fra forvaltningen. Av § 8 nr. (8) følger det at tilsvarende gjelder for tilfeller angitt i nevnte paragraf. Bestemmelsen sier også hvem reservasjonsretten gjelder for. Departementet foreslår at de som skal kunne reservere seg mot elektronisk kommunikasjon av enkeltvedtak er privatpersoner og enheter som ikke er registrert i Enhetsregisteret.

Frivillige organisasjoner som vil registrere seg i Frivillighetsregisteret må også være registrert i Enhetsregisteret. Disse vil da ikke kunne reservere seg mot digital kommunikasjon fra forvaltningen.

Til nr. 3

Bestemmelsen krever at den digitale kontaktinformasjonen registrert i register over digital kontaktinformasjon og reservasjon brukes til varsling av privatpersoner og enheter ikke registrert i Enhetsregisteret. Se imidlertid forslag til overgangsregler i utkastet § 48.

Til nr. 6

Kravet til ekstra elektronisk varsel etter § 8 nr (7) krever at informasjonssystemet registrerer om mottaker har åpnet meldingen.

Løsning for digital post fra forvaltningen vil lagre informasjon om når den enkelte melding ble åpnet. Denne informasjonen vil ikke bli gjort tilgjengelig for avsender så lenge ikke avsender uttrykkelig ber om det. Mottaker må da godta at slik informasjon meddeles avsender for å få tilgang til meldingen,

Til nr. 7

Kravet om ekstra elektronisk varsel gjelder for enkeltvedtak og *forhåndsvarsel etter forvaltningsloven § 16 og for andre meldinger som har betydning for vedkommendes rettsstilling, for behandlingen av saken eller for meldinger som det av andre grunner er av særlig betydning å sikre at vedkommende mottar*, jf § 8 nr (8).

Henvisningen til § 8 nr. (3) innebærer at den digitale kontaktinformasjonen registrert i register over digital kontaktinformasjon og reservasjon skal benyttes for varsling av privatpersoner og enheter som ikke er registrert i Enhetsregisteret, se imidlertid forslag til overgangsregler i utkastet § 48.

Til nr. 8

Ordlyden i § 8 nr. (8) er ikke foreslått endret. Endringen av § 8 nr. (2) til (7) medfører imidlertid at tilsvarende gjelder for *forhåndsvarsel etter forvaltningsloven § 16 og for andre meldinger som har betydning for vedkommendes rettsstilling, for behandlingen av saken eller for meldinger som det av andre grunner er av særlig betydning å sikre at vedkommende*, jf. § 8 nr. (8).

Til ny § 8 a Bruk av fullmektig i forbindelse med elektronisk kommunikasjon med forvaltningen
Bestemmelsen regulerer ikke når det er tillatt å bruke fullmektig og når dette ikke er tillatt. Det vil følge av annet regelverk. Dersom fullmektig brukes i forbindelse med elektronisk kommunikasjon med forvaltningen, må imidlertid bestemmelsen følges.

Det må fremgå av kommunikasjonen at vedkommende er representert ved fullmektig. Fullmektigen skal opptre i eget navn. Bruk av elektronisk ID tilhørende en annen må unngås. Det vil normalt være i strid med bruksvilkårene for elektronisk ID.

Til § 9 ny nr (3)
I Prop. 116 L (2012-2013) er det foreslått å endre forvaltningsloven § 30 første punktum og regulere fristregler i eForvaltningsforskriften. Bestemmelse med tilsvarende innhold er foreslått som § 9 ny nr (3). Bestemmelsen innebærer ingen endring av gjeldende rett.

****

Kapittel 3. Forvaltningsorganets strategi for informasjonssikkerhet

Til § 13 Internkontroll på informasjonssikkerhetsområdet
Forslaget refererer tekst fra Digitaliseringsrundskrivet og er tatt inn i forskriften for at disse tekstene skal harmoniseres.

Kjernen i justert pkt. 1, er pkt.1 i dagens §13 i forskriften.
En setning foreslås tatt ut:

> *"Sikkerhetsstrategien skal danne grunnlaget for forvaltningsorganets beslutninger om innføring og bruk av sikkerhetstjenester og -produkter på en helhetlig, planlagt, systematisk og dokumentert måte. "*

Den erstattes av følgende setning:

> *"Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet."*

På denne måten beholdes mål og strategi (i første setning i punktet) som et tydelig førende startpunkt og grunnlag. Videre tydeliggjøres det at nevnte mål og strategi inngår som grunnlaget i internkontrollen og at det som kreves er en normal internkontroll i forståelsen "styring og kontroll". Dette er både en kjent, men til dels underkommunisert, forståelse av internkontrollbegrepet og et kjent oversettelsesalternativ til originalen "internal contol" (Jf. Difi-rapport 2012:15 kap. 3.5). DFØ signaliserer tilsvarende retning på begrepsbruken i sin nye veileder om internkontroll (april 2013) der de nå benytter ettordsbegrepet "internkontroll" og setter likhetstegn («benyttes synonymt») mellom dette og økonomiregelverkets begrep intern kontroll (i to ord) (Jf. fotnote 14 s.11 i DFØs nye veileder i internkontroll fra april 2013). For det siste begrepet, «intern kontroll», har DFØ/SSØ tidligere ofte presisert at *«Kravene til intern kontroll i økonomiregelverket er også krav til risikostyring. Kravene sier eksplisitt at den interne kontrollen skal være innebygd i virksomhetens interne styring, og øke sannsynligheten for oppnåelse av virksomhetens mål ved at man identifiserer risikoer og tiltak for å redusere risikoene.» (Jf.* SSØ 2005, Risikostyring i staten. Håndtering av risiko i mål og resultatstyringen. Metodedokument, s. 11).

Internkontroll i forståelsen styring og kontroll er også i samsvar med hvordan begrepet internkontroll gjennomgående brukes i mange andre forskrifter. En harmonisering av begrepsbruken og forståelsen av internkontroll som "styring og kontroll" anser vi viktig for å

få helhetlig og reell styring og kontroll både i virksomhetsstyring generelt og innen informasjonssikkerhet spesielt. Styring og kontroll på informasjonssikkerhetsområdet er også tjent med å bli forstått som en ordinær og sammenhengende del av styring og kontroll i virksomheten.

Til sist i punkt 1 under beholdes nå presiseringen fra punkt 1 i opprinnelig §13 om inkludering av krav som er fastsatt i annen lov, forskrift eller instruks, men her supplert til en del av internkontrollen og ikke alene en del av sikkerhetsstrategien. Denne suppleringen gir mer helhetlig inkludering av annet regelverk i forvaltningsorganets styring og kontroll på informasjonssikkerhetsområdet.

Pkt. 2 (nytt) er kjernen i Digitaliseringsrundskrivets pkt 1.7. Dette anses som en presisering av tidligere pkt 2 og deler av tidligere pkt. 1 i nåværende §13. Punktet erstatter nåværende pkt. 2 i §13. Videre gjentas siste del i Digitaliseringsrundskrivets pkt 1.7, som gir en viktig føring for helhetlig virksomhetsstyring. Punktet er i samsvar med anerkjente standarder, jf. pkt. 3, og viktig for å unngå at §13 stimulerer til egne styringssystem på informasjonssikkerhetsområdet som ikke henger sammen med virksomhetsstyringen forøvrig. Det siste vil ofte gi mindre styring og kontroll, være mindre målorientert og koste mer i implementering og bruk.

Pkt. 3 (nytt) er en presisering i hovedsak fra ny nasjonal strategi for informasjonssikkerhet (jf. strategiens pkt. 4.1. siste avsnitt). Punktet tydeliggjør og presiserer som føring også for informasjonssikkerhetsområdet viktige allment anerkjente risikostyringsprinsipp i virksomhetsstyring og økonomistyring generelt. Dette er prinsipp som bl.a. også er nedfelt i økonomiregelverket i staten (jf. kap. 2.2, andre avsnitt) og som i kommunene normalt forstås som en oppfølging av kommuneloven § 23 pkt. 2 om administrasjonssjefens (rådmannens) ansvar for "betryggende kontroll".

Pkt. 4 (nytt/justert) er forskriftens opprinnelige pkt. 3, med en endring i første setning:
"*I den utstrekning det er relevant skal* ***sikkerhetsstrategien*** *også adressere, og om nødvendig stille krav til, bl.a.:....."*
Teksten "***og internkontrollen for øvrig***" foreslås nå lagt inn etter "sikkerhetsstrategien" som nå beholdes. Dette gir samlet en mer helhetlig ramme for å vurdere adressering av de påfølgende bokstavpunktene i pkt 5 (nåværende pkt. 3) i §13.

****

Kapittel 7. Løsning for digital post fra forvaltningen og digitale postkasser

Til § 27. *Bruk av løsning for digital post fra forvaltningen*
Første ledd presiserer at løsningen kan behandle personopplysninger uten samtykke fra den opplysningene gjelder. Det vil blant annet si at digital post som inneholder personopplysninger om andre enn mottaker kan behandles i løsningen. For eksempel kan NAV sende et brev til en mottaker som inneholder opplysninger om mottakers barn, uten at barna har samtykket til dette. Avsendervirksomheten må imidlertid ha behandlingsgrunnlag for behandlingen av opplysningene i sin virksomhet.

Annet ledd gir sentralforvalter mulighet til å sette vilkår for bruken av løsningen. Slike vilkår kan for eksempel være krav til grensesnitt, gyldig virksomhetsertifikat m.v.

Til § 28. *Reservasjonsrett*
Bestemmelsen fastslår at privatpersoner og enheter ikke registrert i Enhetsregisteret kan reservere seg mot å ha en digital postkasse. Slik register over digital kontaktinformasjon og reservasjon er planlagt pr i dag, vil ikke registeret inneholde opplysninger om andre enn privatpersoner (de som har fødselsnummer eller d-nummer). Man har pr i dag heller ikke planlagt registrering av andre enn privatpersoner. Utkastet til § 40 hjemler imidlertid mulighet for å registrerer digital kontaktinformasjon og reservasjonsstatus for andre enheter som ikke er registrert i Enhetsregisteret, dersom det blir aktuelt.

Andre ledd sier at avsendervirksomheter ikke kan sende digital post til mottakere som har reservert seg mot dette.

Til § 29. *Opprettelse av digitale postkasser*
Dersom mottaker ikke selv oppretter en digital postkasse, gir bestemmelsen mulighet til å tildele en digital postkasse til mottaker. Se imidlertid forslag til overgangsregler i utkastet § 47.

Til § 30. *Mottakers rett til varsel*
Denne bestemmelsen gjelder til forskjell fra § 8 nr (3) for alle meldinger uavhengig av hva som sendes til mottakers digitale postkasse. Mottaker kan imidlertid velge å ikke bli varslet om ny post i den digitale postkassen.

Regelen om ekstra varsel i § 8 nr (7) gjelder også for enkeltvedtak osv. som kommuniseres via løsning for digital post fra forvaltningen.

Tredje ledd presiserer at det er den digitale kontaktinformasjonen i register over digital kontaktinformasjon og reservasjon som skal benyttes til varsling. Se imidlertid forslag til overgangsregler i utkastet § 47.

Konfigurering av varsel er naturlig å gjøre hos postkasseleverandøren. Avsendervirksomheten trenger derfor ikke opplysninger om mottaker er varslet eller om mottaker ikke har åpnet meldingen og skal varsles ekstra. Det er derfor ikke lagt opp til at den informasjonen vil være tilgjengelig for avsendervirksomheten. Dersom avsendervirksomheten ønsker informasjon om mottaker har åpnet meldingen, må mottaker samtykke til dette for å få åpnet meldingen.

Til § 31. *Avsendervirksomhetens* ansvar
Første ledd plasserer ansvaret for personopplysninger som behandles i løsningen hos avsendervirksomhetene.

Annet ledd presisere at det er avsendervirksomheten som er ansvarlig for å vurdere om det er forsvarlig å benytte løsningen i det enkelte tilfellet. Krav til forsvarlig saksbehandling fremgår av forvaltningslovens alminnelige bestemmelser og ulovfestet rett.

Til § 32. *Sentralforvalters ansvar*
Sentralforvalters ansvar for informasjonssikkerheten innebærer ivaretakelse av konfidensialitet, integritet og tilgjengelighet, jf personopplysningsloven § 13 første ledd og personopplysningsforskriften kapittel 2.

For omtale av hva som ligger i ansvaret for informasjonssikkerheten, se omtale av dette under punkt 8.3.

Til § 33. *Postkasseleverandørens ansvar*
Postkasseleverandørens ansvar for informasjonssikkerheten innebærer ivaretakelse av konfidensialitet, integritet og tilgjengelighet, jf personopplysningsloven § 13 første ledd og personopplysningsforskriften kapittel 2.

For omtale av hva som ligger i ansvaret for informasjonssikkerheten, se omtale av dette under punkt 8.3.

Til § 35. *Bruk av den digitale postkassen*
Bestemmelsen presiserer at mottaker skal ha bestemmelsesrett over innholdet i sin digitale postkasse. Dersom mottaker dør, skal arvingene få tilgang til avdødes digitale postkasse.

Til § 36. *Bytte av postkasseleverandør*
Mottakers rett til å bytte postkasseleverandør innebærer en rett til å velge mellom de leverandørene sentralforvalter har inngått avtale med, jf definisjonen av postkasseleverandør i § 2 nr. 5. Digital post kan overføres mellom postkasseleverandører mår mottaker bytter digital postkasse. Det er imidlertid mottaker selv som må initiere og kontrollere overføringen.

Til § 37. *Opphør av postkasseleverandørens virksomhet knyttet til løsning for digital post fra forvaltningen*
Bestemmelsen gjelder tilfeller der postkasseleverandøren selv avvikler sin virksomhet, går konkurs, eller ikke lenger har en avtale med sentralforvalter om at postkasseleverandøren skal motta digital post fra løsning for digital post fra forvaltningen.

Mottaker skal i slike tilfeller få velge om vedkommende vil bytte til en ny postkasseleverandør eller få overført innholdet i sin digitale postkasse til seg på annen måte.

****

Kapittel 8. Digital kontaktinformasjon og reservasjon

Til § 38. *Register over digital kontaktinformasjon og reservasjon*
Bestemmelsen angir hva opplysningene i registeret kan brukes til. Formuleringen *"i forbindelse med saksbehandling og utføring av forvaltningsoppgaver for øvrig",* er ment å dekke forvaltningens totale oppgaveløsning.

Departementet vurderer det slik at opplysninger kan utleveres fra register over digital kontaktinformasjon og reservasjon til bruk i saksbehandling og ved utføring av forvaltningsoppgaver også for de virksomheter som har hele eller deler av sin virksomhet unntatt fra forvaltningslovens virkeområde.

Behandlingen av opplysninger i register over digital kontaktinformasjon og reservasjon er hjemlet i forvaltningsloven § 15a. Det forhindrer imidlertid ikke bruk av opplysningene i virksomheter som på ulike måter er unntatt fra forvaltningslovens virkeområde, så lenge opplysningene skal brukes innenfor formålet angitt i utkastet § 41.

Til § 39. *Behandlingsansvarlig*
Med "tilhørende infrastruktur" menes at ansvaret blant annet inkluderer det som i figur 2 under punkt 4.2 er omtalt som oppslagstjenesten.

Til § 40. *Opplysninger i register over digital kontaktinformasjon og reservasjon*
Til nr 7 – *den registrertes fullmaktsforhold*
Det er planlagt at fullmaktsforhold skal registreres i register over digital kontaktinformasjon og reservasjon. Bestemmelsen gir en mulighet for at denne typen opplysninger kan registreres i registeret dersom en løsning for fullmaktsregistrering blir utviklet.

Til nr 10 – *sertifikatinformasjon for kryptering*
Meldinger som sendes fra avsendervirksomhet til mottaker via løsning for digital post fra forvaltningen skal krypteres fra avsendervirksomhet. Dette krever at det registreres informasjon om hvilket sertifikat avsendervirksomheten skal bruke ved kryptering av meldingen. Postkasseleverandøren må gjøre sertifikatet tilgjengelig for kontaktregisteret. Det kan være et unikt krypteringssertifikat tilhørende innbyggeren eller dennes postkasse, eller det kan være postkasseleverandørens virksomhetssertifikat.

Til nr 11 – *andre opplysninger*
Andre opplysninger kan for eksempel være nummer til annen telefon enn mobiltelefon, hvilken målform mottaker bruker osv. Det er imidlertid bare opplysninger som er nødvendige for forvaltningens digitale kommunikasjon relatert til saksbehandlingen og forvaltningsoppgaver for øvrig, som kan registreres.

Til § 41. *Oppdatering av opplysninger i register over digital kontaktinformasjon og reservasjon*
Den registerte bør med jevne mellomrom oppfordres til å oppdatere eller bekrefte at de registrerte opplysningen er korrekte. Det foreslås at dette som hovedregel skjer to ganger i året. Bestemmelsen angir ingen virkning av at den registrerte ikke følger oppfordringen. Se imidlertid forslag til overgangsbestemmelse i utkastet § 47.

Til § 42. *Kobling med andre registre*
Med *kobling* menes nødvendige oppslag i andre registre for å sikre at de registrerte opplysningene er korrekte og oppdaterte, eller andre administrative formål. Opplysninger i registeret må blant annet kontrolleres slik at opplysninger om døde personer fjernes fra registeret og for kontroll av fødselsnumre og d-numre.

Til § 43. *Lagringstid*
Bestemmelsen innebærer at opplysninger i registeret skal slettes når de ikke lenger er nødvendige for å ivareta formålet med registreringen.

Dersom en innbygger reserverer seg mot digital kommunikasjon fra forvaltningen, vil ikke nødvendigvis kontaktopplysningene måtte slettes. Formålet med register over digital kontaktinformasjon og reservasjon er videre en varsling om digital post, og kontaktopplysningene vil derfor fremdeles kunne lagres. Reservasjonsstatus må uansett kunne registreres om vedkommende.

****

Kapittel 10. Overgangsbestemmelser

Til § 47. *Overgangsbestemmelse*
Første og annet ledd innebærer at dagens bestemmelser om samtykke fra mottaker ved elektronisk kommunikasjon fra forvaltningen inntil videre opprettholdes for de forvaltningsorganer som skal kommunisere med privatpersoner eller enheter ikke registrert i

Enhetsregisteret og som ikke er koblet opp mot register over digital kontaktinformasjon og reservasjon. Bakgrunnen for dette er at disse virksomhetene ikke har mulighet for å sjekke om mottaker er reservert eller ikke.

Som en konsekvens av første og annet ledd angir tredje ledd at samtykker avgitt til forvaltningsorganer må gjelder i en overgangsperiode selv om mottaker har reservert seg. Dersom samtykket er tidsavgrenset, faller det bort på vanlig måte før 1. juli 2016. Mottaker kan etter vanlige regler trekke samtykke tilbake når vedkommende måtte ønske det.

Kravet til oppdatert digital kontaktinformasjon i fjerde ledd innebærer i praksis at forvaltningen ikke kan kommunisere digitalt med de som ikke følger oppfordringen om å oppdatere eller bekrefte at kontaktinformasjonen er korrekt, jf § 41.

Femte ledd gir overgangsbestemmelser knyttet til de paragrafene i forskriften som krever at det er den digitale kontaktinformasjonen i register over digital kontaktinformasjon og reservasjon som benyttes til varsling av mottaker. Ettersom ikke alle forvaltningsorganer er koblet opp mot dette registeret i en overgangsperiode, vil forvaltningsorganer måtte kunne benytte annen digital kontaktinformasjon til mottaker. Den elektroniske adressen som ble innhentet sammen med samtykket kan da benyttes så lenge samtykket gjelder.

Overgangsbestemmelsen gjelder til 1. juli 2016. Innen den tid vil trolig alle forvaltningsorganer ha koblet seg opp mot register over digital kontaktinformasjon og reservasjon.

Til § 48. *Gjenbruk av personopplysninger i kontaktregisteret tilknyttet ID-porten*
Bestemmelsen gir hjemmel til å overføre personopplysningene som i dag er registeret i kontaktregisteret tilknyttet ID-porten til register over digital kontaktinformasjon og reservasjon.

Annet ledd presiserer at den enkelte skal informeres om overføringen, om adgangen til å oppdatere opplysningene, om retten til reservasjon og retten til å slette opplysningene.

Til ikrafttredelsen
Ikrafttredelse er foreslått til 1. januar 2014.

Løsning for digital post fra forvaltningen skal i henhold til planer for løsningen kunne starte opp medio 2014. Testing og pilotering av løsningen vil kunne innebære behandling av reelle personopplysninger. Rammebetingelsene for behandlingen av personopplysninger må derfor være på plass før testing og pilotering kan starte.

11. Utkast til forskrift om endringer i eForvaltningsforskriften

I

Endringer i eForvaltningsforskriften

§ 2 første ledd skal lyde:

(1) I denne forskrift menes med:

1. *løsning for digital post fra forvaltningen: løsning etablert for formidling av post digitalt fra forvaltningen til mottakers digitale postkasse.*

2. *sentralforvalter av løsning for digital post fra forvaltningen: den virksomhet departementet utpeker.*

3. *avsendervirksomhet: offentlig virksomhet som har inngått avtale med sentralforvalter om bruk av løsning for digital post fra forvaltningen.*

4. *postkasseleverandør: leverandør av digitale postkasser som har inngått avtale med sentralforvalter av løsning for digital post fra forvaltningen.*

5. *digital postkasse: mottakers digitale postkasse som denne disponerer for mottak og lagring av post som sendes digitalt fra forvaltningen.*

6. *mottaker: privatperson og enhet som ikke er registrert i Enhetsregisteret.*

§ 2 første ledd blir annet ledd.

§ 3 første ledd skal lyde:

§ 3. *Bruk av elektronisk kommunikasjon ved henvendelser til et forvaltningsorgan*

(1) ~~Enhver~~ *Alle* som henvender seg til et forvaltningsorgan kan benytte elektronisk kommunikasjon, *dersom forvaltningsorganet har lagt til rette for dette, det skjer på den anviste måten* ~~når det skjer i henhold til den form og fremgangsmåte~~ og ved bruk av den elektroniske adressen, som forvaltningsorganet har anvist for den aktuelle type henvendelse.

a) Med ~~*form eller fremgangsmåte*~~ *den anviste måten* menes for eksempel bruk av spesielle skjema, bruk av en bestemt prosedyre eller lignende.

(b) Med *elektronisk adresse* menes for eksempel en adresse til et nettsted, en e-postadresse, et nummer til en SMS-tjeneste eller lignende.

(c) Med *elektronisk kommunikasjon* menes bruk av for eksempel Internett, eller liknende kommunikasjonssystem, og bruk av talestyrte eller andre automatiske telefontjenester, men ikke bruk av taletelefon eller annen muntlig kommunikasjon.

<u>§ 8 skal lyde:</u>

§ 8. *Meddelelser fra forvaltningsorgan, herunder underretning om enkeltvedtak*

(1) Et forvaltningsorgan kan benytte elektronisk kommunikasjon når det henvender seg til andre.

(2) Privatpersoner og enheter ikke registrert i Enhetsregisteret kan reservere seg mot å motta enkeltvedtak elektronisk fra forvaltningen. Reservasjonen skal registreres i register over digital kontaktinformasjon og reservasjon, jf kapittel 8.

(*3*) Forvaltningsorganet skal sende parten varsel om at enkeltvedtak er fattet og om hvor og hvordan vedkommende kan skaffe seg kunnskap om innholdet. For *privatpersoner eller enhet som ikke er registrert i Enhetsregisteret, skal den varslingsadresse som er registrert i register over digital kontaktinformasjon og reservasjon benyttes.*

(*4*) Innholdet i enkeltvedtaket skal *sendes til partens digitale postkasse eller* gjøres tilgjengelig fra annet egnet informasjonssystem, jf. blant annet kravene i nr. (3), (5), og (6).

(*5*) Forvaltningsorganet skal forebygge risiko for uberettiget innsyn i enkeltvedtak på en tilfredsstillende måte.

(*6*) Informasjonssystemet skal registrere tidspunktet for når parten har skaffet seg tilgang til enkeltvedtaket og data som bekrefter at vedkommende har rett til å gjøre seg kjent med vedtaket.

(7) Har parten ikke skaffet seg tilgang til enkeltvedtaket innen én uke fra det tidspunktet vedtaket ble gjort tilgjengelig, og varsel ble sendt, skal parten varsles på nytt i samsvar med nr (3).

(*8*) Det som er sagt om underretning om enkeltvedtak i nr. (*2*)–(*7*) ovenfor, gjelder tilsvarende ved forhåndsvarsel etter forvaltningsloven § 16 og for andre meldinger som har betydning for vedkommendes rettsstilling, for behandlingen av saken eller for meldinger som det av andre grunner er av særlig betydning å sikre at vedkommende mottar.

(*9*) I forbindelse med underretning om enkeltvedtaket skal det informeres om forvaltningsorganet har lagt til rette for mottak av klage i elektronisk form og hva som er rette elektroniske adresse. Det skal også informeres om at parten bør kontrollere at han mottar bekreftelse når klage leveres i elektronisk form.

(10) Klagefristen etter forvaltningsloven § 29 begynner å løpe på det tidspunktet vedtaket er tilgjengelig i den digitale postkassen, eller tilgjengelig fra annet egnet informasjonssystem, og varsel om dette er sendt til parten, jf. nr. (3).

<u>Ny § 8a skal lyde:</u>

§ 8 a. *Bruk av fullmektig i forbindelse med elektronisk kommunikasjon med forvaltningen*

Når en person opptrer på vegne av en annen (fullmektig) i forbindelse med elektronisk kommunikasjon med forvaltningen, skal det fremgå av kommunikasjonen at vedkommende er representert ved fullmektig. Fullmektigen skal opptre i eget navn og ikke benytte elektronisk identitetsbevis (e-ID) tilhørende den han opptrer på vegne av.

<u>§ 9 ny nr (3) skal lyde:</u>

(3) Klage er rettidig framsatt dersom den er kommet fram til den elektroniske adressen som forvaltningsorganet har oppgitt for mottak av elektroniske klager, innen klagefristens utløp.

<u>Overskriften til kapittel 3 skal lyde:</u> ***Styring og kontroll med informasjonssikkerheten***
<u>§ 13 skal lyde:</u>

§ 13. *Internkontroll på informasjonssikkerhetsområdet*

(1)Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

(2) Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området.

(3) Omfang og innretning på internkontrollen skal være tilpasset risiko

(4) I den utstrekning det er relevant skal sikkerhetsstrategien og internkontrollen for øvrig også adressere, og om nødvendig stille krav til, bl.a.:

a) prosedyrer for anskaffelse, bruk, oppbevaring og sikring av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel knyttet til personlige sertifikat eller sertifikat for ansatt i forvaltningen, jf. § 15, § 17 og § 20;

b) prosedyrer for anskaffelse, bruk, oppbevaring og sikring av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel knyttet til virksomhetssertifikat, jf. § 14 og § 21;

c) prosedyrer for å etablere og opprettholde et sikkert brukermiljø der det benyttes elektroniske signaturer, kryptering eller andre sikkerhetstjenester, jf. § 18;

d) prosedyrer for varsling og tilbaketrekking av sertifikat og passord/PIN-koder ved mistanke om tap eller misbruk, jf. § 23;

e) prosedyrer for kontroll av sertifikater og tilbaketrekkingslister ved mottak av melding utstyrt med elektronisk signatur, herunder krav til hvor oppdatert informasjon om sertifikaters status bør være for de ulike formål sertifikatene benyttes for, jf. § 25;

f) prosedyrer for å nekte bruk av sertifikat mv. ved misbruk av elektronisk kommunikasjon med forvaltningen, jf. § 12;

g) prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon, jf. § 5 og § 24, se også personopplysningsloven § 13 og personopplysningsforskriften kap. 2;

h) prosedyrer for sikkerhetskopiering, oppbevaring og deponering av dekrypteringsnøkkel for opplysninger som angår forvaltningsorganet, jf. § 22.

Nytt kapittel 7 skal lyde:

Kapittel 7. Løsning for digital post fra forvaltningen og digitale postkasser

§ 27. *Bruk av løsning for digital post fra forvaltningen*

(1) Løsning for digital post fra forvaltningen kan, uten samtykke fra den opplysningene gjelder, behandle de opplysninger som sendes til mottakers digitale postkasse via løsning for digital post fra forvaltningen.

(2) Sentralforvalter setter vilkår for bruk av løsningen for digital post fra forvaltningen.

§ 28. *Reservasjonsrett*

(1) Privatpersoner og enheter ikke registrert i Enhetsregisteret kan reservere seg mot å ha en digital postkasse.

(2) Avsendervirksomheter skal ikke bruke løsning for digital post fra forvaltningen for forsendelse av meldinger til mottakere som har reservert seg, jf første ledd.

§ 29. *Opprettelse av digitale postkasser*

(1) Mottakere som ikke selv oppretter en digital postkasse hos en postkasseleverandør kan tildeles en digital postkasse.

(2) Dersom mottaker tildeles en digital postkasse etter første ledd, skal mottaker varsles om dette. Den digitale kontaktinformasjonen registrert i register over digital kontaktinformasjon og reservasjon skal benyttes til slik varsling.

§ 30. *Mottakers rett til varsel*

(1) Med mindre annet følger av lov eller forskrift for det enkelte område eller den aktuelle type henvendelse, skal mottakeren varsles når det kommer ny post fra et forvaltningsorgan i den digitale postkassen.

(2) Mottaker kan velge å ikke bli varslet om ny post i den digitale postkassen som ikke er regulert i § 8 nr (3),(7) og (8).

(3) Ved varsling skal den varslingsadresse som mottaker har registrert i register over digital kontaktinformasjon og reservasjon benyttes.

§ 31. *Avsendervirksomhetens ansvar*

(1) Avsendervirksomheten er ansvarlig for de personopplysninger og innholdet for øvrig som sendes til mottakers digitale postkasse via løsning for digital post fra forvaltningen.

(2) Avsendervirksomheten er ansvarlig for å vurdere om det er forsvarlig å benytte løsning for digital post fra forvaltningen for formidling av de aktuelle personopplysningene

og innholdet for øvrig. Forsvarlighetsvurderingen skal blant annet knyttes opp mot krav om forsvarlig saksbehandling og risikovurderinger knyttet til informasjonssikkerhet.

(3) Avsendervirksomhetens ansvar for behandlingen av personopplysningene opphører når personopplysningene er mottatt i mottakers digitale postkasse.

§ 32. *Sentralforvalters ansvar*

(1) Sentralforvalter er ansvarlig for informasjonssikkerheten i løsning for digital post fra forvaltningen.

(2) Sentralforvalter skal gjennomføre nødvendige sikkerhetstiltak til vern av kommunikasjon i løsning for digital post fra forvaltningen. Ved sikkerhetsbrudd, og i situasjoner der det oppstår risiko ut over det vanlige for brudd på sikkerheten skal sentralforvalter varsle avsendervirksomhetene og postkasseleverandørene om sikkerhetsbruddet og/eller risikoen.

§ 33. *Postkasseleverandørens ansvar*

(1) Postkasseleverandøren er ansvarlig for informasjonssikkerheten i de digitale postkassene.

(2) Postkasseleverandøren skal gjennomføre nødvendige sikkerhetstiltak til vern av opplysninger lagret i mottakers digitale postkasser. Ved sikkerhetsbrudd, og i situasjoner der det oppstår risiko ut over det vanlige for brudd på sikkerheten skal postkasseleverandøren informere sentralforvalter om sikkerhetsbruddet og/eller risikoen. Sentralforvalter tar stilling til om også mottaker har krav på varsel eller av andre grunner bør varsles om forholdet.

§ 34*. Taushetsplikt*

(1) Enhver som behandler opplysninger om noens personlige forhold, eller andre opplysninger som nevnt i forvaltningsloven § 13, i løsning for digital post fra forvaltningen, har taushetsplikt som fastsatt i forvaltningsloven §§ 13 til 13e. Taushetsplikten omfatter også opplysninger som kan ha betydning for informasjonssikkerheten i løsning for digital post fra forvaltningen.

(2) Taushetsplikt etter første ledd gjelder også for postkasseleverandør og enhver som utfører arbeid eller tjeneste for sentralforvalter, postkasseleverandør, installatør, teknisk kontrollorgan eller myndigheten, også etter at vedkommende har avsluttet arbeidet eller tjenesten.

§ 35. *Bruk av den digitale postkassen*

(1) Bare mottakeren skal ha tilgang til den digitale postkassen.

(2) Mottakeren kan gi tilgang til den digitale postkassen til andre.

(3) Post i mottakers digitale postkasse skal oppbevares så lenge mottakeren ønsker det.

(4) Bare mottakeren kan slette post i den digitale postkassen som denne disponerer.

(5) Ved dødsfall kan mottakers arvinger få tilgang til mottakers postkasse ved framvisning av skifteattest.

§ 36. *Bytte av postkasseleverandør*

(1) Mottaker har rett til å bytte postkasseleverandør.

(2) Dersom mottaker bytter postkasseleverandør, skal all digital post fra forvaltningen i mottakers digitale postkasse overføres til ny postkasseleverandør på bestilling fra mottaker.

§ 37. *Opphør av postkasseleverandørens virksomhet knyttet til løsning for digital post fra forvaltningen*

Dersom virksomheten til en postkasseleverandør avvikles, eller postkasseleverandøren ikke lenger har et avtaleforhold med sentralforvalter, skal all post overføres til digitale postkasser hos en av de andre postkasseleverandørene eller til mottaker selv.

<u>Nytt kapittel 8 skal lyde</u>

Kapittel 8 Digital kontaktinformasjon og reservasjon

§ 38. *Register over digital kontaktinformasjon og reservasjon*

(1) Det etableres et register over digital kontaktinformasjon og reservasjon.

(2) Opplysninger i register over digital kontaktinformasjon og reservasjon kan benyttes i forbindelse med saksbehandling og utføring av forvaltningsoppgaver for øvrig, herunder varsling av mottaker ved utsendelse av digital post.

(3) Forvaltningsorgan kan benytte kopi av registeret for digital kontaktinformasjon og reservasjon når det er nødvendig for saksbehandling og utføring av forvaltningsoppgaver for øvrig. Behandlingsansvarlige avgjør hvem som kan benytte kopi.

(4) Kopier av register for digital kontaktinformasjon og reservasjon skal oppdateres jevnlig, minimum én gang daglig.

(5) Postkasseleverandørene kan benytte opplysningene i registeret for videresending av digital post, inkludert flytting av digital post ved skifte av postkasseleverandør.

§ 39. *Behandlingsansvarlig*

Direktoratet for forvaltning og IKT er behandlingsansvarlig for register over digital kontaktinformasjon og reservasjon med tilhørende infrastruktur.

§ 40. *Opplysninger i register over digital kontaktinformasjon og reservasjon*

Register over digital kontaktinformasjon kan, uten samtykke fra den registrerte, inneholde følgende typer opplysninger om privatpersoner og enheter ikke registrert i Enhetsregisteret:

1. *den registrertes navn og ordinære kontaktopplysninger, samt*
2. *fødselsnummer,*
3. *den registrertes mobiltelefonnummer,*
4. *den registrertes e-postadresse,*
5. *om den registrerte ønsker å motta varsel,*
6. *opplysninger om den registrertes eventuelle reservasjon mot elektronisk kommunikasjon, jf § 8 nr (2) og nr (8) og § 28,*

7. *den registrertes fullmaktsforhold*
8. *opplysninger om hvilken digitale postkasse den registrerte har,*
9. *adresseringsinformasjon for den digitale postkassen,*
10. *sertifikatinformasjon og andre opplysninger som er nødvendige for å kryptre meldinger og*
11. *andre opplysninger som er nødvendige for forvaltningens digitale kommunikasjon i forbindelse med saksbehandling og utføring av forvaltningsoppgaver.*

§ 41. *Oppdatering av opplysninger i register over digital kontaktinformasjon og reservasjon*

Den enkelte som det er registret opplysninger om i register over digital kontaktinformasjon og reservasjon bør minst to ganger årlig, i forbindelse med pålogging til sin digitale postkasse eller ved annen bruk av ID-porten, oppfordres til å oppdatere eller bekrefte at opplysningene registrert om vedkommende i registeret er korrekte. Hvis den registrerte ikke har logget seg på sin digitale postkasse eller på annen måte benyttet ID-porten på mer enn tolv måneder, bør det sendes oppfordring som nevnt ovenfor til den eller de varslingsadresser vedkommende er registrerte med, samt til den digitale postkassen.

§ 42. *Kobling med andre registre*

Opplysninger som registreres i register over digital kontaktinformasjon og reservasjon kan, for å sikre at opplysningene i registeret er korrekte og oppdaterte og for andre administrative formål, kobles med Folkeregisteret.

§ 43. *Lagring av opplysninger*

Opplysninger i register over digital kontaktinformasjon og reservasjon kan oppbevares i ubegrenset tid, med mindre annet følger av denne forskriften eller personopplysningsloven.

§ 44*. Taushetsplikt*

(1) Enhver som behandler opplysninger om noens personlige forhold, eller andre opplysninger som nevnt i forvaltningsloven § 13, i register over digital kontaktinformasjon og reservasjon, har taushetsplikt som fastsatt i forvaltningsloven §§ 13 til 13e. Taushetsplikten omfatter også opplysninger som kan ha betydning for informasjonssikkerheten i register over digital kontaktinformasjon og reservasjon.

(2) Taushetsplikt etter første ledd gjelder også for enhver som utfører arbeid eller tjeneste for behandlingsansvarlig, installatør, teknisk kontrollorgan eller myndigheten, også etter at vedkommende har avsluttet arbeidet eller tjenesten.

Kapittel 7 blir kapittel 9, § 27 blir § 45, og § 28 blir § 46.

<u>Nytt kapittel 10 skal lyde:</u>

Kapittel 10 Overgangsbestemmelser

§ 47. *Overgangsbestemmelse*

(1) Forvaltningsorganer som ikke har koblet seg til register over digital kontaktinformasjon og reservasjoner, kan bare gi forhåndsvarsel og underretning om vedtak ved bruk av elektronisk kommunikasjon til privatpersoner og enheter ikke registrert i Enhetsregisteret, når mottakeren uttrykkelig har godtatt dette og har oppgitt den elektroniske adressen som skal benyttes for slikt formål.

(2) Det samme gjelder for andre meldinger som har betydning for mottakerens rettsstilling, for behandlingen av saken eller for meldinger som det av andre grunner er av særlig betydning å sikre at vedkommende mottar.

(3) Med mindre et avgitt samtykke er tidsbegrenset, gjelder samtykke til elektronisk kommunikasjon avgitt direkte til forvaltningsorganer, frem til det enkelte forvaltningsorgan har koblet seg til register over digital kontaktinformasjon og reservasjoner og uansett ikke ut over 1. juli 2016. Dette gjelder selv om mottaker i perioden reserverer seg mot elektronisk kommunikasjon, jf. § 8 nr. (2) og nr. (8) og § 28. Den elektroniske adressen som ble innhentet sammen med samtykket kan benyttes så lenge samtykket gjelder.

(4) Dersom opplysninger om den enkelte i register over digital kontaktinformasjon og reservasjon ikke har vært brukt, blitt oppdatert eller bekreftet at er korrekte de siste 12 månedene, skal opplysningene ikke brukes til å varsle vedkommende etter § 8 nr (2) eller §§ 29 og 30.

(5) §29 trer i kraft 1. januar 2016. Forvaltningsorganer som kobler seg til register over digital kontaktinformasjon og reservasjon, må bruke den kontaktinformasjonen som er registert om vedkommende i registeret for å sende varsel etter § 8 nr (3) annet punktum og § 30 tredje ledd, fra de er koblet opp. For øvrig trer plikten til å bruke den kontaktinformasjonen som er registrert i register over digital kontaktinformasjon og reservasjon til å sende varsel etter § 8 nr (3) annet punktum og § 30 tredje ledd i kraft 1. januar 2016.

(6) Denne bestemmelsen gjelder ikke utover 1. juli 2016.

§ 48. *Gjenbruk av personopplysninger i kontaktregisteret tilknyttet ID-porten*

(1) Personopplysninger som er registrert om den enkelte i kontaktregisteret tilknyttet ID-porten kan utleveres til og gjenbrukes i register over digital kontaktinformasjon og reservasjon.

(2) Den enkelte skal informeres om utleveringen og om adgangen til å oppdatere opplysningene, samt om adgangen til å reservere seg mot elektronisk kommunikasjon, jf § 8 nr (2) og nr (8) og § 28, og til å slette kontaktopplysningene.

II

Ikrafttredelse

Denne forskrift trer i kraft 1. januar 2014.

VEDLEGG

1. Kryptografisk beskyttelse av digital post[6]

Her beskrives løsningen for å sikre integritet og konfidensialitet i overføringen av digital post fra avsendervirksomhetene til innbyggernes postkasser.

Formatet på den digitale sendingen er ikke bestemt, så detaljnivået på den kryptografiske sikringen er heller ikke endelig bestemt. Valg av format vil gi føringer for om signering og kryptering bør være en del av formatet, noe som vil være naturlig for XML-baserte formater, eller om en vil bruke andre protokoller som er helt uavhengig av formatet til det som skal beskyttes.

Beskrivelsen spesifiserer en av de sikringsmetodene som vil tilbys av sikker digital posttjenesten. Det kan også etableres andre metoder, med høyere eller lavere krav til sikkerhet. Løsningen beskrevet her er tiltenkt å kunne beskytte informasjon av særlig følsomme taushetsbelagte opplysninger, herunder de fleste sensitive personopplysninger, stigmatiserende opplysninger m.v. Eksempelvis opplysninger om sykdom.

Konfidensialitet

Avsendervirksomheten benytter oppslagstjenesten for digital kontaktinformasjon for å få levert innbyggerens digitale postkasseadresse og tilhørende X.509 sertifikat. Postkasseleverandøren må gjøre sertifikatet tilgjengelig for oppslagstjenesten, og det kan enten være et unikt sertifikat tilhørende innbyggeren eller innbyggerens postkasse, eller det kan være postkasseleverandørens virksomhetssertifikat. Løsningen er valgt med tanke på fleksibilitet, der postkasseleverandørene kan konkurrere på sikkerhet, uten at avsendervirksomhetene må endre sine systemer for utsendelse av digital post. Postkasseleverandøren kan tilby beskyttelse under samme virksomhetssertifikat for alle sine kunder, eller de kan tilby unike sertifikater per innbygger, enten i egen kontroll, eller hvor innbyggeren selv sitter på den private nøkkelen som er nødvendig for å se innholdet. Sertifikatene postkasseleverandøren gjør tilgjengelig må være kvalifiserte, og må kostnadsfritt kunne valideres opp mot en sertifikatutsteder.

Avsendervirksomheten validerer sertifikatet og benytter dette for å kryptere de symmetriske nøklene som benyttes for å kryptere selve innholdet i den digitale forsendelsen. Det vil være behov for å endre algoritmer og protokoller over tid, men i første versjon vil det være PKCS#1 v2.1 som benyttes for asymmetrisk beskyttelse av symmetriske nøkler.

Det sensitive innholdet i en digital forsendelse krypteres med symmetriske nøkler. Disse nøklene genereres tilfeldig og gjenbrukes ikke. Fra starten vil det være AES kryptering i en modus som vil bli spesifisert etter formatet på de digitale brevene er bestemt.

Noe metadata må være tilgjengelig under flytting av digital post fra avsender til mottaker, og denne kan ikke være innenfor det som er kryptert. Selv om denne informasjonen er utenfor det krypterte innholdet, så vil den delvis være beskyttet under overførselen, fordi i tillegg til innholdskryptering vil det være kanalkryptering i form av SSL/TLS mellom avsendervirksomheten og meldingsformidleren, og mellom meldingsformidleren og postkasseleverandøren.

[6] Utarbeidet av Direktoratet for forvaltning og IKT.

Integritet

Det er flere forhold som ivaretas ved integritetsbeskyttelse. Meldingsformidler og postkasseleverandør vil benytte integritet av avsender for å hindre uautoriserte avsendere, og for å etablere et trygt sporings- og fakturaregime. Videre kan innbygger være trygg på at brevet faktisk er fra den som har utgitt seg for å sende brevet.

God integritet hindrer at brevets innhold eller metadata endres underveis i transporten mellom avsender og mottaker, og sørger for at brevet kommer frem til riktig postkasse.

Flere løsninger har vært vurdert, og vi har kommet frem til at virksomhetssertifikater er den løsningen som har størst utbredelse og sikrer integritet på best måte.

Avsendervirksomheten signerer den digitale forsendelsen med sitt eget virksomhetssertifikat. Det vil være behov for å endre algoritmer og protokoller over tid, men i første versjon vil signaturen være PKCS #1 v1.5 eller v2.1, enten i XML-format sammen med innholdet eller frittstående.

For å sende digital post må en avsendervirksomhet være registrert med organisasjonsnummer hos sentralforvalteren av sikker digital post, og må inneha et virksomhetssertifikat som benyttes for å signere all digital post. Meldingsformidler og postkasseleverandører vil validere signaturen, og undersøke om avsendervirksomheten er registrert for utsending av digital post.