Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

Forskrift om elektronisk kommunikasjon med og i forvaltningen

Fastsatt ved kgl.res. 25. juni 2004 med hjemmel i lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven) § 15a og lov 15. juni 2001 nr. 81 om elektronisk signatur § 5. Fremmet av Arbeids- og administrasjonsdepartementet (nå Kommunal- og moderniseringsdepartementet). Endret ved forskrifter 2 des 2005 nr. 1398, 17 okt 2008 nr. 1119, 23 nov 2012 nr. 1092, 7 feb 2014 nr. 102 (forskriften endret i sin helhet).

Kapittel 1. Innledende bestemmelser

§ 1 *Forskriftens formål og anvendelsesområde* [1]

Forskriftens formål er å legge til rette for sikker og effektiv[2] bruk av elektronisk kommunikasjon[3] med og i forvaltningen. Den skal fremme forutsigbarhet og fleksibilitet[4] og legge til rette for samordning[5] av sikre og hensiktsmessige tekniske løsninger. Forskriften skal legge til rette for at enhver på en enkel måte kan utøve sine rettigheter og oppfylle sine plikter overfor det offentlige.[6]

---

[1] Se om forskriftens formål og anvendelsesområde i Veilederen del 1, kapittel 2 *eForvaltningsforskriftens formål og virkeområde*.

[2] Sikker og effektiv bruk av elektronisk kommunikasjon oppnås ved å benytte tekniske, organisatoriske og rettslige virkemidler i samvirke. Det er ikke bare teknikken som må være til å stole på, men også det organisasjonsmessige rundt de tekniske løsningene, f eks organisering av loggfunksjoner, tilgangskontroll og revisjonsspor. Det kan også knyttes plikter til aktørene i kommunikasjonen, f eks plikt til å sende en klage på nytt hvis den som har sendt inn en klage ikke mottar kvittering.

[3] Se § 3 første ledd, bokstav c.

[4] Det kan synes som en betydelig utfordring å skulle fremme forutsigbarhet samtidig som en skal fremme fleksibilitet. Tanken er imidlertid å kombinere behovstilpassede løsninger innenfor faste rammer, med krav om å informere brukerne om de valg som er gjort og de krav som er stilt.

[5] I forbindelse med tiltak for å fremme bruk av elektroniske tjenester og for å koordinere forvaltningens bruk av sikkerhetstjenester, er forvaltningsorganets valgfrihet begrenset hvis PKI-baserte sikkerhetstjenester eller –produkter skal benyttes. Alle statlige etater som skal ta i bruk tjenester for autentisering og elektronisk signatur er nå pålagt å benytte *"Kravspesifikasjon for PKI i offentlig sektor"* som er en forvaltningsstandard. I kravspesifikasjonen er det definert tre ulike sertifikattyper med tilhørende krav til sikkerhetstjenester. Sertifikattypene Person Høyt, Person Standard og Virksomhetssertifikater, dekker nivå 4 (Person Høyt) og nivå 3 i "*Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor*" Dette forenkler vurderingen for forvaltningsorganene. De samme løsninger anbefales for kommunene. Bruk av elektronisk identitetsbevis (eID) og elektronisk signatur i offentlig sektor er nå samordnet gjennom ID-porten som forvaltes av Direktoratet for forvaltning og IKT (Difi). Det fremgår av Digitaliseringsrundskrivet (H-7/2014), punkt 1.2 *Bruk nasjonale felleskomponenter* at: «Virksomheten skal ta i bruk ID-porten for digitale tjenester som krever innlogging og autentisering.» Slike føringer er gjenstand for politiske beslutninger og kan endres over tid. Digitaliseringsrundskrivet oppdateres jevnlig. Se også eForvaltningsforskriften § 36 med kommentarer.

[6] Se om Regjeringens digitaliseringsprogram i *«Digital agenda for Norge»* og om konkrete føringer i Digitaliseringsrundskrivet (H-7/2014). Slike føringer er gjenstand for politiske beslutninger og kan endres over tid. Digitaliseringsrundskrivet oppdateres jevnlig. Se også brev fra Kommunal- og moderniseringsdepartementet 10. februar 2014 *«Digital kommunikasjon hovedregel - Viktig informasjon om endringer i forvaltningsloven og eForvaltningsforskriften»* med vedlegg.

Forskriften gjelder for elektronisk kommunikasjon[7] med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen[8] når ikke annet er bestemt i lov eller i medhold av lov.

Denne forskrift gir ikke grunnlag for å gjøre unntak fra de alminnelige reglene om forsvarlig saksbehandling i forvaltningsloven[9].

§ 2 *Begreper* [10]

De begreper som er definert i lov om elektronisk signatur § 3 og i forvaltningsloven § 2 benyttes på samme måte i forskriften her.

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

§ 3 *Bruk av elektronisk kommunikasjon ved henvendelser til et forvaltningsorgan*[11]

Alle[12] som henvender seg til et forvaltningsorgan[13] kan benytte elektronisk kommunikasjon, dersom forvaltningsorganet har lagt til rette for det, det skjer på den anviste måten og ved bruk av den elektroniske adressen, som forvaltningsorganet har anvist for den aktuelle type henvendelse.[14]

---

[7] Se § 3første ledd, bokstav c).

[8] eForvaltningsforskriften gjelder både publikums/borgernes kommunikasjon med forvaltningen og kommunikasjon mellom forvaltningsorganer. Med «forvaltningen» menes ethvert organ for stat eller kommune samt andre virksomheter som er omfattet av forvaltningslovens virkeområde, se forvaltningsloven § 1.

[9] Lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven).

[10] Forskriften benytter de samme begrepene som er brukt i de lovene som forskriften er forankret i. Dette gjelder bl.a. begreper som elektronisk signatur, sertifikat mv. Se mer om disse begrepene i lov av 15. juni 2001 nr. 81 om elektronisk signatur ("esignaturloven") § 3 og i forarbeidene til esignaturloven, samt i forvaltningsloven § 2.

[11] Se Veilederen del 1, kapittel 3.1 *Fleksibilitet og behovstilpassede løsninger* og kapittel 3.2 *Valg av form og fremgangsmåte*.

[12] Bestemmelsen retter seg mot alle som vil kommunisere elektronisk med forvaltningen. Begrepet «alle» benyttes på samme måte som i lov av 19. mai 2006 nr. 16 om rett til innsyn i dokument i offentleg verksemd (offentleglova) § 3.

[13] Se forvaltningsloven § 1.

[14] Man har altså rett til å benytte elektronisk kommunikasjon når forvaltningsorganet har lagt til rette for det, og man gjør det slik forvaltningsorganet krever. Hvis det er opprettet egen nettside eller lenke for et bestemt formål må denne benyttes. Det er for eksempel opprettet en egen tjeneste for søknad om nytt skattekort. Slik søknad kan da ikke sendes til Skattedirektoratets generelle elektroniske adresse. Selv om forvaltningsorganet har lagt til rette for elektronisk kommunikasjon vil man alltid kunne henvende seg til organet muntlig eller ved ordinært brev, med mindre forvaltningsorganet kan påvise et særskilt grunnlag for å *kreve* at det benyttes elektronisk kommunikasjon. Se også Veilederen del 1, kapittel 3.2 *Valg av form og fremgangsmåte,* siste avsnitt.

(a) Med den anviste måten menes for eksempel bruk av spesielle skjema, bruk av en bestemt prosedyre eller lignende.[15]

(b) Med *elektronisk adresse* menes for eksempel en adresse til et nettsted, en e-postadresse, et nummer til en SMS-tjeneste eller lignende.[16]

(c) Med *elektronisk kommunikasjon* menes bruk av for eksempel internett, eller liknende kommunikasjonssystem, bruk av SMS og talestyrte eller andre automatiske telefontjenester. Bruk av taletelefon eller annen muntlig kommunikasjon er ikke omfattet.[17]

Hvis det ikke er anvist noen egen elektronisk adresse, og det heller ikke er stilt noen særskilte krav til fremgangsmåte, for den type henvendelse som er aktuell, kan den som vil henvende seg til forvaltningsorganet, bruke forvaltningsorganets generelle elektroniske adresse.[18]

Når det benyttes elektronisk kommunikasjon ved henvendelse til et forvaltningsorgan, skal henvendelsen ikke rettes direkte til en enkeltperson[19],[20] med mindre forvaltningsorganet har lagt til rette for det,[21] eller det er avtalt i det enkelte tilfelle.[22]

---

[15] Det kan for eksempel være krav om bruk av et særskilt web-skjema eller at man som bruker ledes gjennom en interaktiv prosess der man avgir opplysninger, gjør valg mv. og til slutt godkjenner resultatet av prosessen, for eksempel personlig selvangivelse på web.

[16] Eksempler på dette kan være en URI (URL) der en benytter web-skjema ved henvendelse til organet for å håndtere den økende elektroniske trafikken. Dette vil gi enklere og ryddigere håndtering, samt større muligheter til maskinell behandling av henvendelser. Se for eksempel enkelt kontaktskjema fra Oslo kommune. Ellers vil den generelle elektroniske adressen ofte være organets e-postadresse (eks. postmottak@difi.no).

[17] Dette innebærer at for eksempel en kontofontjeneste vil være omfattet. Tradisjonell telefax omfattes ikke av forskriften.

[18] I tillegg til å opprette særskilte nettbaserte tjenester for bestemte saksområder eller brukere, bør forvaltningsorganet ha en generell side som gir publikum anledning til å ta kontakt med forvaltningsorganet. Henvendelser via denne nettsiden bør sendes til arkivtjenesten. Alle forvaltningsorganer som åpner for bruk av e-post, har plikt til å ha en generell elektronisk adresse. Dette følger av arkivforskriften § 3-2 annet ledd: "Organ som nyttar e-post, skal ha eit sentralt e-postmottak for post til organet. E-post til det sentrale postmottaket skal opnast av arkivtenesta." En slik e-postadresse kan for eksempel være postmottak@oslo.kommune.no. Denne adressen kan brukes dersom publikum er usikre på hvilken måte henvendelser skal fremsettes eller til hvem de skal sendes.

[19] Henvendelser av privat eller personlig karakter som sendes direkte til saksbehandler reguleres ikke av denne bestemmelsen eller forskriften for øvrig.

[20] Det er klare ulemper ved å tillate at henvendelser sendes direkte til saksbehandler. For det første skaper det store utfordringer for arkiv og journalføring. Hvis for eksempel journalføringen svikter som følge av at henvendelsen er sendt direkte til saksbehandler, så glipper også grunnlaget for gjennomføringen av innsynsretten. Dessuten er det vanligvis ikke mulig for andre å lese e-post som sendes direkte til en person, se bl.a. personopplysningsforskriften § 9-2 som begrenser arbeidsgivers rett til innsyn i ansattes e-post. Dermed vil man i mange tilfelle ikke kunne behandle henvendelsen før mottakeren er tilbake på jobb. Hvis saksbehandler har sluttet eller har et lengre fravær, kan det føre til store forsinkelser i saksbehandlingen og i verste fall til at henvendelsen aldri blir lest. E-post kan også sendes til feil forvaltningsorgan. Kunnskapen om håndtering av feilsendte meldinger og hvilken informasjon avsender har krav på og behov for, kan være mindre hos den enkelte saksbehandler enn hos arkivet som håndterer postmottaket. Direkte adressering bør derfor være forbeholdt tilfeller eller typer av saksbehandling der det enten er særskilt behov for det eller det i alle fall er på det rene at det ikke har spesielle ulemper.

Forvaltningsorganet kan bestemme at henvendelser fra andre forvaltningsorganer kan sendes direkte til enkeltpersoner i forvaltningsorganet.[23]

Forvaltningsorganet bør legge til rette for at elektronisk kommunikasjon med forvaltningsorganet er brukervennlig og tilgjengelig for alle.[24]

§ 4 *Krav til bruk av sikkerhetstjenester og –produkter mv. ved henvendelser til et forvaltningsorgan*[25]

Enhver[26] som henvender seg til et forvaltningsorgan ved bruk av elektronisk kommunikasjon i henhold til § 3, kan gjøre det uten bruk av sikkerhetstjenester eller -produkter, med mindre bruk av slike sikkerhetstjenester eller -produkter er nødvendig for å oppfylle krav fastsatt i henhold til annet og tredje ledd nedenfor eller følger av § 5, eller av krav fastsatt i annen lov eller i medhold av lov.[27]

(a) Med *sikkerhetstjenester og -produkter* menes løsninger for å oppnå bl.a. bekreftelse av partenes identitet eller fullmakter (autentisering), at data ikke utilsiktet eller urettmessig endres (integritet), beskyttelse av informasjon mot innsyn fra uvedkommende (konfidensialitet), og at det er mulig å dokumentere henvendelser og

---

[21] Det er altså en betingelse for å sende epost direkte til en saksbehandler at forvaltningsorganet har lagt til rette for det. Et eksempel på at det er lagt til rette for direkte henvendelser til saksbehandler kan være når forvaltningsorganet benytter elektronisk saksbehandling, arkiv- og journalsystem og det er lagt til rette for at saksbehandler selv kan foreta registrering av inngående post. Dersom saksbehandler ikke kan foreta journalføring selv, må organet ha rutiner som sikrer at henvendelsen blir videresendt til arkivtjenesten. Dette følger også av arkivforskriften § 3-1 annet ledd, jf. arkivforskriften § 3-2 første ledd. Dette skal også være beskrevet i organets sikkerhetsstrategi, jf. § 15 i eforvaltningsforskriften.

[22] Det åpnes for at saksbehandler i enkelttilfeller kan åpne for direkte kommunikasjon selv om forvaltningsorganets rutiner generelt ikke er tilrettelagt for dette. Saksbehandler har da ansvaret for at organets interne rutiner for håndtering av ekstern kommunikasjon følges. Forvaltningsorganet bør ha interne rutiner nedfelt i organets sikkerhetsstrategi jf. § 15, for hvordan saksbehandlere skal håndtere direkte elektronisk kommunikasjon.

[23] Dette forutsetter naturligvis at forvaltningsorganene har rutiner for journalføring av epost. Det er også grunn til å anta at forvaltningsorganene har bedre innsikt i hvem som er rette adressat, og i den aktuelle prosessen, enn en utenforstående bruker av forvaltningens tjenester.

[24] I dette ligger bl.a. en påminnelse om at løsninger for elektronisk kommunikasjon bør være lette å forstå og anvende og at de også bør være tilgjengelige for personer med nedsatt funksjonsevne. Krav til universell utforming følger nå også av lov av 21. juni 2013 nr. 61 om forbud mot diskriminering på grunn av nedsatt funksjonsevne (diskriminerings- og tilgjengelighetsloven) § 13 og av forskrift 21. juni 2013 nr. 732 om universell utforming av informasjons- og kommunikasjonsteknologiske (IKT)-løsninger. Tjenestene bør også være tilgjengelige fra ulike tekniske plattformer, for eksempel fra mindre bærbare enheter.

[25] Se Veilederen del 1, kapittel 3.4 *Krav til bruk av sikkerhetstjenester og –produkter*.

[26] Bestemmelsen retter seg mot alle som vil kommunisere elektronisk med forvaltningen. Begrepet benyttes på samme måte som begrepet «alle» i offentleglova § 3.

[27] Utgangspunktet er at henvendelser til et forvaltningsorgan kan skje uten bruk av sikkerhetstjenester og produkter. Forvaltningsorganet kan ikke sette krav om bruk av slike bare ”for sikkerhets skyld”. De krav som organet setter til kommunikasjonen skal reflektere relevante og legitime behov som fremkommer i organets risikovurdering, internkontrolldokumentasjon og sikkerhetsstrategi, jf. § 15. Sikkerhetsstrategien skal også omfatte relevante krav som er stilt i annet regelverk.

aktiviteter og hvem som har sendt eller utført dem (ikke-benekting),[28] og andre løsninger, i henhold til forvaltningsorganets sikkerhetsstrategi, jf. § 15. Slike løsninger kan for eksempel være basert på bruk av elektronisk signatur og kryptering.[29]

(b) Med *elektronisk signatur* menes løsninger som definert i lov om elektronisk signatur § 3. Med *kryptering* menes omforming av data slik at de ikke er rekonstruerbare for uvedkommende. Krypterte data skal kunne rekonstrueres ved *dekryptering*.

(c) Med *krypteringsnøkkel* og *dekrypteringsnøkkel* menes data som benyttes for henholdsvis kryptering og dekryptering.[30]

Forvaltningsorganet kan i det enkelte tilfelle[31] be om opplysninger som bekrefter avsenders identitet eller fullmakter, eller stille krav om at bestemte sikkerhetstjenester og -produkter skal tas i bruk, dersom dette er av betydning for håndtering av henvendelsen.

Forvaltningsorganet kan bestemme at krav som nevnt i annet ledd ovenfor skal gjelde generelt for nærmere angitte typer av henvendelser. Kravene skal være basert på forvaltningsorganets sikkerhetsstrategi, jf. § 15.[32]

---

[28] Begrepet ikke-benekting benyttes vanligvis bare i sammenheng med elektronisk signaturer, og da i betydningen at det er mulig å etablere en forholdsvis høy grad av sannsynlighet for at en person eller virksomhet har sendt en melding med et bestemt innhold eller utført en nærmere bestemt handling. I forskriftene her, er siktemålet å oppnå en tilfredsstillende grad av sannsynlighet som nevnt over, f.eks. gjennom autentisering og loggføring. Hvor høy sannsynligheten må være vil variere mellom ulike anvendelsesområder, basert på en risikovurdering.

[29] I henhold til efvf § 4, kan forvaltningsorganet selv velge hvilke sikkerhetstjenester og -produkter de skal benytte. Valg av løsninger skal være forankret i forvaltningsorganets sikkerhetsstrategi, jf. § 15. I forbindelse med tiltak for å fremme bruk av elektroniske tjenester og for å koordinere forvaltningens bruk av sikkerhetstjenester, er forvaltningsorganets valgfrihet likevel begrenset. Det fremgår av Digitaliseringsrundskrivet (H-7/2014), punkt 1.2 *Bruk av nasjonale felleskomponenter* at: «Virksomheten skal ta i bruk ID-porten for digitale tjenester som krever innlogging og autentisering.» Slike føringer er gjenstand for politiske beslutninger og kan endres over tid. Digitaliseringsrundskrivet oppdateres jevnlig. For øvrig skal alle statlige etater som skal ta i bruk tjenester for autentisering og elektronisk signatur benytte "Kravspesifikasjon for PKI i offentlig sektor" som er en forvaltningsstandard. De samme løsninger anbefales for kommunene. Se brev fra Moderniseringsdepartementet til samtlige statsetater 7. juni 2005 og brev til samtlige statsetater fra Fornyings- og administrasjonsdepartementet 20. september 2006.

Det er etablert en ordning for selvdeklarering av sertifikattjenester som oppfyller kravene i "*Kravspesifikasjon for PKI i offentlig sektor*", jf. forskrift 21. november 2005 nr. 1296. Selvdeklarasjonen skal sendes til Post- og teletilsynet som er tilsynsorgan. Tilsynet publiserer en liste over tilsendte selvdeklarasjoner. Sertifikattjenester på denne listen ansees å tilfredstille kravene i kravspesifikasjonen. Selvdeklarasjonsordningen er forankret i eSignaturloven (esl.) § 16a. Denne bestemmelsen danner rammen for etablering av frivillige sertifiserings-, godkjennings- eller selvdeklareringsordninger. Slike ordninger gjør det enklere for brukerne å orientere seg blant de sikkerhetstjenester og –produkter som er tilgjengelige i markedet, og kan bidra til å etablere tillit til deres pålitelighet.

[30] Begrepene «*krypteringsnøkkel*» og «*dekrypteringsnøkkel*» er teknologiuavhengige begrep som brukes generelt innenfor sikring av elektronisk kommunikasjon. Formuleringene er ikke identiske (men i harmoni) med definisjoner i forskrift om informasjonssikkerhet (jf. sikkerhetsloven), fordi definisjonene der er mer omfattende enn det er behov for i denne forskriften. Begrepene er ikke brukt i lov om elektronisk signatur fordi loven ikke omhandler kryptering.

[31] Formålet med bestemmelsen er å unngå at forvaltningsorganene stiller generelle krav om bruk av sikkerhetstjenester eller -produkter "for sikkerhets skyld" hvis det bare er i unntakstilfellene det er behov for dem.

Forvaltningsorganet skal gjøre tilgjengelig sikkerhetstjenester og -produkter som oppfyller de krav forvaltningsorganet har stilt i henhold til annet og tredje ledd ovenfor eller anvise hvilke løsninger som ellers kan benyttes.[33] Det samme gjelder for sikkerhetstjenester og -produkter som er nødvendig for å oppfylle kravene i § 5.

§ 5 *Formidling av taushetsbelagte opplysninger og personopplysninger til forvaltningen*[34]

Når et forvaltningsorgan legger til rette for bruk av elektronisk kommunikasjon for mottak av opplysninger som på forvaltningens hånd kan være underlagt taushetsplikt, eller som kan være underlagt krav til sikring etter reglene om behandling av personopplysninger eller tilsvarende regler, skal risiko for uberettiget innsyn i opplysningene være forebygget på tilfredsstillende måte.[35]

Forvaltningsorgan som legger til rette for å motta opplysninger som nevnt i første ledd, skal på hensiktsmessig måte informere[36] om eventuelle risikoer ved elektronisk overføring av slike opplysninger og om hva som er rette elektroniske adresse.[37]

Forvaltningsorganet skal opplyse generelt[38] om hvordan taushetsbelagte opplysninger og personopplysninger sikres under behandling i forvaltningsorganet.

Ved kryptering av melding til forvaltningen skal forvaltningsorganets krypteringsnøkkel eller krypteringsnøkkel til en nærmere angitt enhet ved forvaltningsorganet benyttes[39]. Hvis forvaltningsorganet benytter ekstern databehandler i henhold til personopplysningsloven § 15, kan databehandlerens krypteringsnøkkel benyttes hvis det godtgjøres, eller er alminnelig kjent, at databehandleren opptrer på vegne av forvaltningsorganet.[40]

---

[32] Forvaltningsorganets krav til bruk av sikkerhetsteknikker og –produkter skal være gjennomtenkte og grunnet i rettslige krav eller et reelt praktisk behov. Dette er søkt tydeliggjort i tredje ledd ved å henvise til bestemmelsen i § 15, om internkontroll, sikkerhetsmål og sikkerhetsstrategi.

[33] Forvaltningsorganet skal konkret angi hvorledes de krav de selv har stilt kan oppfylles. Dette kan gjøres ved enten selv å tilby relevante tjenester og produkter eller å navngi tjenesteytere og produkter som tilfredsstiller kravene.

[34] Se Veilederen del 1, kapittel 3.5 *Formidling av taushetsbelagte opplysninger og personopplysninger til forvaltningen.*

[35] Forvaltningen har en plikt til å sikre informasjon i henhold til regler om bl.a. taushetsplikt og personvern. Når forvaltningen inviterer publikum til å kommunisere elektronisk, må det også informeres om hvordan publikum skal gå frem for å gjøre dette på en trygg måte.

[36] Det er nødvendig å presisere forvaltningens veiledningsplikt på et område som for mange er nytt og ukjent. En "hensiktsmessig måte" å informere på kan være å legge informasjon om risikoer og nødvendige tiltak på hjemmesiden som publikum må besøke for å kunne kommunisere med organet. Det skal også informeres om hva som er korrekt elektroniske adresse til forvaltningsorganet.

[37] Se § 3 første ledd, bokstav b.

[38] Ordet "*generelt*" er benyttet for å presisere at forvaltningsorganets opplysningsplikt ikke er så omfattende at det kan blottstille og derved true sikkerhetssystemene til forvaltningsorganet.

[39] Se Veilederen del 1, kapittel 3.5 og kapittel 4.5. Det er vanligvis forvaltningsorganets krypteringsnøkkel som skal benyttes; i praksis i form av et virksomhetssertifikat (som kan være et SSL-sertifikat).

[40] Skattetaten, Statens lånekasse og flere andre benytter f eks Altinn portalen, der det enkelte rettssubjekt registrerer sine opplysninger. Felles portaler som Altinn er ikke en del av det enkelte forvaltningsorganet,

Kryptering med en enkeltpersons krypteringsnøkkel kan bare benyttes dersom forvaltningsorganet har lagt spesielt til rette for det.

§ 6 *Bekreftelse på at en henvendelse er mottatt* [41]

Et forvaltningsorgan som mottar henvendelser i elektronisk form skal gi bekreftelse[42] til avsender om at en henvendelse er mottatt.

Bekreftelse bør gis straks henvendelsen er mottatt. Den bør inneholde et referansenummer eller lignende og angi på hvilket tidspunkt henvendelsen ble mottatt.[43]

Forvaltningsorganet kan unnlate å sende bekreftelse, hvis henvendelsen er av en slik art at den ikke utløser saksbehandling, eller mottaket fremgår på annen betryggende måte,[44] og ved bruk av automatiserte systemer der henvendelsen straks blir besvart. Forvaltningsorganet kan også inngå avtale med næringsdrivende og med andre forvaltningsorganer om ikke å sende egen bekreftelse etter denne bestemmelsen i forbindelse med rutinemessig eller periodisk rapportering.[45]

---

men en teknisk løsning, utviklet og forvaltet av Brønnøysundregistrene, som utfører nærmere bestemte oppgaver for et eller flere andre forvaltningsorgan. Etter alminnelig sikkerhetsoppfatning, skal hjelperen benytte egne krypteringsnøkler og ikke forvaltningsorganets nøkler. Dermed mister man den direkte knytningen mellom forvaltningsorganet og den enkelte avgiver av informasjonen. Det er derfor oppstilt et krav om å bekrefte fullmaktforholdet mellom forvaltningsorganet og databehandleren (portalen). Dette kan skje med både tekniske og organisatoriske løsninger. Se Veilederen del 1, kapittel 4.5 *Kryptering av meldinger til forvaltningsorganet*.

[41] Se Veilederen del 1, kapittel 3.6 *Tilbakemeldinger på henvendelser som forvaltningsorganet mottar.*

[42] Bestemmelsen oppstiller et krav om kvittering på at en henvendelse er mottatt ved bruk av elektronisk kommunikasjon av forvaltningsorganet. Dersom forvaltningsorganet tilbyr Web-baserte søknadsskjemaer, kan IT-systemet som mottar en søknad kunne definere dette som et saksdokument og oppgi et referansenummer i dialogen med avsenderen av opplysningene. Ved bruk av e-post kan det gis automatisk bekreftelse på at en henvendelse er mottatt, men automatiske løsninger klarer ikke å skille mellom henvendelser som utløser saksbehandling og henvendelser som ikke gjør det, for eksempel ”spam”, jf. bestemmelsens tredje ledd. Det enkleste vil ofte være å legge opp til bekreftelse på alle mottatte henvendelser.

[43] Når henvendelser sendes i strukturert form via web-baserte skjemaer vil det være mulig å opprette saksnummer automatisk. Referansenummeret som oppgis i bekreftelsen kan da være det samme som saksnummeret. I tillegg skal bekreftelsen angi på hvilket tidspunkt henvendelsen er mottatt. Dette kan ha betydning bl.a. i forbindelse med avbrytelse eller beregning av frister mv. Dersom avsender bruker e-post, må forvaltningsorganet først vurdere om en henvendelse skal journalføres og få et saksnummer. Siden denne manuelle behandlingen kan ta noe tid, bør det opprettes et eget referansenummer slik at bekreftelse kan gis straks henvendelsen er mottatt.

[44] F eks hvis brukeren får tilbakemelding på skjermen om at en overføring er vellykket.

[45] Det kreves her en særskilt avtale med organet. En forutsetter her at kommunikasjonen med forvaltningsorganet er betryggende løst på andre måter. Generelt bør en være forsiktig med å benytte unntaksregelen.

§ 7 *Henvendelser som ikke tilfredsstiller aktuelle krav*

Henvender noen seg til urette myndighet eller benytter uriktig elektronisk adresse[46] ved en henvendelse til et forvaltningsorgan, skal det forvaltningsorgan som mottar henvendelsen gi avsender beskjed om feilen og om mulig vise vedkommende til rett organ og rett elektronisk adresse, jf. forvaltningslovens § 11.

Er en henvendelse avgitt i en annen form eller på en annen måte enn det som er angitt i eller i medhold av forskriften her, skal organet gi avsenderen beskjed om dette dersom feilen har betydning for behandling av saken eller det av andre grunner finnes nødvendig. Organet bør samtidig gi frist til å rette opp feilen og gi veiledning om hvordan dette kan gjøres. [47]

Forvaltningsorganet skal registrere tidspunkt for når det er sendt varsel etter første og annet ledd ovenfor, og til hvem varselet ble sendt. Dersom feilen er av en slik art at det ikke er mulig å identifisere avsender, og varsel ikke kan sendes, skal det registreres opplysning om dette.

§ 8 *Bruk av elektronisk kommunikasjon ved meddelelser fra et forvaltningsorgan, herunder underretning om enkeltvedtak m.v.*[48]

Et forvaltningsorgan kan benytte elektronisk kommunikasjon når det henvender seg til andre.[49]

Innholdet i enkeltvedtaket skal gjøres tilgjengelig i egnet informasjonssystem.[50] Dersom parten ber om det, det ikke er hensiktsmessig å kommunisere digitalt med parten via

---

[46] Et forvaltningsorgan kan ha flere elektroniske adresser, for eksempel inndelt geografisk, etter saksområder eller avdelinger. Benytter avsender feil adresse, skal det gis veiledning om hva som er korrekt adresse for den aktuelle type henvendelse. I tillegg til veiledning bør det også internt i forvaltningsorganet være rutiner for å videresende slike feilsendte henvendelser til rett instans. Avsender bør i så fall få beskjed om at henvendelsen er videresendt.

[47] Dersom en henvendelse til et forvaltningsorgan inneholder feil, misforståelser, unøyaktigheter eller andre mangler som avsenderen bør rette, skal organet om nødvendig gi beskjed om dette. Et eksempel på at henvendelsen har en feil som er av betydning for saksbehandlingen, er at en søknad mangler nødvendige opplysninger. Det kan også foreligge feil som kan være av mindre betydning, for eksempel hvis feilen ikke har betydning for saksbehandlingen og andre forhold ikke taler mot det, eksempelvis fordi forvaltningsorganet sitter inne med andre opplysninger som bekrefter de aktuelle forhold.
Dersom en søknad ikke er undertegnet i de tilfellene dette er et krav eller at signaturen av tekniske grunner ikke kan verifiseres, kan forvaltningsorganet likevel være forpliktet til å behandle søknaden. Uansett skal avsender få veiledning og en rimelig frist til å rette feilen.

[48] Se Veilederen del 1, kapittel 3.7 *Underretning om enkeltvedtak mv*.

[49] Bestemmelsen slår fast hovedregelen om at forvaltningen kan benytte elektronisk kommunikasjon når den henvender seg til andre. Se også forvaltningsloven § 15a første ledd.

[50] I vurderingen av hva som er et «egnet informasjonssystem» må det bl.a. sees hen til at krav til varsling, forebygging av risiko for uberettiget innsyn, tidspunktet for når parten skaffer seg tilgang til vedtak og mekanismer for autentisering skal ivaretas i løsningen. Eksempler på egnede informasjonssystemer kan være tjenester hos den enkelte virksomhet (Lånekassen, Statens pensjonskasse og lignende), Altinn eller Digital postkasse til innbyggere. For å få tilgang til vedtaket, må parten gå frem slik det er bestemt i henhold til tredje og fjerde ledd i bestemmelsen.

egnet informasjonssystem, det er forsvarlig og annet regelverk ikke er til hinder for dette, kan vedtaket likevel[51] sendes til en elektronisk adresse parten oppgir.[52]

Forvaltningsorganet skal sørge for at varsel[53] om at enkeltvedtak er fattet[54] blir sendt parten, og om hvor og hvordan vedkommende kan skaffe seg kunnskap om innholdet. For privatpersoner eller enheter som ikke er registrert i Enhetsregisteret, skal den varslingsadresse som er registrert i register over digital kontaktinformasjon og

---

Bestemmelsen selv gir ingen føringer når det gjelder *hvilke informasjonssystemer* forvaltningen kan eller skal bruke til hva (utover kravene til egnethet). Slike føringer følger imidlertid av for eksempel Digitaliseringsrundskrivet (H-7/2014). Slike føringer er gjenstand for politiske beslutninger og kan endres over tid. Digitaliseringsrundskrivet oppdateres jevnlig. Et "egnet informasjonssystem" kan også gi mulighet for at forvaltningen står for oppbevaring av vedtakene i elektronisk form på vegne av publikum. Da vil vedtaket være tilgjengelig, uavhengig hvor brukeren befinner seg. Brukeren kan skrive ut eller lagre vedtaket på sin PC etter behov, men vil fortsatt ha tilgang til en verifiserbar elektronisk versjon hos forvaltningsorganet.

[51] Bruk av ordet «likevel» i annet punktum indikerer at annet punktum er et unntak fra hovedregelen i første punktum.

[52] Bruk av e-post til formidling av enkeltvedtak skal kun skje dersom parten a) ber om det, b) det ikke er hensiktsmessig å kommunisere digitalt med parten via egnet informasjonssystem, c) det er forsvarlig, og d) annet regelverk ikke er til hinder for dette. Det dreier seg altså om fire kumulative vilkår (alle vilkårene må være oppfylt). At det er presisert at det ikke skal være hensiktsmessig å kommunisere digitalt med parten via egnet informasjonssystem, betyr at bruk av egnet informasjonssystem skal vurderes før ordinær e-post benyttes. Hensiktsmessighetsvurderingen foretas av forvaltningsorganet som avsender. Ansvaret for å vurdere om det er *forsvarlig* å benytte ordinær e-post som kanal for formidling av vedtaket ligger også i det enkelte tilfellet til forvaltningsorganet som avsender. Forvaltningsorganet må her vurdere om hensynene bak bestemmelsen kan oppfylles uten at det som ellers regnes som et "egnet informasjonssystem" benyttes. Ordinær e-post vil som utgangspunkt ikke være egnet som kanal for formidling av vedtaket som inneholder taushetsbelagte opplysninger. Krav til informasjonssikkerhet, for eksempel krav fastsatt i personopplysningsforskriften kapittel 2, vil være til hinder for dette. Dersom parten ønsker bruk av en forsendelsesmåte som forvaltningsorganet ellers ikke ville kunne benytte, vil det påhvile forvaltningen et særlig ansvar for å sikre at situasjonen er slik at det likevel fremstår som forsvarlig og at parten har forstått og akseptert restrisikoen, jf. den tilsvarende veiledningsplikten i § 5 annet ledd for kommunikasjon til organet. I utgangspunktet skal det sendes varsel etter annet ledd også i disse tilfellene, men har vil det nok ofte være slik at varslingsadressen er sammenfallende med den adressen parten har bedt om å få vedtaket sendt til. Departementet bemerker i motivene til endringen i § 8 tredje ledd (på s. 11) at: "Dersom vedtaket er sendt via ordinær e-post, anses varslingen etter tredje ledd å være foretatt ved at vedtaket sendes e-postadressen." Forvaltningsorganet må ta dette med i sin forsvarlighetsvurdering.

[53] Underretning om enkeltvedtak skjer ved at det sendes et varsel om at vedtaket er truffet med en beskrivelse av hvor vedtaket kan hentes, for eksempel adresse til en nettside. Dette varselet kan sendes som ordinær e-post eller via SMS forutsatt at kravene i blant annet fjerde ledd kan ivaretas.

Kravet til varsling er en videreføring av gjeldende rett. Bestemmelsen krever at digitale kontaktopplysninger som er registrert i register over digital kontaktinformasjon og reservasjon brukes til varsling av privatpersoner og enheter som ikke er registrert i Enhetsregisteret.

[54] Kravet til varsling gjelder enkeltvedtak, forhåndsvarsler, andre meldinger som har betydning for mottakerens rettsstilling eller for behandlingen av saken, og andre meldinger som det av andre grunner er av særlig betydning å sikre at vedkommende mottar, se § 8 siste ledd. For andre meldinger stiller ikke forskriftene krav om at det sendes varsel, men forvaltningsorganet bør vurdere om det kan være hensiktsmessig å varsle av andre grunner, f.eks. hvis mottakeren ikke har noen spesiell grunn til å vente at henvendelsen kommer, men det er i forvaltningsorganets interesse at mottakeren gjør seg kjent med den.

reservasjon benyttes.[55] [56] For enheter som er registrert i Enhetsregisteret skal en oppdatert elektronisk adresse som enheten har oppgitt benyttes for å sende varsel.[57]

Forvaltningsorganet skal forebygge risiko for uberettiget innsyn i enkeltvedtak på en tilfredsstillende måte.[58]

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.[59] 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 en gang til i samsvar med tredje ledd.[60] Første og annet punktum gjelder ikke dersom vedtaket er sendt en elektronisk adresse mottaker oppgir jf. annet ledd annet punktum.[61]

---

[55] Se også merknaden til overgangsreglene i § 37. En konsekvens av plikten til å bruke varslingsadressene fra register over digital kontaktinformasjon og reservasjon er at de forvaltningsorganer som ikke er koblet mot registeret innen 1. januar 2016, heller ikke kan kommunisere blant annet enkeltvedtak digitalt til privatpersoner og enheter som ikke er registrert i Enhetsregisteret.

[56] Dersom vedtak er sendt via ordinær e-post i henhold til unntaksregelen i annet ledd, anses varslingen etter tredje ledd å være foretatt ved at vedtaket sendes e-postadressen.

[57] For enheter som er registrert i enhetsregisteret skal varslingen skje til den adressen enheten har oppgitt. Dette kan eksempelvis være en adresse som er oppgitt i forbindelse med den aktuelle saksbehandlingen/vedtaket. Bestemmelsen åpner også for bruk av adresser som registreres i et digitalt kontaktregister for virksomheter.

[58] Enkeltvedtak vil i mange tilfeller inneholde opplysninger som gjør at de er omfattet av regler om taushetsplikt. Det er først og fremst partene og deres representanter som skal ha tilgang til enkeltvedtaket, jf. fvl. § 18 og § 19, og forvaltningsorganet må sikre at de har kontroll med at ikke uvedkommende får tilgang. I forbindelse med tiltak for å fremme bruk av elektroniske tjenester og for å koordinere forvaltningens bruk av sikkerhetstjenester, ble det bestemt at alle statlige etater som skulle ta i bruk tjenester for autentisering og elektronisk signatur skal benytte "*Kravspesifikasjon for PKI i offentlig sektor*". Løsningen er også anbefalt for kommunene. Difi har etablert ID-porten som en fellesoffentlig løsning for verifisering av elektronisk identitetsbevis som tilfredsstiller kravene i *Kravspesifikasjon for PKI i offentlig sektor*, som er selvdeklarert i henhold til forskrift 21. november 2005 nr. 1296 og som er utstedt av sertifikatutstedere som Difi har avtale med, og for elektronisk identitetsbevis som er utstedt av Difi selv (MinID). Det fremgår av Digitaliseringsrundskrivet (H-7/2014), punkt 1.2 *Bruk av nasjonale felleskomponenter* at: «Virksomheten skal ta i bruk ID-porten for digitale tjenester som krever innlogging og autentisering.» Slike føringer er gjenstand for politiske beslutninger og kan endres over tid. Digitaliseringsrundskrivet oppdateres jevnlig.

[59] Registrering av tidspunkt og kontroll med at parten har fått tilgang til enkeltvedtaket kan skje automatisk ved å ha et system som loggfører tidspunkt og opplysninger som identifiserer parten. Det er nødvendig med entydig og sikker identifisering av parten før enkeltvedtaket kan hentes frem fra informasjonssystemet. Kravet til ekstra elektronisk varsel etter annet punktum krever at informasjonssystemet registrerer om mottaker har åpnet meldingen. Henvisningen til tredje ledd innebærer at den digitale kontaktinformasjonen registrert i register over digital kontaktinformasjon og reservasjon skal benyttes også for varsling på nytt dersom enkeltvedtak ikke er åpnet.

[60] Den såkalte "syvdagersregelen" som tidligere fantes i eForvaltningsforskriften ble opphevet med virkning fra 1. januar 2013. Den innebar at dersom et forvaltningsorgan sendte for eksempel et enkeltvedtak til mottaker digitalt, og mottaker ikke åpnet vedtaket innen syv dager, måtte forvaltningsorganet sende enkeltvedtaket på papir til mottaker. Syvdagersregelen ble i sin tid innført for å forhindre at mottaker skulle lide rettstap når enkeltvedtaket ble formidlet til vedkommende ved bruk av elektronisk kommunikasjon.
I motivene til endring av § 8 i februar 2014, skriver departementet:

Det som gjelder enkeltvedtak i annet til femte ledd ovenfor, gjelder tilsvarende for:[62]

a) forhåndsvarsel etter forvaltningsloven § 16,

b) for andre meldinger som har betydning for mottakerens rettsstilling eller for behandlingen av saken, og

c) for meldinger som det av andre grunner er av særlig betydning å sikre at vedkommende mottar.

§ 9 Reservasjon

Privatpersoner og enheter som ikke er registrert i Enhetsregisteret[63] kan reservere seg mot å motta følgende meddelelser elektronisk fra forvaltningen:[64]

a) enkeltvedtak,

«Departementet mener at det bør stilles som krav i forskriften at mottaker varsles ekstra én gang dersom enkeltvedtak ikke er åpnet en uke etter at vedtaket ble mottatt. Det er etter departementets oppfatning viktig å gjøre en innsats for at mottaker ikke lider rettstap. Departementet mener at det ikke er av avgjørende betydning om mottaker oppfatter varselet som «spam» eller lignende. At mottaker får med seg innholdet i enkeltvedtak denne er part i er også i avsenders interesse.

Ordningen innebærer at informasjonssystemene som benyttes følger med på om mottaker åpner meldingene som sendes til denne. Dette vil i stor grad være en teknisk funksjonalitet, og det er derfor som utgangspunkt ikke behov for at enkeltpersoner hos avsendervirksomheten får kunnskap om konkrete vedtak er åpnet eller ikke. Departementet vurderer det dit at i den grad dette kan sies å innebære overvåkning av mottaker, så vil hensynet til å forhindre at mottaker lider rettstap veie tyngre.»

Skulle det vise seg at parten, til tross for dobbelt varsling, likevel ikke blir oppmerksom på vedtaket (eller forhåndsvarselet mv), slik at en frist blir oversittet, må tilfellet håndteres som om parten hadde oversett, eller hevder ikke å ha mottatt, et papirbasert brev, herunder om det kan gis oppreisning for fristoversittelse etter forvaltningsloven § 31. Det skal i den sammenheng legges vekt på om parten kan lastes for å ha oversittet fristen.

[61] Hvis henvendelsen er sendt i henhold til unntaksregelen i annet ledd, annet punktum, til en e-postadresse parten selv har angitt, er det ikke mulig for forvaltningsorganet å vite om meldingen er åpnet, eller på annen måte sikre ekstra varsling. Behovet for ekstra varsling må dessuten antas å være mindre i disse tilfellene, da parten har spesiell foranledning til å være oppmerksom på, og åpne meldingen, i og med at vedkommende har bedt om å få den direkte til en oppgitt e-postadresse.

[62] Bestemmelsen angir virkeområdet for § 8 annet til femte ledd. Bokstavene a) til c) angir virkeområdet til å være enkeltvedtak og andre henvendelser som er viktige for mottaker å få med seg. Opplistingen er ikke endret ved den siste forskriftsendringen.

[63] Bestemmelsen angir hvem som har reservasjonsrett. Reservasjonsretten gjelder for 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.

[64] Bestemmelsen angir også hva reservasjonsretten knytter seg til. Innbygger skal kunne reservere seg mot de tilfeller av elektronisk kommunikasjon som det tidligere var knyttet et samtykkekrav til. Det vil si at det ikke innføres en rett til å reservere seg mot all elektronisk kommunikasjon fra forvaltningen. I så fall ville endringen av regelverket ført til en snevrere adgang til å kommunisere elektronisk enn etter dagens regelverk. Som eksempel på tilfeller der mottaker ikke kan reservere seg mot digital kommunikasjon, nevnes ulike former for servicemeldinger, for eksempel varsel om stenging av vann og lignende.

b) forhåndsvarsel etter forvaltningsloven § 16,

c) andre meldinger som har betydning for vedkommendes rettsstilling eller for behandlingen av saken, og

d) meldinger som det av andre grunner er av særlig betydning å sikre at vedkommende mottar.

Reservasjonen skal registreres i register over digital kontaktinformasjon og reservasjon, jf. kapittel 7.

§ 10 Bruk av fullmektig i forbindelse med elektronisk kommunikasjon med forvaltningen

Når en person opptrer på vegne av en annen i forbindelse med elektronisk kommunikasjon med forvaltningen,[65] skal det fremgå av kommunikasjonen at vedkommende er representert ved fullmektig. Fullmektigen skal opptre i eget navn, og ikke benytte elektronisk identitetsbevis tilhørende den han opptrer på vegne av.[66]

§ 11 *Klage*

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.[67] Det skal også informeres om at parten bør kontrollere at han mottar bekreftelse når klage leveres i elektronisk form.

Klagefristen etter forvaltningsloven § 29 begynner å løpe fra det tidspunktet enkeltvedtaket er gjort tilgjengelig for parten, og varsel om dette er sendt, jf. § 8 tredje ledd.[68]

---

[65] Bestemmelsen regulerer ikke når det er tillatt å bruke fullmektig og når dette ikke er tillatt. Det vil følge av annet regelverk. Av forvaltningsloven § 12 fremgår det at: "Alle henvendelser i en sak kan gjøres ved fullmektig, …" Dersom fullmektig brukes i forbindelse med elektronisk kommunikasjon med forvaltningen, må imidlertid bestemmelsen følges.

[66] Det må fremgå av kommunikasjonen at vedkommende er representert ved fullmektig. Fullmektigen skal opptre i eget navn. Bruk av elektronisk identitetsbevis tilhørende en annen må unngås. Det vil normalt være i strid med bruksvilkårene for elektronisk identitetsbevis. I henhold til forvaltningsloven § 12, skal fullmektig som ikke er advokat fremlegge skriftlig fullmakt. I henhold til forvaltningsloven § 2 bokstav g), kan kravet til skriftlighet også oppfylles ved bruk av elektronisk melding (som legges ved henvendelsen til forvaltningsorganet). En mer praktisk ordning vil være å registrere fullmaktsforholdet i kontaktregisteret når slik funksjonalitet blir tilgjengelig, se eForvaltningsforskriften § 31 nr. 4.

[67] Det er forvaltningsorganet som velger form eller fremgangsmåte, jf. § 3 og § 4.

[68] Bestemmelsen presiserer innholdet i den alminnelige regelen om at fristen begynner å løpe når underretning om vedtaket har kommet frem til parten, se forvaltningsloven § 29. Ved papirbasert post er dette vanligvis når brevet er lagt i partens postkasse. Ved bruk av elektronisk kommunikasjon begynner fristen å løpe når vedtaket er gjort tilgjengelig slik at parten kan skaffe seg tilgang til det, og det er sendt varsel til parten om dette. Fra dette tidspunkt vil parten vanligvis kunne gjøre seg kjent med vedtaket. Hvis

Klage over enkeltvedtak kan fremsettes ved bruk av elektronisk kommunikasjon dersom det forvaltningsorganet som skal motta klagen har lagt til rette for det, jf. § 3 og § 4.[69]

Hvis klager ikke mottar bekreftelse etter § 6, skal klagen sendes på nytt.

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.[70]

§ 12 *Innsyn i opplysninger og dokumenter ved bruk av elektronisk kommunikasjon*

Krav om innsyn i opplysninger eller dokumenter i en sak kan sendes forvaltningsorganet ved bruk av elektronisk kommunikasjon, jf. § 3 og § 4.[71]

Fører forvaltningsorganet elektronisk arkiv, kan det gis tilgang til opplysninger og dokumenter i elektronisk form dersom den som krever innsyn samtykker eller ber om dette.

Innsyn etter annet ledd gis bare når det kan oppnås:

a) tilfredsstillende bekreftelse på at vedkommende har krav på innsyn,[72] og

b) at risiko for uberettiget innsyn i opplysningene eller dokumentene er forebygget på en tilfredsstillende måte, [73] [74] eller når innsyn kan kreves etter offentlighetsloven eller annen lovbestemt allmenn innsynsrett.[75]

---

parten, f.eks. på grunn av en teknisk feil hos vedkommendes bredbåndleverandør e.l., midlertidig er ute av stand til å skaffe seg tilgang til vedtaket, anses det likevel for å ha kommet frem, slik at eventuelle frister begynner å løpe. Bestemmelsen innebærer en endring sammenliknet med tidligere § 8 sjette ledd i eForvaltningsforskriften, der prinsippet var at fristen begynte å løpe når parten faktisk hadde skaffet seg tilgang til vedtaket.

[69] Det er det forvaltningsorganet *"som skal motta klagen"* som må ha lagt til rette for elektronisk kommunikasjon. Dette vil regelmessig være instansen som fattet vedtaket som påklages og som skal forestå saksforberedelsen før oversendelse til klageorganet. Det vises her for øvrig til forvaltningsloven § 32 og § 33.

[70] Forvaltningsloven § 30 første punktum ble endret i juni 2013. Endringen forutsatte en regulering av fristregler knyttet til klage i eForvaltningsforskriften. Bestemmelse med tilsvarende innhold som i tidligere § 30 første ledd andre punktum i forvaltningsloven er tatt inn som ny § 11 femte ledd. Bestemmelsen innebærer ingen endring av gjeldende rett.

[71] Begjæring om innsyn kan sendes elektronisk hvis forvaltningsorganet har lagt til rette for det, jf. § 3 og § 4 .

[72] Hvis opplysningene det begjæres innsyn i er underlagt taushetsplikt eller innsynsretten på annen måte er begrenset, må forvaltningsorganet være tilstrekkelig sikker på at den som spør virkelig har krav på innsyn. Særlig praktisk er partenes innsynsrett etter reglene i forvaltningsloven § 18 flg. Den enkelte har også rett til innsyn i behandling av personopplysninger i henhold til personopplysningsloven § 18. Videre har pasienter innsynsrett i sin journal etter reglene i pasientrettighetsloven § 5-1 og helsepersonelloven § 41. Dersom pasientjournalen føres elektronisk, kan også innsyn gis elektronisk så lenge kravene i bokstav a) og b) er oppfylt.

[73] I tillegg til å sikre at bare rette vedkommende får innsyn, kan det være behov for å sikre at ikke de opplysningene det er tale om kommer på avveie når innsynsretten utøves. Et tiltak vil være å sikre opplysningene under overføring ved hjelp av kryptering, for eksempel ved SSL-sesjon el. Risikoen for videre spredning av elektronisk lagrede dokumenter eller opplysninger er større enn ved papirbasert

Hvis den som krever innsyn i dokumenter som er signert med avansert elektronisk signatur[76] ber om det, skal relevante sertifikater, og øvrige opplysninger som er nødvendige for å få bekreftet[77] signaturen, utleveres sammen med dokumentet. Alternativt kan forvaltningsorganet legge til rette for at verifisering kan skje i forbindelse med at det gis tilgang til dokumentet.

Forvaltningsorganet skal også legge til rette for at den enkelte kan få tilgang til dokumentene i en form som gjør det mulig å dokumentere[78] innholdet overfor tredjepart. Dette kan om nødvendig skje i form av en papirutskrift av dokumentet som er bekreftet av forvaltningsorganet.

§ 13 *Høring*

Høringsbrev til institusjoner og organer som har egen elektronisk adresse kan sendes i elektronisk form. I stedet for utsending av alle sakens dokumenter kan det sendes melding om hvor høringsdokumentene er gjort tilgjengelige.[79]

---

distribusjon. Hvorledes det elektronisk lagrede materialet det kreves innsyn i skal gjøres tilgjengelig, vil være opp til organet å håndtere ut fra hensynet til forsvarlig saksbehandling.

[74] Hvis den som begjærer innsyn er part i saken, og den informasjonen det begjæres innsyn i er av en slik art at det fremstår som forsvarlig å sende det direkte til vedkommendes alminnelige e-postadresse hvis vedkommende ber om det, kunne man tenke seg en løsning tilsvarende den unntaksregel som fremgår av forskriftene § 8 annet ledd, siste setning, for underretning om enkeltvedtak. (Forskriften § 8 annet ledd lyder: «*Dersom parten ber om det, det ikke er hensiktsmessig å kommunisere digitalt med parten via egnet informasjonssystem, det er forsvarlig og annet regelverk ikke er til hinder for dette, kan vedtaket likevel sendes til en elektronisk adresse parten oppgir.*») Dette forutsetter imidlertid som et minimum at forvaltningsorganet kan etablere tilfredsstillende grad av sikkerhet for at den som ber om innsyn, og som oppgir en elektronisk adresse for å få tilsendt materialet, faktisk er den opplysningene gjelder. Hvis vilkårene i § 8 annet ledd, siste setning, bl.a. om forsvarlighet, er oppfylt, kan det hevdes at risiko for uberettiget innsyn i opplysningene er forebygget på tilfredsstillende måte ved sending til en adresse parten (den som har krav på beskyttelse) har oppgitt. Se også note 52 til § 8 annet ledd, siste setning, ovenfor.

[75] Sikkerhetskrav er ikke nødvendig ved innsyn etter "lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)". Derfor har innsyn etter offentleglova blitt plassert som alternativ, jf. "*eller*". I offentleglova § 30, fremgår det at forvaltningsorganet ut fra hensynet til forsvarlig saksbehandling bestemmer hvordan dokumenter skal gjøres kjent, og det fremgår at det kan kreves papirkopi eller elektronisk kopi av dokumentet.

[76] Se lov om elektronisk signatur § 3 nr. 2.

[77] For de dokumenter der det kreves avansert elektronisk signatur vil det kunne være av betydning for den som begjærer innsyn å kunne foreta verifikasjon av avsender, at sertifikatet var gyldig på det tidspunkt dokumentet ble påført signaturen og for å verifisere dokumentets innhold mv. Dette kan det være like viktig å få innsyn i som selve dokumentet.

Opplysninger som er nødvendige for å verifisere en signatur, skal oppbevares sammen med meldingen, jf. § 26. Der dokumentet er konvertert til nytt format og man derved har brutt bindingen mellom dokumentet og signaturen skal en kunne etablere den nødvendige bekreftelse på at knytningen mellom dokumentet og signaturen var i orden ved mottak og at arkivet deretter har sikret dokumentets integritet.

[78] For eksempel i form av en bekreftet utskrift dersom tredjepart ikke kan behandle elektroniske signaturer eller bekreftet med forvaltningsorganets elektroniske signatur dersom meldingen er arkivert i en form som utelukker verifisering med opprinnelig signatur, jf. § 26 annet ledd.

[79] Muligheten for å sende høringsbrev elektronisk forutsetter at mottaker har egen elektronisk adresse. Et annet alternativ er kun å sende melding om at høringsbrev er publisert på forvaltningsorganets hjemmeside, med adresse til den nettsiden hvor høringsbrevet ligger. Se også utredningsinstruksen kapittel 5.

Uttalelser til høringen kan avgis i elektronisk form, jf. § 3 og § 4.[80]

§ 14 *Forvaltningsorganets adgang til å nekte bruk av elektronisk kommunikasjon*[81]

Hvis det er grunn til å anta at noen misbruker adgangen[82] til elektronisk kommunikasjon med forvaltningsorganet, kan vedkommende helt eller delvis nektes videre bruk av slik kommunikasjon med forvaltningsorganet.

Før adgangen til å nekte bruk av elektronisk kommunikasjon med forvaltningsorganet iverksettes, skal forvaltningsorganet sende vedkommende varsel[83] om at det vurderer å nekte videre bruk av slik kommunikasjon og begrunnelsen for dette. Vedkommende skal oppfordres til å uttale seg om grunnlaget for avgjørelsen. Forvaltningsorganet skal sette en frist for slik uttalelse. Hvis det finnes nødvendig av sikkerhetsmessige årsaker kan forvaltningsorganet iverksette avgjørelsen straks.

Den som blir nektet bruk av elektronisk kommunikasjon etter første ledd kan påklage avgjørelsen. Reglene i forvaltningsloven[84] kap. VI gjelder tilsvarende så langt de passer.

---

[80] For å kunne effektivisere behandlingen av uttalelser til høringen, vil det være en fordel om høringsinstansene gir sin uttalelse ved å fylle ut et nettbasert skjema på forvaltningsorganets hjemmeside. Adresse, fremgangsmåte og eventuelle sikkerhetstjenester kan fastsettes etter behov med hjemmel i § 3 og § 4.

[81] Bestemmelsen gir adgang til helt eller delvis å sperre for elektronisk kommunikasjon *"hvis det er grunn til å anta"* at den elektroniske kommunikasjonskanalen misbrukes. Andre sanksjoner kan følge av annen lovgiving, for eksempel straffelovens regler om bedrageri og dokumentfalsk, jf. spesialmotivene til forvaltningsloven § 15a. Se Veilederen del 1, kapittel 3.10 *Reaksjoner mot misbruk av elektronisk kommunikasjon*. Hjemmel for forvaltningsorganets sanksjonsmulighet er forvaltningsloven § 15a innledningen, samt bokstav (e). Se også Ot.prp. nr. 108 (2000-2001) pkt. 3.5.4.7.2 (s. 42), samt 20.5 (s.180) om §15a.

[82] Forvaltningsorganet gis adgang til helt eller delvis å nekte videre bruk av elektronisk kommunikasjon hvis enten kommunikasjonsløsningen eller sikkerhetstjenester og –produkter som benyttes misbrukes. Vedkommende må da benytte tradisjonell kommunikasjon mot forvaltningsorganet.

[83] Regelen er et utslag av det kontradiktoriske prinsipp. Adressaten for varselet skal få anledning til å bli kjent med anførselen og eventuelt imøtegå den før sanksjonen iverksettes. Fristens lengde må settes slik at dette blir mulig å gjennomføre. Varselet må være skriftlig, jf. "sende". Slikt varsel kan sendes elektronisk i henhold til hovedregelen i eForvaltningsforskriften § 8 forutsatt at vilkårene i bestemmelsen for øvrig er oppfylt.
I tilfeller der det er særlig alvorlige brudd, for eksempel når organets kommunikasjonsløsning er truet, kan forvaltningsorganet sperre kommunikasjonen samtidig som varselet sendes.

[84] Lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven) kap. VI.

Kapittel 3. Styring og kontroll med informasjonssikkerheten

§ 15[85] *Internkontroll på informasjonssikkerhetsområdet*

Forvaltningsorgan som benytter elektronisk kommunikasjon[86] skal ha beskrevet mål og strategi for informasjonssikkerhet[87] i virksomheten (*sikkerhetsmål* og *sikkerhetsstrategi*).[88] Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet.[89] Sikkerhetsstrategien og

---

[85] Se Veilederen del 1, kapittel 3.3 *Etablering av sikkerhetsstrategi og internkontroll mv.* Begrepene *"Sikkerhetsmål og sikkerhetsstrategi"* er også benyttet i personopplysningsforskriften § 2-3.

[86] Se eForvaltningsforskriften § 3 første ledd, bokstav c).

[87] Informasjonssikkerhet handler om tiltak for sikring av konfidensialitet, integritet og tilgjengelighet. Informasjonssikkerhet er et ledelsesansvar. Det er viktig at ledelsen og forvaltningsorganet forøvrig har tilstrekkelig styring og kontroll med det som gjøres i forvaltningsorganet for å ivareta informasjonssikkerheten.

[88] Forvaltningsorganet har plikt til å utarbeide sikkerhetsmål og sikkerhetsstrategi. Sikkerhetsmålene beskriver hva som ønskes oppnådd på informasjonssikkerhetsområdet. De skal understøtte og bidra til realisering av forvaltningsorganets overordnede mål, etterlevelse av lover og regler og kostnadseffektiv drift. Sikkerhetsstrategien beskriver hvordan forvaltningsorganet skal nå sikkerhetsmålene.

Enkelte forvaltningsorgan velger å legge overordnede prinsipper og kanskje enkelte andre føringer inn i et eget dokument kalt informasjonssikkerhetspolicy. Forskriftens bruk av sikkerhetsstrategi dekker alle de overordnede føringene fra ledelsen, uavhengig av omfang, om innholdet kalles policy, strategi eller annet og om det styrende innholdet samles i ett dokument eller deles i flere dokument med ulike navn.

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

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

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

[89] Mål og strategi for informasjonssikkerhet (sikkerhetsmål og sikkerhetsstrategi) er ledelsens viktigste redskap i styringen av informasjonssikkerheten innenfor forvaltningsorganets ansvarsområde. Ledelsen bør derfor delta aktivt i utformingen og behandlingen av disse og ikke bare koples inn i forbindelse med endelig godkjenning av mål- og strategi. Videre inngår mål og strategi som grunnlaget i *internkontrollen*. Internkontroll i betydningen «styring og kontroll» er i samsvar med hvordan begrepet internkontroll gjennomgående brukes i mange andre forskrifter. En harmonisering av begrepsbruken anses viktig for å få helhetlig og reell styring og kontroll både i virksomhetsstyring generelt og innen informasjonssikkerhet spesielt. Se tilsvarende krav i personopplysningslovens § 13, som krever planlagte og systematiske tiltak for informasjonssikkerhet for personopplysninger, med dokumentasjon. Se også personopplysningslovens § 14 om internkontroll med tilsvarende krav.

internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.[90]

Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet.[91] Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem.[92] Det organet departementet peker ut skal gi anbefalinger på området.[93]

Omfang og innretning på internkontrollen skal være tilpasset risiko.[94]

---

[90] Krav til informasjonssikkerhet forekommer i flere lover, forskrifter og instrukser. Denne regelen peker på nødvendigheten av å se slike krav i sammenheng, og gjennomføre vurderinger og tiltak for informasjonssikkerhet på en helhetlig måte i den enkelte virksomhet, ut fra de regelverkene som stiller relevante krav. Slike krav vil av og til fremkomme direkte som krav til informasjonssikkerhet, og i andre tilfeller mer indirekte, for eksempel som bestemmelser om taushetsplikt eller som krav til tilfredsstillende autentisering eller lignende.

I noen regelverk er kravene mer eller mindre harmonisert, men ikke alle. Se for eksempel krav til sikkerhet også i helseregisterloven (lov av 18. mai 2001, nr 24), §§ 16 og 17, lov om Schengen informasjonssystem (SIS-loven av 16. juli 1999, nr 66) § 3, samt tilhørende SIS-forskrift kapittel 7, som i stor grad gir politiet tilsvarende regler som i personopplysningsforskriftens kapittel 2.

[91] Internkontrollen (styring og kontroll) på informasjonssikkerhetsområdet skal være basert på anerkjente standarder for styringssystem for informasjonssikkerhet. I det ligger en klar føring om at det ikke er tilstrekkelig å basere seg på generelle rammeverk eller standarder for virksomhetsstyring alene. Når det gjelder informasjonssikkerhetsområdet må forvaltningsorganet baserer seg på de standarder som er utviklet innenfor informasjonssikkerhetsområdet spesielt og som oftest omtales som styringssystem for informasjonssikkerhet. De må i tillegg være anerkjente. Samtidig gir eForvaltningsforskriften gjennom nøkkelordene "basere seg på" et viktig handlingsrom til det enkelte forvaltningsorgan for å tilpasse anvendelsen av anerkjente standarder på informasjonssikkerhetsområdet til egne behov og egen helhetlig virksomhetsstyring. Selv om den anerkjente standarden en velger å basere seg på stiller spesifikke krav, må forvaltningsorganet selv beslutte ut fra egen risikovurdering om det enkelte kravet i standarden er noe forvaltningsorganet faktisk skal følge eller ikke. Alle kravstandarder om internkontroll/styringssystem blir derfor i eForvaltningsforskriftens forstand veiledende. Vesentlige avvik fra valgt kravstandard bør imidlertid begrunnes, da de er ment å representere god praksis "for de fleste".

[92] Det handlingsrommet som ligger i bestemmelsen gjør det også lettere å tilpasse anvendelsen av standarden til eventuelle andre rammeverk, standarder, mv. som forvaltningsorganet baserer seg på innen andre områder i egen virksomhetsstyring. En slik tilpasning understøttes av forskriftens føring om at internkontrollen på informasjonssikkerhetsområdet bør være en integrert del av virksomhetens helhetlige styringssystem. Det betyr at forvaltningsorganet normalt ikke bør etablere et eget selvstendig og uavhengig styringsstyrings- eller internkontrollsystem på informasjonssikkerhetsområdet.

[93] Kommunal- og moderniseringsdepartementet har i brev datert 12. mars 2014 utpekt Difi til det organ som iht. forskriften skal gi anbefalinger på området. Difi sine anbefalinger om standarder fremkommer i "Referansekatalog for IT-standarder i offentlig sektor" og på Difis veiledningssider for informasjonssikkerhet. Difi utarbeider i tillegg i 2014-2015 et praktisk rettet veiledningsmateriale for internkontroll/styringssystem i praksis innen informasjonssikkerhet.

[94] Kravet om tilpasningen til risiko gjelder både informasjonssikkerhetsrisikoene og risikoene ved selve internkontrollsystemet – altså det virksomheten gjør for å ha tilstrekkelig styring og kontroll på informasjonssikkerhetsområdet.

Alle tiltak som etableres i og gjennom internkontrollen, og som ikke er direkte pålagt gjennom lov, regelverk eller avtaler, skal være basert på en risikovurdering. Denne kan være overordnet eller detaljert avhengig av risikoens type og tiltakets kostnad. Det er kun risiko utover det ledelsen har definert som akseptabel risiko som det skal brukes resurser på å etablere og vedlikeholde tiltak mot. Et unntak kan

I den utstrekning det er relevant skal sikkerhetsstrategien og internkontrollen for øvrig også adressere, og om nødvendig stille krav til, bl.a.:[95]

a) prosedyrer for anskaffelse, bruk, oppbevaring og sikring av signaturfremstillingsdata[96], passord/PIN-koder og dekrypteringsnøkkel[97] knyttet til personlige sertifikat eller sertifikat for ansatt i forvaltningen,[98] jf. § 17, § 19 og § 22;

b) prosedyrer for anskaffelse, bruk, oppbevaring og sikring av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel knyttet til virksomhetssertifikat[99], jf. § 16 og § 23;

c) prosedyrer for å etablere og opprettholde et sikkert brukermiljø der det benyttes elektroniske signaturer[100], kryptering eller andre sikkerhetstjenester, jf. § 20;

d) prosedyrer for varsling og tilbaketrekking[101] av sertifikat og passord/PIN-koder ved mistanke om tap eller misbruk, jf. § 25;

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. § 27;

f) prosedyrer for å nekte bruk av sertifikat mv. ved misbruk av elektronisk kommunikasjon med forvaltningen, jf. § 14;

g) prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon, jf. § 5 og § 26, se også personopplysningsloven[102] § 13 og personopplysningsforskriften[103] kap 2;[104]

---

være der tiltakene har en klar positiv kost-nytte. Tiltakene må videre være formåls- og kostnadseffektive, ikke ha utilsiktede eller uønskede sideeffekter og ikke koste mer i etablering og drift enn nødvendig. Det bør heller ikke etableres eller benyttes unødvendige tiltak. Er slike etablert tidligere bør de fjernes. Lite formåls- og kostnadseffektive tiltak bør også justeres eller erstattes med bedre tiltak.

[95] Oppregningen i fjerde ledd, av krav til innhold i sikkerhetsstrategien og internkontrollen for øvrig, er tillegg og presiseringer til det som sikkerhetsstrategien og internkontrollen for øvrig skal omfatte. Disse kravene er omtalt i noter til de bestemmelsene det er henvist til i tredje ledd.

[96] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5. I denne forskriftens sammenheng vil *signaturfremstillingsdata* vanligvis være den private nøkkelen i et nøkkelpar som benyttes for assymetrisk kryptering (signering eller autentisering).

[97] Med *krypteringsnøkkel* og *dekrypteringsnøkkel* menes data som benyttes for henholdsvis kryptering og dekryptering. Se § 4 første ledd, bokstav c).

[98] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9. I veiledningen benytter vi fellesbetegnelsen "personsertifikater" for disse to typene (private personlige sertifikater og ansattsertifikater).

[99] Virksomhetssertifikatet identifiserer forvaltningsorganet (jf. eForvaltningsforskriften § 16), i motsetning til personsertifikatene som identifiserer enkeltpersoner som brukere eller ansatte i forvaltningen. Se også "Kravspesifikasjon for PKI i offentlig sektor".

[100] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3.

[101] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 12.

[102] Lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).

[103] Forskrift av 15. desember 2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften).

[104] Forvaltningsorganet skal beskrive sine prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon, se også personopplysningsloven §§ 13 og 14 med utfyllende forskrifter. Forvaltningens plikt til å sikre informasjon etter reglene om taushetsplikt og behandling av

h) prosedyrer for sikkerhetskopiering, oppbevaring og deponering av dekrypteringsnøkkel for opplysninger som angår forvaltningsorganet, jf. § 24.

Kapittel 4. Anskaffelse og bruk av sikkerhetstjenester mv

§ 16 *Sertifikat for forvaltningsorgan (virksomhetssertifikat)* [105]

Forvaltningsorgan som benytter elektronisk signatur[106] kan benytte sertifikat som identifiserer forvaltningsorganet (*virksomhetssertifikat*).[107]

Hvis det skal benyttes sertifikat ved underretning om enkeltvedtak og varsling etter § 8 og ved høringer etter § 13, bør det benyttes virksomhetssertifikat.[108]

---

personopplysninger bør, om ikke annet som et utslag av veiledningsplikten, også utløse plikt til å informere borgerne om de risikoer som hefter ved elektronisk formidling av (person)opplysninger, og til å legge til rette for at borgerne enkelt kan få tilgang til hensiktsmessige sikkerhetstjenester. Taushetsplikten og behandlingsreglene gjelder normalt forvaltningsorganet som sådant. Den enkelte borger kan nok beslutte at vedkommende selv vil sende opplysninger ubeskyttet til forvaltningen, men en slik beslutning bør være basert på relevant og tilstrekkelig informasjon slik at vedkommende gjør et "opplyst valg".

[105] Brukere av forvaltningens tjenester vil vanligvis ha større nytte av å kunne identifisere selve forvaltningsorganet enn å få bekreftet identiteten til den enkelte saksbehandler. Det er forvaltningsorganet som sådant, og ikke den enkelte saksbehandler, som er involvert i samhandlingen, av og til som part, av og til i en annen myndighetsrolle i en sak mellom to private parter. Se i Veilederen del 1, kapittel 4.2 *Sertifikat for forvaltningsorgan (virksomhetssertifikat)*. Når det benyttes sertifikat ved kommunikasjon som involverer andre enn representanter for forvaltningsorganet selv, bør det i størst mulig grad benyttes virksomhetssertifikat.

[106] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 1.

[107] Det er utarbeidet en norsk profil for virksomhetssertifikater (en spesifikasjon der det bl.a. fremgår hvilke opplysninger et slikt sertifikat skal inneholde), se SEID-prosjektet; "*Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater*" versjon 1.02 (februar 2005), pkt. 6. Krav om å følge sertifikatprofilene er innarbeidet i "*Kravspesifikasjon for PKI i offentlig sektor*", se bl.a. punkt 4.1.1.8 i kravspesifikasjonen.

[108] I forbindelse med underretning om vedtak er det forvaltningsorganet som sådant som er avsender. Mottakerens behov er å få bekreftet at forvaltningsorganet står bak meddelelsen. Saksbehandlerens signatur og sertifikat er til liten hjelp i denne forbindelse. Hvis det benyttes sertifikat *bør* det derfor identifisere forvaltningsorganet. Når det benyttes virksomhetssertifikat kan naturligvis saksbehandlers identitet fremgå av vedtaket selv i den utstrekning det er relevant. Skulle det være behov for det kan man evt benytte både saksbehandlers og virksomhetens sertifikat i forbindelse med samme melding. Det samme gjelder høringsdokumenter, men disse vil det nok sjeldnere være behov for å utstyre med signatur.

§ 17 *Informasjon om bruk av sikkerhetstjenester mv* [109]

Et forvaltningsorgan skal gi sine ansatte anvisning på hvilke sikkerhetstjenester og -produkter de skal benytte under tjeneste for organet, og hvorledes de skal gå frem for å anskaffe nødvendig utstyr og data, herunder signaturfremstillingsdata[110] og dekrypteringsnøkkel med tilhørende sertifikat[111] samt passord og PIN-koder mv. [112]

Ved anskaffelse av utstyr og data som nevnt i første ledd, plikter forvaltningsorganet å sørge for at den ansatte får informasjon om:

a) vedkommendes ansvar og plikter i forbindelse med oppbevaring og bruk av signaturfremstillingsdata og dekrypteringsnøkkel med tilhørende sertifikat samt passord og PIN-koder mv., jf. §§ 22 og 25,[113]

b) restriksjoner på bruk av data som nevnt i bokstav a),[114]

c) egen og andres mulighet for å trekke tilbake eller suspendere sertifikat,[115]

d) sertifikatets ikrafttredelses- og utløpsdato og virkningen av at sertifikatet løper ut eller blir trukket tilbake,[116]

---

[109] Aktsom og lojal bruk av sikkerhetstjenester og –produkter er viktig for sikkerheten i, og tilliten til, IT-systemene og til forvaltningens saksbehandling. En forutsetning for å oppnå dette er at arbeidstakerne får tilstrekkelig informasjon om disse forholdene. Det er viktig at slik informasjon er relevant og tilstrekkelig utfyllende, men like viktig er det at informasjonen er tilrettelagt på en måte som innebærer at arbeidstakeren faktisk setter seg inn i den. Et tykt hefte, som kanskje er vanskelig å forstå, og som arbeidstakerne ikke "orker" å lese, kan derfor gi falsk trygghet med hensyn til hva arbeidstakerne vet om forvaltningsorganets sikkerhetsbehov –prosedyrer. Og det er slett ikke sikkert det hjelper stort om man avkrever dem en skriftlig erklæring om at heftet er mottatt og lest. Men *sikkerhetsarbeidet er viktig*. Det er av stor betydning at arbeidstakerne er innforstått med forvaltningsorganets sikkerhetsstrategi. Det kan være en god investering å gi arbeidstakerne personlig veiledning om disse forholdene, for eksempel i form av kurs eller korte veiledningsmøter, i tillegg til det skriftlige informasjonsarbeidet.

[110] I denne forskriftens sammenheng omfatter signaturfremstillingsdata også privat nøkkel som benyttes for autentiseringsformål, det vil si for å bekrefte identiteten til en person eller en virksomhet, uten å knytte vedkommende til innholdet i en bestemt melding. Se for øvrig lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5.

[111] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9.

[112] I dette ligger for det første det selvfølgelige, at en arbeidsgiver skal bistå arbeidstakeren med å skaffe de "verktøy" arbeidstakeren trenger i sitt arbeid. Men det er også en påminnelse om at arbeidstakeren ikke fritt kan velge hvilke sikkerhetstjenester og –produkter som skal benyttes i tjenesten, men må følge arbeidsgivers instrukser. Hvilke tjenester og produkter som skal benyttes, og prosedyrer for anskaffelse og bruk, skal være basert på de behov og krav som er beskrevet i forvaltningsorganets sikkerhetsstrategi, jf. § 15.

[113] Den enkelte skal informeres om kravene til forsvarlig oppbevaring og bruk av signaturfremstillingsdata, dekrypteringsnøkler, passord og koder, se nærmere om kravene i §§ 22 og 25.

[114] Hvis det er begrensninger i hva den enkelte kan bruke sine signaturfremstillingsdata og brukerrettigheter til, skal vedkommende informeres om dette. En slik begrensning kan for eksempel være at signaturfremstillingsdata med tilknyttet personsertifikat bare skal kunne benyttes i tjeneste for arbeidsgiver og ikke til privat bruk, jf. § 19. Et virksomhetssertifikat kan naturligvis aldri benyttes for private formål.

[115] Den enkelte vil være forpliktet til å gi varsel og begjære tilbaketrekking av sitt sertifikat dersom for eksempel signaturfremstillingsdata kommer på avveie eller det inntrer andre forhold som gjør at sertifikatet ikke lenger skal benyttes, for eksempel mistanke om misbruk, se § 25. Når det benyttes virksomhetssertifikat, eller personsertifikat som er beregnet for bruk i tjenesten, vil også forvaltningsorganet være berettiget til begjære sertifikatet trukket tilbake. Sertifikatinnehaveren skal informeres om dette.

e) hvilke opplysninger om den enkelte som vil fremgå av sertifikatet[117] og sertifikatutsteders[118] behandling av personopplysninger,[119] jf. personopplysningsloven § 19,[120] og

f) forvaltningsorganets sikkerhetsstrategi for øvrig, jf. § 15.[121]

§ 18 *Innhenting av samtykke ved bruk av elektronisk signatur*[122]

Når det benyttes elektroniske signaturer, skal forvaltningsorganet ha innhentet samtykke fra de ansatte i henhold til lov om elektronisk signatur § 7 og § 14 annet ledd bokstav b om utstedelse og utlevering av sertifikat.[123]

§ 19 *Restriksjoner på bruk av sertifikat mv.*[124]

Signaturfremstillingsdata[125], sertifikat[126] eller passord/PIN-koder som er ment for bruk i tjeneste for forvaltningen, skal ikke benyttes for andre formål.[127]

---

[116] Sertifikater har begrenset gyldighetstid (to til tre år er vanlig). Dette skyldes bl.a. administrative forhold. Etter at sertifikatet har løpt ut vil det vanligvis ikke være mulig å få vanlig statusopplysning om sertifikatet.
[117] Dette vil avhenge av hvilken type sertifikat det er tale om, men for personsertifikater vil de personrelaterte opplysningene gjerne være begrenset til sertifikatinnehaverens navn og et løpenummer tildelt av sertifikatutstederen.
[118] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 10.
[119] På grunnlag av opplysningene i sertifikatet kan sertifikatutstederen kople sertifikatet til for eksempel innehaverens fødselsnummer. Dette kan i visse tilfelle utleveres til sertifikatmottaker, men det forutsetter bl.a. at kravene i personopplysningsloven § 12 er oppfylt. I praksis vil forvaltningen i forbindelse med sin myndighetsutøvelse vanligvis oppfylle kravet til behandling av fødselsnummer.
[120] Det er naturlig at slik informasjon gis i forbindelse med innhenting av samtykke etter efvf § 18.
[121] I tillegg til de forhold som er listet ovenfor, er det viktig at arbeidstakeren får informasjon om de alminnelige reglene om forsvarlig bruk av forvaltningsorganets informasjonssystem, se § 15 fjerde ledd bokstav (c) og § 20. Se også de generelle merknadene til § 17 om betydningen av at slik informasjon gis på en måte som er effektiv.
[122] Personopplysningsloven kommer til anvendelse på behandling av personopplysninger i forbindelse med sertifikater og elektroniske signaturer. I tillegg finnes enkelte, delvis overlappende, særbestemmelser om sertifikatutstederes behandling av personopplysninger i lov om elektronisk signatur § 7.
[123] For *kvalifiserte sertifikater* gjelder det særvilkår at sertifikatene bare kan gjøres offentlig tilgjengelig når sertifikatinnehaveren har samtykket til det. Hvis forvaltningsorganets ansatte skal benytte personsertifikater i tjenesten, er det i praksis en forutsetning at slikt samtykke er gitt. For virksomhetssertifikat er det derimot ikke krav om slikt samtykke. Dette gjelder også om det disponeres av en enkeltperson (arbeidstaker i forvaltningen), jf. § 23 annet ledd. For *alle* sertifikater gjelder at opplysningene som samles inn til bruk i forbindelse med utstedelse og bruk av sertifikater, enten må samles inn direkte fra den opplysningene gjelder, eller med dennes uttrykkelige samtykke. Dette innebærer en begrensning i mulighetene for automatisk å tildele alle ansatte sertifikat. Opplysninger som er innsamlet for utstedelse og bruk av sertifikater, kan ikke benyttes for andre formål.
[124] Bestemmelsen fastlegger hovedreglene for når sertifikater kan benyttes i og utenfor tjeneste og for kommunikasjon med andre enn forvaltningsorganer. Bestemmelsens første og annet ledd gjelder den forvaltningsansattes bruk av sertifikat mv. Tredje ledd gjelder mulige restriksjoner rettet mot den enkelte bruker av forvaltningens tjenester.
[125] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5.
[126] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9.

Personlige sertifikat skal ikke benyttes i tjeneste for forvaltningen med mindre det er utstedt eller godkjent for slik bruk.[128]

Et forvaltningsorgan kan bestemme at et sertifikat som er utstedt spesielt for kommunikasjon med forvaltningen, eller med et bestemt forvaltningsorgan, ikke skal benyttes for andre formål. Slike begrensninger må fremgå av sertifikatet, og brukeren skal opplyses om begrensningene.[129]

§ 20 *Forvaltningsansattes bruk av forvaltningsorganets informasjonssystem*[130]

Forvaltningsansatte skal følge instruksene arbeidsgiver har fastsatt om bruk og sikring av virksomhetens informasjonssystemer, herunder om kontroll med materiale som skal lastes ned eller installeres på den ansattes arbeidsstasjon, og forvaltningsorganets sikkerhetsstrategi for øvrig, jf. § 15.[131]

---

[127] Virksomhetssertifikat skal naturligvis bare benyttes når det handles på vegne av forvaltningsorganet. Men også for personsertifikater som er utstedt for bruk i tjeneste for forvaltningsorganet skal bruken begrenses i henhold til dette formålet. Dette vil gjelde for bl.a. ansattsertifikater, der tilknytningsforholdet til forvaltningsorganet fremgår, men kan også gjelde andre personsertifikater som er utstedt for samme formål. Det vil nok sjeldnere forekomme at personsertifikater som bare identifisere innehaveren som enkeltperson kan sies å være utstedt til bruk i tjeneste for forvaltningsorganet. Sertifikatinnehaveren skal informeres om begrensningene, jf. § 17.

[128] Forvaltningsorganet har behov for å koordinere bruk av sertifikater, og personsertifikater som den enkelte ansatte selv har anskaffet kan bare benyttes i tjenesten dersom forvaltningsorganet har godkjent det. Dette bør fremgå av sikkerhetsstrategien, jf. efvf. § 15 siste ledd, bokstav a). Av hensyn til forvaltningens brukere (som mottar henvendelser fra forvaltningen) bør det vanligvis benyttes virksomhetssertifikat når forvaltningen benytter sertifikatbaserte løsninger, se også eforvaltningsforskriften § 16 ovenfor. Også den sertifikatpolicy sertifikatet er utstedt under, eller dårlig tilgjengelighet til statusinformasjon om den enkeltes sertifikat, kan gjøre det uegnet for bruk i tjenesten. Ved kryptering av melding til forvaltningen skal forvaltningsorganets krypteringsnøkkel eller krypteringsnøkkel til en nærmere angitt enhet ved forvaltningsorganet benyttes, se eforvaltningsforskriften § 5. Kryptering med en enkeltpersons krypteringsnøkkel kan bare benyttes dersom forvaltningsorganet har lagt spesielt til rette for det.

[129] Hvis et forvaltningsorgan utsteder, eller får utstedt, sertifikater til bruk ved kommunikasjon med forvaltningsorganet, og tilpasset den risikoprofil det representerer, kan det være aktuelt å begrense bruken av sertifikatet til dette formålet. Man kan for eksempel tenke seg at brukeren logger seg inn på en tjeneste med en tildelt engangskode, og at det deretter lastes ned "softsertifikater" som skal benyttes for videre kommunikasjon (nivå *"standard"* i henhold til *"Kravspesifikasjon for PKI i offentlig sektor"*). Bruk av engangskoden og de aktuelle sertifikatene kan være tilfredsstillende for kommunikasjon med forvaltningsorganet i en sammenheng der transaksjonstypene er kjent, men det er ikke dermed sagt at utsteder er parat til å anbefale sertifikatet for andre formål. En slik begrensning skal imidlertid fremgå av sertifikatet, og brukeren skal varsles om begrensningene, jf. §§ 17 og 21.

[130] Aktsom og lojal bruk av forvaltningsorganets informasjonssystemer er viktig for sikkerheten i, og tilliten til, IT-systemene og til forvaltningens saksbehandling. Bestemmelsen er en påminnelse om at de ansatte skal følge de instrukser arbeidsgiver har fastsatt når det gjelder bruk og sikring av virksomhetens informasjonssystemer. En forutsetning for å oppnå dette er at arbeidstakerne får tilstrekkelig informasjon om disse forholdene, jf. § 17. Det er av stor betydning at arbeidstakerne er innforstått med forvaltningsorganets sikkerhetsstrategi.

[131] I tillegg til de alminnelige tiltak for sikring av passord og andre tilgangskoder til IT-systemene, er det viktig at forvaltningsorganet har kontroll med at det ikke lastes ned programvare på brukernes datamaskiner som kan sette sikkerheten til systemene i fare. Slik risiko kan være knyttet til datavirus og

§ 21 *Informasjon*[132]

Forvaltningsorganet skal sørge for at enhver, i den utstrekning det er nødvendig, får tilsvarende informasjon som nevnt i § 17 og § 19 tredje ledd i forbindelse med anskaffelse av sertifikat eller, hvis det ikke er mulig, ved første gangs bruk av slike tjenester ved kommunikasjon med et forvaltningsorgan.[133] Forvaltningsorganet skal på samme måte informere publikum om at håndtering av signaturfremstillingsdata[134], passord/PIN-koder og dekrypteringsnøkkel skal skje i henhold til §§ 22 og 25.

Kapittel 5. Beskyttelse av signaturfremstillingsdata og dekrypteringsnøkkel mv

§ 22 *Krav til oppbevaring og bruk av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel*[135]

Innehaver av signaturfremstillingsdata[136] skal oppbevare og benytte disse på en slik måte at de ikke gjøres tilgjengelige for andre.[137]

"passordsniffere" mv, men også til skadelig kode som kan gripe inn i bruken av sikkerhetstjenester og -produkter og for eksempel endre data som skal signeres uten at brukeren kan oppdage det.

[132] Bestemmelsen pålegger forvaltningsorganet å gi forvaltningens brukere informasjon og veiledning om anskaffelse og forsvarlig bruk av sikkerhetstjenester og –produkter etter de samme linjer som gjelder for forvaltningsansatte, jf. § 17, og om eventuelle restriksjoner på bruk av den enkeltes sertifikat, jf. § 19 tredje ledd.

[133] Hvis tjenestene leveres av tredjepart, må forvaltningsorganet enten sørge for at tilstrekkelig veiledning gis av tjenesteleverandøren, eller forvaltningsorganet må selv informere brukeren ved første henvendelse der det gjøres bruk av tjenestene. Veiledningen må være tilstrekkelig til at brukeren blir i stand til å benytte tjenestene på en effektiv og forsvarlig måte, og til at kravene i sikkerhetsstrategien blir realisert.

[134] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5.

[135] Bestemmelsen fastlegger kravene til aktsom og forsvarlig oppbevaring og bruk av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkler. Kravene tilsvarer det som ellers må regnes som "god skikk" på området. Kravene er rettet mot den enkelte bruker (også forvaltningsansatte). Forvaltningsorganet skal informere den enkelte om dette i henhold til eforvaltningsforskriften § 21.

[136] Se lov om elektronisk signatur § 3 nr. 5. Når det benyttes digital signatur og sertifikater, er signaturfremstillingsdata ensbetydende med den "private nøkkelen".

[137] Ettersom signaturfremstillingsdataene er de dataene som gjør den elektroniske signaturen unik for innehaveren og den signerte meldingen, er det viktig at ikke signaturfremstillingsdataene kommer på avveie. Skulle en annen få kontroll over signaturfremstillingsdataene kan vedkommende opptre som den egentlige innehaverens "elektroniske dobbeltgjenger". Det er flere løsninger for oppbevaring av signaturfremstillingsdata. De kan være oppbevart i for eksempel et smartkort (eller SIM-kortet til mobiltelefonen), de kan ligge kryptert i programvare på brukerens datamaskin, eller de kan være lagret på en sentral server. Valg av løsning er avhengig av sikkerhetsprofil og bruksområde. Beskyttelsesmekanismene for signaturfremstillingsdata som er lagret sentralt eller i programvare har brukeren liten innflytelse over, men dersom brukeren selv kan velge passord eller kode som gir tilgang til dataene, er det viktig å velge passord og koder som er tilstrekkelig sikre (slik som for koder til bankkort og for passord til arbeidsgivers datasystem mv). Man bør typisk unngå bruk av for eksempel fødselsdato eller år, navn på familiemedlemmer og naturlige ord som man vil finne igjen i en ordbok. En utfordring med

Innehaver skal aldri forlate arbeidsstasjon og lignende uten å sikre at signaturfremstillingsdata ikke er tilgjengelige for andre.[138] Innehaver skal sikre:

a) at signaturfremstillingsdata fjernes fra arbeidsstasjonen dersom dataene er lagret i smartkort eller i en annen enhet som lett kan fjernes, og

b) at den aktuelle arbeidsoperasjonen er avsluttet og eventuelle lagrede eller behandlede signaturfremstillingsdata er deaktivert, eller

c) at signaturfremstillingsdata på annen måte er sikret mot misbruk.

Innehaver av signaturfremstillingsdata skal ikke overlate disse til andre eller gi andre tilgang til dem. Skal noen handle på vegne av en annen skal dette skje med fullmektigens egne signaturfremstillingsdata.[139]

Bestemmelsene om oppbevaring og bruk av signaturfremstillingsdata gjelder tilsvarende for bruk av passord/PIN-koder o.l. og dekrypteringsnøkkel.[140]

§ 23 *Sikring av signaturfremstillingsdata og dekrypteringsnøkkel ved bruk av virksomhetssertifikat*[141]

Ved bruk av virksomhetssertifikat skal forvaltningsorganet sikre at ikke uvedkommende får tilgang til eller kan benytte tilhørende signaturfremstillingsdata[142].[143] Organet skal også sikre tilfredsstillende kontroll med og registrering av personell og aktiviteter som

---

"kompliserte" koder og passord er at man av og til vil ha behov for å notere dem ned. Kodene bør i så fall skjules, og ikke oppbevares sammen med kortet eller i naturlig tilknytning til datamaskinen.

[138] Brukeren skal sikre at ikke uvedkommende får tilgang til signaturfremstillingsdataene. Hvis de er oppbevart i smartkort eller lignende bør brukeren vanligvis ikke etterlate kortet i kortleseren på datamaskinen, men ta det med seg, eller oppbevare det på et forsvarlig sted når vedkommende ikke er tilstede ved datamaskinen eller dataene ikke er i bruk (som for et bankkort). Alternativt må signaturfremstillingsdataene sikres på annen måte, slik at ikke uvedkommende får tilgang til dem, se bokstav c) i samme bestemmelse.

[139] Signaturfremstillingsdata og personsertifikat skal ikke overlates til andre. Hvis en person skal signere på vegne av en annen, skal dette fremgå ved at underskriveren benytter sine egne signaturfremstillingsdata og sertifikat, med angivelse av at det signeres på vegne av en annen.

[140] For at bestemmelsen skal bli så enkel som mulig å lese, er bare signaturfremstillingsdata nevnt i teksten ovenfor, men de samme prinsippene gjelder for dekrypteringsnøkkel (som vanligvis også er en privat nøkkel) og for beskyttelse av passord og PIN-koder.

[141] Reglene om sikring av signaturfremstillingsdata i § 22 ovenfor, gjelder også når det benyttes virksomhetssertifikat. I tillegg kommer kravene i denne bestemmelsen om særlige forholdsregler ved bruk av virksomhetssertifikat. Bestemmelsen er rettet mot forvaltningsorganet. Se Veilederen del 1, kapittel 4.6 *Sikring av forvaltningsorganets krypteringsnøkler mv*.

[142] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5.

[143] Et virksomhetssertifikat kan disponeres av en eller flere ansatte i virksomheten, eller være koplet direkte til en server eller en bestemt systemaktivitet (for eksempel saksbehandlingssystemet). Virksomhetssertifikatet skal sikre at mottakeren kan verifisere at forvaltningsorganet er avsender eller kommunikasjonsmotpart, og det er naturligvis viktig at ikke uvedkommende kommer i posisjon til å opptre som om de var forvaltningsorganet. Det er forvaltningsorganets oppgave å legge til rette for at ikke uvedkommende får tilgang til signaturfremstillingsdataene. Hvis signaturfremstillingsdataene er lagret i smartkort gjelder de samme regler som for kort knyttet til personsertifikat, jf. § 22. Hvis signaturfremstillingsdataene er lagret sentralt i forvaltningsorganets datasystem, må tilgangskontroll og øvrige sikringstiltak sørge for at ikke uvedkommende får tilgang.

benytter slike signaturfremstillingsdata.[144] Sikringstiltakene skal skje i henhold til organets sikkerhetsstrategi.[145]

Når flere personer hver for seg skal disponere virksomhetssertifikat, bør hver enkelt disponere eget virksomhetssertifikat med tilhørende signaturfremstillingsdata.[146]

Ved bruk av virksomhetssertifikat skal det være lagt opp rutiner som sikrer at systemet raskt kan settes i drift med nye signaturfremstillingsdata og nytt sertifikat dersom det sertifikatet som er i bruk, blir trukket tilbake eller signaturfremstillingsdata går tapt.[147]

Det skal vurderes om forvaltningsorganet bør være utstyrt med signaturfremstillingsdata og virksomhetssertifikat fra mer enn én sertifikatutsteder[148].

Signaturfremstillingsdata og dekrypteringsnøkkel skal være sikret mot misbruk i henhold til forvaltningsorganets sikkerhetsstrategi, jf. § 15.[149]

---

[144] Selv om virksomhetssertifikatet utad skal signalisere at det er forvaltningsorganet det kommuniseres med, må organet selv ha kontroll med hvilke personer eller systemaktiviteter (i et automatisert system) som utløser bruk av signaturfremstillingsdata knyttet til forvaltningsorganet. Praktisk sett betyr dette at systemet skal realisere tilfredsstillende tilgangskontroll og det skal logge hvilke personer og/eller systemaktiviteter som utløser bruk av signaturfremstillingsdata som er knyttet til (den offentlige nøkkelen i) et virksomhetssertifikat.

[145] Forvaltningsorganets risikovurdering, internkontrollsystem og sikkerhetsstrategi er nøkkelen til en helhetlig, planlagt og dokumentert gjennomføring av forvaltningsorganets sikringstiltak. Dette gjelder også sikring av virksomhetssertifikat som er kritisk for tilliten til å kunne kommunisere trygt med forvaltningsorganet.

[146] Selv om virksomhetssertifikatet identifiserer forvaltningsorganet, er hvert sertifikat unikt med eget serienummer og eget nøkkelpar. I de tilfellene der enkeltpersoner skal disponere slikt sertifikat på vegne av forvaltningsorganet, bør de ha hvert sitt (men i mange tilfeller vil det altså være lagret sentralt og styrt via tilgangskontroll mv). Når de aktuelle personer disponerer hvert sitt sertifikat (og nøkkelpar), kan forvaltningsorganet ved kontroll av signaturen med tilhørende sertifikat se hvem av de ansatte som står bak meldingen. Dessuten behøver ikke alle få nytt sertifikat selv om et nøkkelpar skulle komme på avveie eller lignende. Dette kan lette administrasjonen av meldinger og sertifikater. Se også Veilederen del 1, kapittel 4.2 *Sertifikat for forvaltningsorgan (virksomhetssertifikat)*, tredje avsnitt.

[147] Når et forvaltningsorgan, eller en annen virksomhet for den delen, baserer mye av sin eksterne kommunikasjon på bruk av elektroniske kanaler, oppstår det risiko for avbrudd som er ny i forhold til tradisjonelle metoder. Dette gjelder for det første tekniske avbrudd i IT-systemene generelt, men i denne sammenheng gjelder det å forebygge stans i kommunikasjonen som følge av svikt i de sikkerhetsmekanismene som benyttes. Et forvaltningsorgan som overfor omverdenen identifiserer seg ved hjelp av virksomhetssertifikat, vil i en periode være avskåret fra å kommunisere dersom sertifikatet av en eller annen årsak må trekkes tilbake. Dette kan skje for eksempel fordi en mistenker at forvaltningsorganets egne nøkler er misbrukt, eller fordi sertifikatutstederens sertifikat av en eller annen grunn er trukket tilbake, eller er ute av drift. For å redusere risikoen for slike driftsavbrudd til et minimum, kan det være fornuftig for et forvaltningsorgan å disponere to virksomhetssertifikater, og forvaltningsorganet skal som et minimum ha beskrevet rutiner for hvordan man raskt kan ta nye signaturfremstillingsdata og sertifikater i bruk. Dette skal fremgå av sikkerhetsstrategien, jf. § 15 fjerde ledd bokstav (b). Det kan av de samme grunner være fornuftig å ha virksomhetssertifikat fra to forskjellige sertifikatutstedere, og forvaltningsorganet er pålagt å vurdere om det er behov for et slikt tiltak, jf. § 23 fjerde ledd.

[148] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 10.

[149] Som for sikringstiltak ellers, skal signaturfremstillingsdata og dekrypteringsnøkler sikres i henhold til sikkerhetsstrategien.

§ 24 *Sikkerhetskopiering av dekrypteringsnøkkel mv.*[150]

Forvaltningsorganet skal sikre at opplysninger og annet materiale som oppbevares av forvaltningsorganet i kryptert form, ikke blir utilgjengelige som følge av at dekrypteringsnøkler går tapt. Forvaltningsorganet plikter å oppbevare kopi av dekrypteringsnøkler for slikt materiale.[151]

Prosedyrer for sikkerhetskopiering, oppbevaring, deponering og utlevering av dekrypteringsnøkkel skal følge anerkjente prinsipper og skal fremgå av forvaltningsorganets sikkerhetsstrategi, jf. § 15.[152]

§ 25 *Varslingsplikt ved tap eller mistanke om misbruk av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel*[153]

Innehaver av signaturfremstillingsdata[154] skal straks varsle sertifikatutsteder[155] eller den som ellers er utpekt til å motta varsel, dersom det oppstår mistanke om at signaturfremstillingsdata er tapt, kommet på avveie eller på annen måte blir eller kan bli misbrukt.[156] Det samme gjelder for bruk av passord/PIN-koder o.l. og dekrypteringsnøkkel.

---

[150] Det er viktig at forvaltningsorganets dokumenter mv alltid er tilgjengelige når det er behov for dem, og at man ikke risikerer at data går tapt som følge av at de ikke kan dekrypteres dersom dekrypteringsnøkler av en eller annen grunn bli utilgjengelige. Det skal derfor alltid finnes kopier av dekrypteringsnøkler som er knyttet til forvaltningsorganet. Bestemmelsen retter seg mot forvaltningsorganet. Se også § 26 nedenfor.

[151] Det finnes motforestillinger av bl.a. personvernmessig art når det gjelder krav om sikkerhetskopiering og deponering av dekrypteringsnøkler generelt. Men ettersom det her dreier seg om dekrypteringsnøkler til data som gjelder *forvaltningsorganet* (og ikke til saksbehandler), utløser det ikke noe personvernmessig problem, jf. § 5 fjerde ledd.

[152] Både av sikkerhetsmessige grunner, og av effektivitetshensyn, er det viktig at rutiner for kopiering, oppbevaring, og utlevering (ved behov) av kopierte dekrypteringsnøkler er beskrevet i sikkerhetsstrategien. Sikkerhetskopiering og/eller deponering av krypteringsnøkler forutsetter gode prosedyrer for sikring av kopiene slik at materiale ikke blir gjort tilgjengelig for uvedkommende. Tilgang til slikt materiale bør kunne gjøres tilgjengelig uten tidkrevende prosedyrer når behovet først oppstår. Det er naturlig at retten til utlevering er knyttet til bestemte roller i forvaltningsorganet, for eksempel etatsjef eller den/de vedkommende bemyndiger, og at de det gjelder er kjent med rutinene.

[153] Varsling om tilbaketrekking av sertifikat ved mistanke om at signaturfremstillingsdata er kommet på avveie, og blir eller kan bli misbrukt, er en viktig del av sikkerheten rundt elektroniske signaturer og sertifikattjenester. Regler om dette vil regelmessig også foreligge som avtalevilkår mellom sertifikatinnehaveren og utstederen av sertifikatet. Bestemmelsen retter seg mot den enkelte bruker (og forvaltningsansatte).

[154] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5.

[155] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 10.

[156] En viktig side ved sikkerheten rundt elektroniske signaturer og sertifikater er at potensielle mottakere blir varslet dersom det er mistanke om misbruk av signaturfremstillingsdata. Dette skjer gjerne ved at en statustjeneste vedlikeholder oversikt over sertifikater som av en eller annen grunn ikke lenger skal benyttes. Slik oversikt kan gjøres tilgjengelig som en såkalt "tilbaketrekkingsliste" (revokeringsliste), eller i form av en oppslagstjeneste der det i sanntid gis opplysning om sertifikatets status, se for eksempel lov om elektronisk signatur § 12. Den som disponerer signaturfremstillingsdata, enten de er knyttet til personsertifikat eller virksomhetssertifikat, skal alltid varsle (rette instans) hvis det er mistanke om misbruk eller signaturfremstillingsdataene har kommet på avveie. Det samme gjelder for dekrypteringsdata og passord/PIN-koder. Hvor varsel skal gis kan variere avhengig av løsning, men brukeren skal være gjort kjent med rutinene for dette, jf. § 17 og 21.

Kapittel 6. Forvaltningsorganets behandling av meldinger som er kryptert eller signert

§ 26 *Mottak av kryptert melding*[157]

Melding som mottas av forvaltningsorganet i kryptert form, skal straks dekrypteres.[158]

Hvis meldingen ikke lar seg dekryptere ved mottak, skal det straks sendes melding til avsender med beskjed om at forvaltningsorganet ikke får tilgang til meldingens innhold. § 7 gjelder tilsvarende.[159]

Forvaltningsorganet skal sikre opplysningene under den videre behandling i organet i henhold til de regler som gjelder for de aktuelle opplysningene.[160]

---

[157] Bestemmelsen stiller krav til håndtering av meldinger som er kryptert når de mottas av forvaltningsorganet. Bestemmelsen retter seg mot forvaltningsorganet.

[158] Når forvaltningsorganet mottar en kryptert melding skal den straks dekrypteres. Dette er for det første nødvendig for å kunne ta stilling til innholdet i meldingen, og eventuelt varsle avsenderen dersom noe viser seg ikke å være som det skal, jf. § 7. Men det vil også gjerne være slik at det benyttes andre mekanismer, eller i alle fall andre krypteringsnøkler, for å sikre dataene internt i forvaltningsorganet enn de som benyttes for å sikre kommunikasjonen med eksterne brukere. Når det benyttes offentlig-nøkkel kryptering med eksterne brukere, vil selve meldingen være kryptert med en engangsnøkkel, og denne engangsnøkkelen er kryptert med forvaltningsorganets offentlige nøkkel. Det er unødig krevende å administrere alle disse engangsnøklene over tid. Internt er det mer hensiktsmessig om alle data som skal krypteres (eller i alle fall alle data av en viss type eller tilhørende samme enhet) krypteres med en felles nøkkel, eller sikres etter de regler som ellers gjelder for de aktuelle dataene. Det er nok bare unntaksvis behov for å lagre dataene i kryptert form hos forvaltningsorganet. Hvis dataene er både signert og kryptert når de mottas, må forvaltningsorganet håndtere signaturene i henhold til §§ 27 og 28.

[159] Avsenderadressen er vanligvis ikke kryptert, så med mindre det er benyttet en annen avsenderadresse enn den avsenderen vanligvis treffes på, vil det i de fleste tilfelle være mulig å varsle vedkommende selv om selve meldingen ikke kan leses.

[160] Det kan foreligge særlige retningslinjer for den interne behandlingen av opplysningene. Se også note 158 ovenfor.

§ 27 *Krav til kontroll av sertifikater og tilbaketrekkingslister*[161]

Ved mottak av melding som er underlagt krav om bruk av avansert elektronisk signatur[162],[163] skal forvaltningsorganet kontrollere, i henhold til kravene fastsatt i organets sikkerhetsstrategi, jf. § 15:[164]

a) at signaturen lar seg verifisere, herunder at meldingen ikke er endret,[165]

b) at tilknyttet sertifikat[166] fortsatt er gyldig og ikke suspendert eller trukket tilbake,[167] eller det dokumenteres at sertifikatet var gyldig på signeringstidspunktet,[168]

c) at sertifikatet er egnet for den aktuelle anvendelse, herunder sertifikatets sikkerhetsnivå og eventuelle begrensninger i sertifikatets anvendelsesområde,[169]

---

[161] En viktig, men ofte undervurdert side ved sertifikatbruk, er prosessen rundt kontroll av sertifikater i forbindelse med mottak av meldinger som er signert, eller i forbindelse med bekreftelse av en brukers identitet eller rolle. Se mer om dette i Veilederen del 1, kapittel 4.3 *Kontroll av sertifikater mv*. Bruk av elektronisk identitetsbevis (eID) og elektronisk signatur i offentlig sektor er nå samordnet gjennom ID-porten som forvaltes av Direktoratet for forvaltning og IKT (Difi). Det fremgår av Digitaliseringsrundskrivet (H-7/2014), punkt 1.2 *Bruk av nasjonale felleskomponenter* at: «Virksomheten skal ta i bruk ID-porten for digitale tjenester som krever innlogging og autentisering.» Slike føringer er gjenstand for politiske beslutninger og kan endres over tid. Digitaliseringsrundskrivet oppdateres jevnlig.

Kravene til sertifikatverifisering i § 27 er minimumsregler. Det kan være behov for å foreta tilsvarende kontroller også når det ikke er stilt krav om avansert elektronisk signatur, men det likevel benyttes sertifikater. For eksempel vil det vanligvis være nødvendig å kontrollere sertifikater som benyttes i forbindelse med innholdskryptering. Bestemmelsen retter seg først og fremst mot forvaltningsorganet som skal legge til rette for at de beskrevne kontroller kan gjennomføres.

[162] Se lov om elektronisk signatur § 3 nr. 2.

[163] Bestemmelsen kommer til anvendelse i de tilfellene det er stilt krav om bruk av avansert elektronisk signatur. Når det først er stilt et slikt krav får man anta at det er behov for den sikkerheten en slik signatur representerer. For å oppnå dette er det nødvendig at signatur og sertifikat kontrolleres som angitt nedenfor.

[164] Det kan variere fra område til område hvor strenge krav som skal stilles, eller i alle fall hvor oppdaterte statusopplysninger mv må være. Dette må forvaltningsorganet ta stilling til i sin sikkerhetsstrategi.

[165] Dette er en rent teknisk kontroll for å sjekke at meldingen er uendret, at signaturen hører til den aktuelle meldingen, og at signaturen kan verifiseres ved hjelp av et bestemt sertifikat (eller en offentlig nøkkel som forvaltningsorganet på annen måte kjenner).

[166] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9.

[167] Sikkerhetsstrategien fastsetter krav til hvor oppdatert slik statusinformasjon skal være, for eksempel om det kreves oppslag mot en kontinuerlig oppdatert tjeneste som leverer opplysninger om status på oppslagstidspunktet, eller om det er tilstrekkelig at det benyttes en tilbaketrekkingsliste med lavere ajourføringsfrekvens, for eksempel en liste som oppdateres daglig. Oppdateringskrav til statustjenestene fremgår av "Kravspesifikasjon for PKI i offentlig sektor", pkt. 5.1.

[168] For å sikre at ikke signaturen er avgitt av noen som misbruker signaturfremstillingsdataene, skal forvaltningsorganet kontrollere sertifikatets status (om det er trukket tilbake) når det mottar meldingen. Alternativt kan meldingen fra avsenders side for eksempel være utstyrt med en tidsstemplet statusopplysning som viser at sertifikatet var gyldig på signeringstidspunktet. En slik tilleggsopplysning vil også være nyttig ved arkivering av meldingen. Hvorvidt det er avsender eller mottaker som innhenter slik statusopplysning beror på partenes "signaturpolicy". Dersom statusopplysningen sendes med fra avsender, må man imidlertid være oppmerksom på muligheten for at en tilbaketrekkingserklæring ennå ikke var behandlet på det tidspunkt statusopplysningen ble avgitt.

[169] Ikke alle sertifikater er pålitelige eller beregnet for en hvilken som helst bruk. De kan være utstedt etter begrensede undersøkelser, eller utstederen kan ha hatt et helt bestemt formål med utstedelsen. Sertifikatmottaker må derfor kontrollere at sertifikatet er egnet for det formålet det benyttes for i det aktuelle tilfellet. Rent praktisk skjer dette gjerne ved at man på forhånd har godkjent visse typer sertifikater fra bestemte utstedere, eller sertifikater som er utstedt i henhold til en eller flere sertifikatpolicier

d) at sertifikatet er utstedt av en sertifikatutsteder som anbefales eller er anerkjent av koordineringsorganet, jf. § 36, eller som forvaltningsorganet kan akseptere i henhold til sin sikkerhetsstrategi.[170]

Hvis en melding som er signert med avansert elektronisk signatur ikke tilfredsstiller kontrollene i første ledd, og dette har betydning for behandling av meldingen i forvaltningsorganet,[171] skal det sendes melding til avsender i henhold til reglene i § 7.

§ 28 *Arkivering av avansert elektronisk signatur mv.*[172]

Melding som er signert med en avansert elektronisk signatur[173], og som blir arkivert,[174] skal arkiveres sammen med de opplysninger som er nødvendige for å bekrefte signaturen.[175]

(erklæringer som angir hvordan sertifikatene utstedes og behandles, og hvem som har ansvaret for dette, jf. forskrift om kvalifiserte sertifikater § 4). Bruk av elektronisk identitetsbevis (eID) og elektronisk signatur i offentlig sektor er nå samordnet gjennom ID-porten som forvaltes av Direktoratet for forvaltning og IKT (Difi). Det fremgår av Digitaliseringsrundskrivet (H-7/2014), punkt 1.2 *Bruk av nasjonale felleskomponenter* at: «Virksomheten skal ta i bruk ID-porten for digitale tjenester som krever innlogging og autentisering.» Slike føringer er gjenstand for politiske beslutninger og kan endres over tid. Digitaliseringsrundskrivet oppdateres jevnlig.

[170] Selv om sertifikatet etter sitt innhold og sin policy er anvendelig for det aktuelle formålet, er troverdigheten til sertifikatet avhengig av om forvaltningsorganet anser utstederen som pålitelig. Også denne vurderingen kan forvaltningsorganet ha overlatt til andre, f.eks. ID-porten, jf. noten ovenfor. De sertifikatene som skal benyttes må være omfattet av selvdeklarasjons- eller tilsynsordninger som er etablert i henhold til esignaturloven § 16a.

[171] Det er ikke alltid det spiller noen rolle om disse kravene er oppfylt. Hvis verifisering av signaturen er uten betydning for behandling av meldingen, for eksempel fordi signatur ikke er påkrevet, eller feilen er at sertifikatet har gått ut etter at meldingen ble signert, men uten at man har grunn til å mistenke at noe er galt, eller at man har andre opplysninger som på tilfredsstillende måte reparerer feilen, er det ikke nødvendig å forsinke saksbehandlingen, eller påføre parten merarbeid, ved å returnere meldingen.

[172] Det er mange utfordringer knyttet til bruk av elektroniske signaturer. En av dem er å oppbevare det signerte materialet på en slik måte at det også i ettertid er mulig å foreta en tilfredsstillende verifisering av signaturen og av at opplysningene ikke har endret seg. Arkivering av signaturer mv omfattes generelt av arkivloven og arkivforskriften. I tillegg kommer kravene i eForvaltningsforskriften og i NOARK-5 Standard for elektronisk arkiv, som behandler arkivering av digitale signaturer i pkt. 6.3.. Se også Veilederen del 1, kapittel 4.4. SEID leveranse 3 gir krav til hva som skal lagres.

[173] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 2.

[174] Det er ikke alle meldinger som er arkivverdige, jf. arkivloven og arkivforskriften.

[175] Hvilke opplysninger som er nødvendige er bl.a. avhengig av hvor lenge det er aktuelt å verifisere signaturen. I noen tilfeller har signaturen bare betydning i forbindelse med gjennomføring av transaksjonen, i andre tilfeller vil signaturen kunne være et viktig bevismiddel også flere år senere. Når det benyttes avansert elektronisk signatur får man anta at signaturens pålitelighet har betydning og at en del kontroller blir gjennomført ved mottak, jf. § 27. Som et minimum bør man i disse tilfellene arkivere kopi av meldingen, signaturen, sertifikatet og opplysning om at sertifikatet ble kontrollert og ikke var trukket tilbake på det tidspunkt den signerte meldingen ble mottatt (eller arkivert). Hvis sertifikatet etter sitt innhold kommer til å løpe ut i den perioden det kan være aktuelt å verifisere signaturen, kan det være aktuelt at opplysningene tidsstemples (dvs påføres dato og klokkeslett og signeres med en digital signatur med en beregnet levetid som er minst like lang som den tid det kan være behov for å verifisere signaturen på den aktuelle meldingen eller den type melding det er tale om), jf. § 28 annet ledd nest, siste setning. En kan her som eksempel tenke seg en situasjon der et sertifikats gyldighetsperiode uløper i løpet av måneden

For meldinger som skal konverteres til annet format,[176] skal arkivet ved mottak verifisere signaturen, og deretter på hensiktsmessig måte bekrefte tilknytningen mellom meldingen, meldingens signatur og relevante opplysninger fra sertifikatet[177] sammen med opplysning om tidspunktet for bekreftelsen.[178] Arkivet skal sikre at ikke meldingene, eller dataene som bekrefter de nevnte forholdene, utilsiktet eller urettmessig endres i oppbevaringsperioden.[179] Tilsvarende gjelder meldinger der tilhørende sertifikaters gyldighetsperiode er kortere enn den tiden det kan være behov for å bekrefte meldingens innhold, med mindre det benyttes tidsstempel[180] eller annen tjeneste som sikrer at signaturen ikke endres og at den også i ettertid kan verifiseres. Det enkelte forvaltningsorgan kan bestemme at denne fremgangsmåten skal benyttes også for andre meldinger.

Dersom arkivet ikke lykkes i å verifisere signaturen, skal opplysning om dette lagres, om mulig sammen med opplysninger om årsaken til at verifisering ikke lyktes.

(sertifikaters gyldighetstid er vanligvis to til tre år), og at dokumentet signaturen er knyttet til gjelder spørsmål om pengekrav der foreldelse er en relevant problemstilling. Se også NOARK-5 punkt 6.3.

[176] Det kan av tekniske og arkivfaglige grunner være nødvendig å konvertere (omgjøre) meldingen til et annet format for å kunne oppbevare den over tid. Det er urealistisk for arkivet å ta vare på alle tidligere generasjoner av maskin- og programvare. Konvertering foretas for å gjøre informasjon flyttbar og håndterlig på nye teknologiplattformer. Konvertering kan også skje fordi arkivet ønsker å lagre alle dokumenter/meldinger i et bestemt (NOARK-godkjent) format med én gang (Se NOARK-5, pkt. 5.13.1). Ved konvertering oppheves bindingen mellom meldingen/dokumentet og signaturen. Det vil ikke være mulig å verifisere den opprinnelige signaturen overfor meldingen i det nye formatet. Da må det iverksettes andre tiltak. For å sikre fortsatt notoritet omkring knytningen mellom dokument og signatur, må arkivet oppbevare tilstrekkelige opplysninger til at man i ettertid kan sannsynliggjøre at signaturen ble tilfredsstillende verifisert på relevant tidspunkt. Dette skjer ved at arkivfunksjonen innhenter nødvendige opplysninger og gjennomfører nødvendige verifiseringer, jf. kommentarene til bestemmelsens første ledd. Deretter arkiveres meldingen sammen med arkivets bekreftelse på at korrekt verifisering fant sted på et bestemt tidspunkt. Se også NOARK-5, punkt 6.3.

[177] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9.

[178] Dette er altså en alternativ fremgangsmåte til det som er beskrevet i § 28 første ledd. Hvis meldingen skal konverteres til et annet format, *må* denne fremgangsmåten benyttes. I andre tilfeller *kan* den benyttes, se § 28 annet ledd, siste setning.

[179] Man overlater altså til arkivet å sikre meldingens integritet og troverdighet gjennom sine rutiner for sikker kontroll, lagring og oppbevaring. Tilliten til arkivfunksjonen og arkivets rutiner skal etablere den nødvendige bekreftelse på at knytningen mellom meldingen og sertifikatet var i orden ved mottak, eller at det på annen måte ble gjennomført tilfredsstillende autentisering, og at arkivet deretter har sikret meldingens integritet (at meldingens innhold ikke bevisst eller ubevisst er endret). Arkivet kan også tidsstemple den konverterte meldingen og de aktuelle informasjonsuttrekk fra det tilknyttede opprinnelige sertifikatet. Se også § 12 fjerde og femte ledd om utlevering av materiale som er signert med avansert elektronisk signatur.

[180] Tidsstempling er en sikkerhetsfunksjonalitet som dokumenterer at et dokument eksisterte eller faktisk var i noens besittelse på et gitt tidspunkt. Tidsstempling kan foretas av arkivet selv eller av en uavhengig og tiltrodd tredjepart. Et forvaltningsorgan som mottar en signert melding, og som ønsker å få meldingen tidsstemplet, kan for eksempel videresende til tidsstemplingstjenesten hash-verdien av dokumentet (som er en matematisk representasjon av dokumentet som er signert) samt signaturen og avsenders sertifikat sammen med opplysning om sertifikatets status som er hentet fra statustjenesten. Tidsstemplingsfunksjonen legger så til opplysning om tidspunkt for mottak og påfører sin signatur på det hele og returnerer det.

Melding eller resultat av en automatisert databehandling som er bekreftet på annen måte enn ved avansert elektronisk signatur, bør lagres sammen med opplysninger om at korrekt bekreftelse har funnet sted, og om mulig hvilken teknikk som er blitt benyttet.

Kapittel 7. Digital kontaktinformasjon og reservasjon

§ 29 *Bruk av digital kontaktinformasjon og reservasjon*[181]

Det etableres register over digital kontaktinformasjon og reservasjon med tilhørende infrastruktur.[182]

Opplysninger i register over digital kontaktinformasjon og reservasjon kan benyttes i forbindelse med saksbehandling og utføring av forvaltningsoppgaver for øvrig,[183] og skal benyttes til varsling etter § 8 tredje ledd.[184]

Behandlingsansvarlig avgjør hvordan forvaltningen skal gis tilgang til registeret, herunder om forvaltningsorgan skal kunne benytte kopi av registeret. Forvaltningsorgan som mottar kopi har plikt til å holde kopien à jour.[185]

---

[181] Bestemmelsen hjemler etablering av register for, og behandling av, digital kontaktinformasjon og reservasjon med tilhørende infrastruktur, og angir hva opplysningene kan brukes til.

[182] Med «tilhørende infrastruktur» menes blant annet nødvendige oppslagstjenester.

[183] Formuleringen «i forbindelse med saksbehandling og utføring av forvaltningsoppgaver for øvrig», er ment å dekke forvaltningens totale oppgaveløsning, se note 184. Det er derimot ikke anledning til å benytte kontaktregisteret for næringsformål eller ande private formål, f.eks. til utsending av reklame eller spørreundersøkelser, eller for å kvalitetssikre e-postadresser i andre registre. I og med at kontaktregisteret er opprettet spesielt for å ivareta hensynet til forvaltningens utøvelse av forvaltningsoppgaver, og utsending av varsler til den registrerte, vil bruk for private formål være uforenlig med det opprinnelige behandlingsformålet, se personopplysningsloven § 11 c).

[184] Informasjonen i kontaktregisteret skal kunne benyttes for å varsle innbyggerne om alle former for elektroniske henvendelser fra forvaltningen. For varsling i henhold til eForvaltningsforskriften § 8 tredje ledd er forvaltningsorganene pålagt å benytte kontaktregisteret. 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. Mottakers digitale kontaktinformasjon (for eksempel mobiltelefonnummer) skal også kunne benyttes til å kontakte mottaker pr telefon, så lenge bruken er innenfor det formålet som er foreslått for bruk av opplysningene: «i forbindelse med saksbehandling og utføring av forvaltningsoppgaver for øvrig».

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 § 29.

[185] Difi er behandlingsansvarlig for registeret, se § 30, og avgjør hvordan forvaltningen skal gis tilgang til registeret. Normalt vil tilgang bli gitt ved mulighet til online oppslag, men bestemmelsen hjemler også at

Behandlingsansvarlig skal treffe tiltak for å sikre tilfredsstillende kvalitet på opplysningene.[186] Behandlingsansvarlig kan sette vilkår for bruken av registeret.

§ 30 *Behandlingsansvarlig*

Direktoratet for forvaltning og IKT er behandlingsansvarlig[187] for register over digital kontaktinformasjon og reservasjon med tilhørende infrastruktur.[188]

§ 31 *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 som ikke er registrert i Enhetsregisteret:[189]

1. navn og personentydig identifikator[190]
2. nødvendige kontaktopplysninger for elektronisk kommunikasjon med den registrerte[191]
3. opplysninger om den registrertes eventuelle reservasjon mot elektronisk kommunikasjon, jf. § 9
4. den registrertes fullmaktsforhold[192]
5. andre opplysninger som er nødvendige for forvaltningens elektroniske

---

mottaker får kopi av registeret. I disse tilfeller vil mottaker være pålagt å sikre tilstrekkelig ajourhold av kopien. Opplysninger som benyttes bør ikke være mer enn maksimalt 24 timer gamle.

[186] Behandlingsansvarlig vil måtte iverksette tiltak for å sikre tilfredsstillende kvalitet, eksempelvis ved at innbygger i forbindelse med innlogging i ID-porten bes om å kontrollere at registrerte kontaktopplysninger er korrekte. Kvalitetssikringsarbeidet skal baseres på erfaring. Det bør vurderes jevnlig hvor ofte slik spørring bør skje, se § 32 og note 194.

[187] Se personopplysningsloven § 2 nr. 4.

[188] Med «tilhørende infrastruktur» menes at ansvaret blant annet inkluderer nødvendige oppslagstjenester.

[189] For enheter som *er* registrert i Enhetsregisteret vil kontaktopplysninger og varslingsadresser bli lagret i eget register.

[190] I dagens kontaktregister benyttes kun fødselsnummer og d-nummer, men bestemmelsen dekker også bruk av personentydig pseudonym og lignende.

[191] Kontaktopplysninger inkluderer for eksempel mobilnummer, e-postadresse, adresse til fremtidig digital postkasse og lignende.

[192] Hvis en person gir en annen fullmakt til å opptre på sine vegne i (en eller flere) saker overfor forvaltningen, er det behov for å gjøre denne informasjonen tilgjengelig for forvaltningsorganet. Bestemmelsen gir mulighet for at denne typen opplysninger kan registreres i kontaktregisteret dersom en løsning for fullmaktsregistrering blir utviklet. Se også eForvaltningsforskriften § 10 og forvaltningsloven § 2 bokstav g), om bruk av fullmektig og krav til fullmakt.

kommunikasjon i forbindelse med saksbehandling og utføring av forvaltningsoppgaver.[193]

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

Den enkelte som det er registrert opplysninger om i register over digital kontaktinformasjon og reservasjon bør minst to ganger årlig, oppfordres til å oppdatere eller bekrefte at opplysningene som er registrert om vedkommende er korrekte.[194]

Dersom opplysninger om den enkelte i register over digital kontaktinformasjon og reservasjon ikke har blitt oppdatert eller bekreftet at er korrekte de siste 18 månedene, skal opplysningene ikke brukes til å varsle vedkommende etter § 8 tredje ledd.

§ 33 *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 Det sentrale folkeregister.[195]

§ 34 *Lagring av opplysninger*

Den registrerte kan slette opplysninger om seg i register over digital kontaktinformasjon og reservasjon. For øvrig kan opplysninger i register over digital kontaktinformasjon og reservasjon oppbevares i ubegrenset tid.[196]

---

[193] «Andre opplysninger» kan for eksempel være sertifikatinformasjon for kryptering, språkpreferanser mv.

[194] Den registrerte bør med jevne mellomrom oppfordres til å oppdatere eller bekrefte at de registrerte opplysningen er korrekte. Det fremgår av bestemmelsen at dette bør skje minst to ganger i året. Kontaktregisteret legger i første omgang (per 2014) opp til at det skal skje hvert kvartal. Bestemmelsen angir ingen reaksjon overfor den registrerte dersom denne ikke følger oppfordringen. Kravet til oppdatert digital kontaktinformasjon i tredje ledd innebærer imidlertid i praksis at forvaltningen ikke kan kommunisere digitalt med de som ikke følger oppfordringen om å oppdatere eller bekrefte at kontaktinformasjonen er korrekt.

[195] Med kobling menes nødvendige oppslag i andre registre for å sikre at de registrerte opplysningene er korrekte og oppdaterte. Opplysninger i registeret må blant annet kontrolleres slik at opplysninger om døde personer fjernes fra registeret og for kontroll av fødselsnumre og d-numre.

[196] Den registrerte vil kunne slette kontaktinformasjon fra registeret. Dessuten skal opplysningene i registeret slettes når de ikke lenger er nødvendige for å ivareta formålet med registreringen. Oppbevaring i "ubegrenset tid", slik det er angitt i § 34, forutsetter at fortsatt lagring er nødvendig for å oppnå formålet med registreringen. At en innbygger benytter seg av reservasjonsretten mot elektronisk underretning m.v., vil imidlertid ikke i seg selv innebære at kontaktopplysningene må slettes. Reservasjonsstatus må uansett kunne registreres om vedkommende.

§ 35 *Om forholdet til personopplysningsloven og personopplysningsforskriften*

Bestemmelsene i lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven) og forskrift 15. desember 2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften) gjelder for behandlingen av personopplysninger om digital kontaktinformasjon og reservasjon.[197]

Kapittel 8. Diverse bestemmelser

§ 36 *Koordinerende organ*[198]

Kongen kan utpeke et organ som har koordineringsansvar for forvaltningens bruk av sikkerhetstjenester og -produkter ved elektronisk kommunikasjon med og i forvaltningen.[199]

Koordineringsorganet skal utarbeide krav til sikkerhetstjenester og -produkter som anbefales brukt ved elektronisk kommunikasjon med og i forvaltningen.[200] Koordineringsorganet skal også vurdere om tilgjengelige sikkerhetstjenester eller -produkter tilfredsstiller kravene.[201]

Koordineringsorganet kan bestemme at det under tjeneste for forvaltningsorganer kun skal benyttes sertifikater[202] fra sertifikatutstedere[203] som har inngått rammeavtale om

---

[197] Bestemmelsen innebærer blant annet at Datatilsynet fører tilsyn med behandling av personopplysninger og at tilhørende sanksjonsbestemmelser kommer til anvendelse.

[198] Bestemmelsen fastlegger rammene for etablering av et koordineringsorgan for forvaltningens bruk av sikkerhetstjenester og –produkter ved elektronisk kommunikasjon. Se også Veilederen del 1, kapittel 4.8 *Koordinering av forvaltningens bruk av elektronisk kommunikasjon mv*.

[199] Kommunal- og moderniseringsdepartementet er oppnevnt som koordineringsorgan etter denne bestemmelsen, se forskrift 7. oktober 2005 nr. 1117, sist endret (per april 2014) ved forskrift 11. april 2014 nr. 530.

[200] En slik "anbefaling" foreligger i form av, se *Kravspesifikasjon for PKI i offentlig sektor*. Regjeringen besluttet 28. februar 2005, på bakgrunn av et strateginotat av 17. februar 2005 at alle statlige etater som skal benytte PKI er pålagt å følge kravspesifikasjonen. **Feil! Hyperkoblingsreferansen er ugyldig.** Se også brev fra Fornyings- og administrasjonsdepartementet til samtlige statsetater av 20. september 2006. Anbefalinger for sertifikatprofiler er utarbeidet av SEID-prosjektet og gjort til del av kravspesifikasjonen. Dette følger av kravspesifikasjonen, som henviser til SEID. Bruk av elektronisk identitetsbevis (eID) og elektronisk signatur i offentlig sektor er nå samordnet gjennom ID-porten som forvaltes av Direktoratet for forvaltning og IKT (Difi). Det fremgår av Digitaliseringsrundskrivet (H-7/2014), punkt 1.2 *Bruk av nasjonale felleskomponenter* at: «Virksomheten skal ta i bruk ID-porten for digitale tjenester som krever innlogging og autentisering.» Slike føringer er gjenstand for politiske beslutninger og kan endres over tid. Digitaliseringsrundskrivet oppdateres jevnlig.

[201] Denne funksjonen ivaretas i dag i praksis gjennom selvdeklareringsordningen, se forskrift 21. november 2005 nr. 1296 med henvisning til "Kravspesifikasjon for PKI i offentlig sektor".

[202] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9.

[203] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 10.

levering av slike tjenester til forvaltningen eller som er anerkjent av koordineringsorganet.[204]

Koordineringsorganet kan bestemme at det ved elektronisk kommunikasjon med og i forvaltningen bare skal benyttes sertifikater som er oppført på liste publisert i henhold til forskrift 21. november 2005 nr. 1296 om frivillige selvdeklarasjonsordninger for sertifikatutstedere § 11 første ledd.[205]

§ 37 *Overgangsbestemmelse - kobling mot register over digital kontaktinformasjon og reservasjon - bruk av samtykker og varslingsadresser*

Forvaltningsorganer som kobler seg til register over digital kontaktinformasjon og reservasjon, må bruke den kontaktinformasjonen som er registrert om vedkommende i registeret for å sende varsel etter § 8 tredje ledd annet punktum fra de er koblet opp. Alle forvaltningsorganer skal benytte den kontaktinformasjonen som er registrert i register over digital kontaktinformasjon og reservasjon til å sende varsel etter § 8 tredje ledd annet punktum senest fra 1. januar 2016.[206]

Forvaltningsorganer som ikke har koblet seg til register over digital kontaktinformasjon og reservasjoner, kan bare gi forhåndsvarsel og underretning om enkeltvedtak ved bruk av elektronisk kommunikasjon til privatpersoner og enheter som ikke er registrert i Enhetsregisteret, når mottakeren uttrykkelig har godtatt dette og har oppgitt den elektroniske adressen som skal benyttes for slikt formål. 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.[207]

---

[204] Statlige etater som skal ta i bruk PKI er pålagt å benytte *Kravspesifikasjon for PKI i offentlig sektor* (som integrerer SEID sertifikatprofil). Kravspesifikasjonen definerer to sikkerhetsnivåer for personsertifikater og ett sikkerhetsnivå for virksomhetssertifikater. Se også note 201.

[205] Det er truffet slikt vedtak, se brev fra Fornyings- og administrasjonsdepartementet til samtlige statsetater av 20. september 2006.

[206] Første ledd gir overgangsbestemmelser knyttet til § 8 tredje ledd som krever at den digitale kontaktinformasjonen i register over digital kontaktinformasjon og reservasjon benyttes til varsling av privatpersoner og enheter som ikke er registrert i Enhetsregisteret. Ettersom ikke alle forvaltningsorganer vil være koplet til kontaktregisteret fra oppstart, er det behov for, i en overgangsperiode, å kunne benytte annen digital kontaktinformasjon, se § 37 annet ledd.

En konsekvens av plikten til å bruke varslingsadressene registrert i register over digital kontaktinformasjon og reservasjon er at de forvaltningsorganer som ikke er koblet mot registeret innen 1. januar 2016, ikke kan kommunisere digitalt med privatpersoner og enheter som ikke er registrert i Enhetsregisteret. Se også § 37 tredje ledd.

[207] 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.

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 reservasjon. Dette gjelder selv om mottaker i perioden reserverer seg mot elektronisk kommunikasjon, jf. § 9. Den elektroniske adressen som ble innhentet sammen med samtykket kan benyttes så lenge samtykket gjelder.[208]

Denne bestemmelsen gjelder ikke utover 1. januar 2016.

§ 38 *Gjenbruk av personopplysninger i kontaktregisteret tilknyttet ID-porten*

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

Den enkelte skal informeres om utleveringen og om adgangen til å oppdatere opplysningene, samt om adgangen til å reservere seg mot elektronisk kommunikasjon, jf. § 9, og om adgang til å slette kontaktopplysningene.[209]

§ 39 *Ikrafttredelse*

Forskriften trer i kraft 1. juli 2004.[210]

---

[208] Som en konsekvens av annet ledd angir tredje ledd at samtykker avgitt til forvaltningsorganer gjelder i en overgangsperiode selv om mottaker har reservert seg. Mottaker kan etter vanlige regler trekke samtykket tilbake når vedkommende måtte ønske det. Overgangsperioden går ut når forvaltningsorganet er koplet til kontaktregisteret, men senest 1. januar 2016.

[209] I og med at registrering og bruk i kontaktregisteret går ut over det opprinnelige innsamlingsformålet, har departementet som et personvernøkende tiltak stilt krav om den registrerte skal informeres om utleveringen og om adgangen til å reservere seg, og til å rette eller slette opplysningene.

[210] Forskriften avløser en tidligere forskrift av 28. juni 2002 nr. 656 med samme navn. Forskriften har senere gjennomgått endringer særlig når det gjelder underretning om enkeltvedtak (§ 8), reservasjon og reservasjonsregister (§ 9), bruk av fullmektig (§ 10), krav til internkontrollsystem (§ 15) og nytt kontaktinformasjonsregister (kapittel 7).