Veileder for bruk av eID for ansatte i offentlig forvaltning (manus til web)

Veilederen vil publiseres på web i samråd med KDD. Ved transformering til web vil lenker bli lagt til og enkelte redegjørelser vil inntas i faktabokser, nedtrekkbare felt o.l. Det bes tatt hensyn til at veilederen på web vil ha et nokså annet visuelt inntrykk med fokus på brukervennlighet.

Innhold

0 Ingress (banner på forsiden)

Digital samhandling krever at vi på en trygg måte kan bevise hvem vi er på nett og at andre skal ha tillit til det elektroniske identitetsbeviset (eID-en). På samme måte som arbeidstakere tidvis må bevise hvem de er på jobben ved hjelp av mer tradisjonelle identitetsbevis, kan det være et behov for at man identifiserer seg digitalt.

Behovet for identifisering er i mange tilfeller større i en digital sammenheng, ettersom det er vanskelig å knytte en handling eller et utsagn til en person som ikke er synlig eller fysisk til stede. Vi kaller det elektroniske identitetsbeviset for «eID» og vil i denne veilederen informere og gi retningslinjer for hvordan dette bør benyttes av ansatte i offentlig sektor.

1 Innledning (hvordan bruke veilederen)

Denne veilederen gir retningslinjer for bruk av eID for ansatte i offentlig forvaltning. Den inneholder nødvendig informasjon for arbeidsgivere og arbeidstakere, og har en sjekkliste for de viktigste vurderingene som bør gjøres i forbindelse med bruk av eID.

Veilederen tar utgangspunkt i og beskriver den faktiske og rettslige situasjonen slik den er i dag.

Se kapittel 8 for en innledende beskrivelse av hvordan du bør bruke veilederen.

1.1 Formål

Formålet med veilederen er at arbeidsgivere og arbeidstakere skal ha tilgang til oversiktlig informasjon om bruk av eID i offentlig forvaltning. De skal oppleve forholdene rundt bruk av eID i arbeidsforhold som forståelige, og ha tilgang til retningslinjer for de konkrete vurderingene som må foretas. På sikt er det ønskelig å oppnå en mer ensartet praksis og harmonisert forståelse av de arbeidsrettslige og personvernsrettslige spørsmålene bruk av eID reiser.

Veilederen vil si noe om:

• Hvilke regler og krav som gjelder for bruk av eID i offentlig sektor

• Hvilke løsninger som er tilgjengelig som kan dekke behovene, og hva som er forutsetningene for å ta disse løsningene i bruk.

• Arbeidsrettslige problemstillinger:

- Kan bruk av privat eID pålegges arbeidstakeren?
- Kan bruk av ansatt eID pålegges arbeidstakeren?
- Medfører bruk av eID i arbeidet en tilleggsrisiko i forhold til bruk av eID til private formål?
- Hvem bærer de økonomiske kostnadene og hvem har ansvaret for sikkerheten?
- Hva bør eventuelt avtales mellom arbeidsgiver/arbeidstaker?

• Personvernrettslige problemstillinger:

- Definering av roller etter GDPR
- Behandlingsgrunnlag
- Hvilke personopplysninger behandles om den ansatte?

1.2 Hva omfatter veilederen og hva avgrenses det mot?

Veilederen gjelder for offentlig ansatte og arbeidsgivere, men kan også ha relevans for privat næringsliv. Veilederen har fokus på eID-ordninger til fysiske personer, som er selvdeklarert på sikkerhetsnivå betydelig eller høyt. Det vil si MinID, og markedsløsningene Buypass, Commfides og

BankID. I en fellesbetegnelse vil begrepet «privat eID» benyttes om disse løsningene, med mindre annet er spesifisert.

Markedsløsningene tilbyr også særskilte ansatte-løsninger for eID, heretter benevnt «ansatt-eID». Ansatt-eID vil omtales nærmere i kapittel 2.2.2.

Regelverket for eID er teknologinøytralt, og det ikke lenger noe eksplisitt krav om bruk av PKI og sertifikater for å oppnå sterk autentisering. Fortsatt er det vanlig at både privat eID og ansatt-eID benytter et personidentifiserende sertifikat («personlig sertifikat») basert på PKI, men det finnes også løsninger uten sertifikater etter FIDO2-standarden.

Veilederen vil også svare på spørsmål om elektronisk signatur. I mange tilfeller blir vurderingen av sertifikatbaserte eID-ordninger og elektroniske signaturer sammenfallende, ettersom de begge benytter en eID på nivå betydelig eller høyt i forbindelse med henholdsvis autentisering og produksjon av en elektronisk signatur.

Veilederen gjelder ikke oppdragstakere under forvaltningen eller bruk av virksomhetssertifikater og lukkede systemer. Veilederen vil likevel kunne være nyttig for å svare ut tilsvarende problemstillinger utenfor veilederens målområde.

1.3 Begreper – slik de benyttes i veilederen

Autentisering	Handling for å bekrefte identitet. Sterk autentisering innebærer en form for autentisering med flere autentiseringsfaktorer.
Autentiseringsfaktor[1]	En faktor som er bekreftet å være knyttet til en person, og som tilhører en av følgende kategorier: a) «besittelsesbasert autentiseringsfaktor» en autentiseringsfaktor som personen skal bevise at den er i besittelse av, b) «kunnskapsbasert autentiseringsfaktor» en autentiseringsfaktor som personen skal bevise at den har kjennskap til, c) «iboende autentiseringsfaktor» en faktor som er basert på et fysisk attributt hos en fysisk person, og som personen skal bevise at den har.
To-faktorautentisering	En form for autentisering der man benytter to forskjellige autentiseringsfaktorer i kombinasjon. Datatilsynet benytter gjerne begrepet «sterk autentisering». I veilederen for identifikasjon og sporbarhet benyttes også begrepet «To-faktorløsning».
eIDAS-forordningen	eIDAS (Forordning (EU) nr. 910/2014) er et europeisk regelverk som skal sikre et velfungerende indre marked og oppnå et tilfredsstillende sikkerhetsnivå for elektronisk identifikasjon (eID) og tillitstjenester på tvers av EU/EØS-land. Forordningen er inntatt i norsk lov. eIDAS er under revisjon i EU per. 31. august 2022.

[1] https://lovdata.no/static/NLX3/32015r1502.pdf

Lov om elektroniske tillitstjenester	Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (LOV-2018-06-15-44). Loven gjennomfører eIDAS i norsk rett og etablerer blant annet selvdeklarasjonsordninger og tilsyn.
Selvdeklarasjonsforskriften	Forskrift om selvdeklarasjon av ordninger for elektronisk identifikasjon med hjemmel i Lov om elektroniske tillitstjenester.
Identifikasjonsnivåforskriften	Kommisjonens gjennomføringsforordning (EU) 2015/1502 av 8. september 2015 til eIDAS-forordningen, jf. forskrift 21. november 2019 nr. 1577 om tillitstjenester for elektroniske transaksjoner § 6
eID	Elektronisk ID som brukes for autentisering på nett, for å bevise at du er den du er. Det kan sammenlignes med mer tradisjonelle legitimasjonsbevis som for eksempel førerkort, bankkort med bilde, og pass. eIDAS har gitt følgende definisjon av eID: «*elektronisk identifikasjon» en prosess som omfatter bruk av personidentifikasjonsdata i elektronisk form som på en entydig måte representerer enten en fysisk eller juridisk person, eller en fysisk person som representerer en juridisk person»*, jf. Artikkel 3 (1).[2]
Privat eID	I denne veilederen brukes begrepet om eID-er på sikkerhetsnivå betydelig og høyt som ikke utelukkende er ment for bruk i arbeid.
Ansatt-eID	I denne veilederen brukes begrepet «ansatt-eID» om eID-er på sikkerhetsnivå betydelig og høyt som er utstedt etter arbeidsgivers initiativ og som er ment for bruk i arbeid. Se nærmere beskrivelse i kapittel 2.2.2.
eID-ordninger	*«ordning for elektronisk identifikasjon» et system for elektronisk identifikasjon der det utstedes elektroniske identifikasjonsmidler til fysiske eller juridiske personer, eller til fysiske personer som representerer juridiske personer»*, jf. eIDAS Artikkel 3 (4). Ofte benyttes begrepene «eID-løsninger» og «eID-ordninger» om det samme.
eID-leverandør	En juridisk person som tilbyr og utsteder eID-løsninger, slik som Commfides, Buypass og Vipps (BankID).
Tjenesteeier	I denne veilederen brukes begrepet om eier av en nettbasert tjeneste som krever innlogging med eID, for eksempel Altinn, Lånekassen og Skatteetaten.
Tjenestebruker/bruker	En fysisk person som benytter seg av elektronisk identifikasjon eller en tillitstjeneste. I denne veilederen vil det ofte være det samme som den ansatte.

[2] https://lovdata.no/static/NLX3/32014r0910.pdf

HelseID	Felles påloggingsløsning for helse- og omsorgssektoren som legger til rette for at helsepersonell og andre ansatte kan få engangspålogging med én elektronisk ID (eID) i hele helsetjenesten, og for at sektoren lettere kan dele data og dokumenter.
ID-porten	ID-porten er en felles innloggingsløsning for flere offentlige tjenester og aksepterer eID-ordninger som innloggingsmetode.
Innrullering	Utlevering av en ny eID til en bruker. Begrepet innrulling inkluderer utlevering, aktivering og utstedelse i en sammenhengende prosess.
BankID	BankID er en kommersiell eID på høyt sikkerhetsnivå, som leveres av Vipps.
Buypass	Kommersiell eID-leverandør som tilbyr flere eID-ordninger på betydelig og høyt sikkerhetsnivå.
Commfides	Kommersiell leverandør som tilbyr eID på høyt sikkerhetsnivå.
Feide	Feide er den nasjonale løsningen for innlogging og datadeling i utdanning og forskning. Feide leveres av kunnskapssektorens tjenesteleverandør (Sikt) som samarbeider med Utdanningsdirektoratet om forvaltningen av tjenesten. Feide tilbyr også sterk autentisering for løsninger tilknyttet ansatte. Feide har ikke selvdeklarert sin eID-løsning på et angitt sikkerhetsnivå.
PKI	Public Key Infrastructure (PKI) er et rammeverk for bruk av digitale sertifikater over datanettverk. PKI benytter asymmetriske kryptografiske nøkkelpar som hemmeligheter (en offentlig nøkkel og en privat nøkkel). PKI har mange anvendelsesområder, deriblant eID. For eID har de private nøklene tradisjonelt blitt beskyttet i en HSM modul, slik som smartkort eller SIM-kort.
Smartkort	Et kort med integrert mikroprosessor. Kortene har mange bruksområder, og teknologien benyttes stadig oftere blant annet på grunn av fleksibiliteten og sikkerhetsmulighetene. Blir også ofte kalt for PKI-kort i sammenheng med eID-ordninger. Da oppbevares den private nøkkelen på kortet, og beskyttes normalt av en pinkode. Andre typer bærere av eID er for eksempel SIM-kort i mobiltelefon, FIDO2-nøkkelbærere og USB-pinner.
Sikkerhetsnivå	Sikkerhetsnivåene[3] angir ulike grader av tillit til at påstanden om identitet, i en elektronisk kommunikasjon, er korrekt.

[3] Forskrift om tillitstjenester for elektroniske transaksjoner: https://lovdata.no/pro/forskrift/2019-11-21-1577/§6

	Hvilket sikkerhetsnivå som skal kreves, beror på risikoen i tjenesten, herunder hvilke konsekvenser identifikasjonssvikt vil ha, samt trusselbildet for den aktuelle tjeneste mv[4]. Det er virksomheten som eier tjenesten som bestemmer hvilket sikkerhetsnivå tjenesten deres skal ha. eIDAS er gjennomført i lov om elektroniske tillitstjenester m/forskrifter. Sikkerhetsnivåene er der kategorisert som «lavt», «betydelig» og «høyt»[5].
Single-sign-on (SSO)	Omtales også som «engangspålogging». Gir brukeren muligheten til å få tilgang til flere tjenester ved å kun logge seg inn én gang, f.eks. gjennom ID-porten. Identifikasjonssystem på nettsider som lar brukere verifisere seg ved å bruke andre pålitelige nettsider. Se nærmere beskrivelse i kap. 2.2.1.2.
Kjernejournal	Nasjonal e-helseløsning, en samhandlingsløsning etablert for å øke pasientsikkerheten. I den enkeltes kjernejournal er et utvalg viktige opplysninger gjort tilgjengelige for helsepersonell med tjenstlig behov, uavhengig av hvor pasienten tidligere har mottatt helsehjelp. Kjernejournal forutsetter bruk av eID på sikkerhetsnivå «høyt».
Personlig sertifikat	I denne veilederen benyttes begrepet om et personidentifiserende sertifikat som anvendes i både private og ansatte eID-ordninger for å entydig identifisere en fysisk person.
FIDO2	En åpen standard utviklet av FIDO-alliansen[6], som blant annet kan benyttes for passordfri sterk autentisering.

[4] Identifikasjonsnivåforskriften: https://lovdata.no/pro/eu/32015r1502
[5] https://lovdata.no/forskrift/2019-11-21-1577/§6
[6] FIDO-alliansen er en industrisammenslutning som utvikler autentiseringsstandarder

2 Hva er eID?

På samme måte som for et fysisk ID-bevis, benyttes en eID for å bekrefte at en person er den vedkommende utgir seg for å være. Det kan sammenlignes med mer tradisjonelle legitimasjonsbevis som for eksempel førerkort, bankkort med bilde, og pass. Brukernavn og passord til en tjeneste er en type elektronisk identitet.

Det sentrale prinsippet bak ditt elektroniske identifikasjonsmiddel (eID) er at du skal kunne bevise via digitale løsninger at du er en bestemt fysisk person. eID-en inneholder personidentifiserende opplysninger og den tillater deg å føre bevis for at du er rette eier av denne identiteten. Beviset ditt kan være at du kjenner til en hemmelighet som forutsetningsvis ingen andre kan (for eksempel et passord). Ved å kjenne til passordet kan andre være rimelig sikker på at du er den du utgir deg for å være.

Ved innlogging i løsninger som krever høy sikkerhet, er det ønskelig at andre skal være *så sikker som mulig* på din påståtte identitet. For å styrke tilliten til identitetspåstanden kan vi ta i bruk gjenstander som eID-leverandøren har knyttet opp til din eID. Dette er gjenstander som gjerne ble gitt til deg i forbindelse med utstedelse av eID-en, og som det må antas at bare du har kontroll over, for eksempel en kodebrikke, et smartkort eller en mobiltelefon. Når du logger inn i en tjeneste kan du bli bedt om å bekrefte at disse gjenstandene fortsatt er i dine hender. For eksempel ved at du skriver inn en kode på gjenstanden. Gjenstanden vil da kommunisere med innloggingsløsningen og sannsynliggjør at den fortsatt er i dine hender.

Ved bruk av passord og en gjenstand har du ført to ulike bevis som samlet gir stor tillit til at din identitetspåstand stemmer. En eID som bruker slik «to-faktorautentisering» (*noe du vet* og *noe du har)*, kategoriseres gjerne som *sikre*.[7]

Det er ulike aktører som tilbyr slike eIDer, de omtales gjerne som eID-leverandører eller eID-utstedere. Aktørene påser at utstedelse av deres eIDer følger et system som oppfyller bestemte lovfestede krav ut i fra hvilket sikkerhetsnivå de ønsker å tilby. Et slik system kalles eID-ordninger.

Det er de selvdeklarerte eID-ordningene som oppfyller lovfestede krav for de to høyeste sikkerhetsnivåene vi skal se nærmere på i denne veilederen. I Norge er det selvdeklarert seks ulike eID-ordninger: BankID, BankID på mobil, Buypass ID på smartkort, Buypass ID i mobil, Commfides eID og MinID.[8]

Pålitelige eID-er er en viktig forutsetning for digital kommunikasjon og samhandling med offentlig sektor. eID-ene kan benyttes til en rekke forskjellige gjøremål og tjenester, som for eksempel elektronisk signering eller innlogging til en tjeneste.

Det er flere aktører med ulike roller i «eID-økosystemet». For en ansatt er det nyttig å kjenne til hvem de ulike aktørene er, og hvilken rolle de har:

1. Arbeidsgiver er ansvarlig for arbeidsoppgaver som forutsetter bruk av eID,

---

[7] Det finnes også en tredje type autentiseringsfaktor; Noe du er. Dette kan for eksempel være ansiktsgjenkjenning eller annen bruk av biometriske kjennetegn. Du trenger kun 2 av de 3 nevnte autentiseringsfaktorene for å være en løsning med «to-faktorautentisering». I dag oppnås to-faktorautentisering ofte med autentiseringsfaktorene «noe du vet» og «noe du har».

For en nærmere beskrivelse av eID vises det til veilederen for identifikasjon og sporbarhet, og overskriftene «Hva er identifikasjon?» og «Hva er autentisering?». Lenke: Veileder for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor | Digdir

[8] Elektronisk identifikasjon (eID) - Nkom

2. Tjenesteeier administrerer den tjenesten du ønsker å benytte og krever at du identifiserer deg.
3. ID-porten er en fellesløsning som tjenesteeierne kan benytte for å identifisere deg med ulike eID-er.
4. eID-leverandørene er de som har utstedt eID-en til deg, og som foretar en ID-kontroll av deg ved utstedelse av eID og når eID-en brukes.

2.1 Beskrivelse av sikkerhetsnivåer

Hvert sikkerhetsnivå har ulike krav som stilles til identitetskontrollen og til utlevering av eID-ene, og til hvilke autentiseringsfaktorer som benyttes i bruksfasen. Kommunal- og distriksdepartementet har sammen med Digitaliseringsdirektoratet utarbeidet en egen veileder for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor. Les mer i «*Veileder for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor*» og overskriften «Definisjon av sikkerhetsnivåer for identifikasjon».

I korthet er det tre ulike sikkerhetsnivåer som er kategorisert som hhv. «lavt», «betydelig» og «høyt». Forskjellen på disse nivåene ligger i hvilke tekniske og regulatoriske krav som må være oppfylt for at eID-en skal ansees å ha «oppnådd» et bestemt sikkerhetsnivå.

BankID, Buypass og Commfides leverer eID-ordninger på sikkerhetsnivå «høyt». Disse aktørene er også omtalt som «eID-leverandører» eller «markedsløsningene».

eID-leverandørene må bestemme hvilket sikkerhetsnivå de ønsker å oppfylle. Deretter kan de bruke kravsettet til det aktuelle sikkerhetsnivået og sørge for at deres løsning er i overenstemmelse med alle relevante krav. Dersom eID-leverandøren mener at alle krav er oppfylt, kan de selvdeklarere eID-ordningen på det aktuelle sikkerhetsnivået. Dette følger av Forskrift om selvdeklarasjon av ordninger for elektronisk identifikasjon (selvdeklarasjonsforskriften).[9]

At en løsning er selvdeklarert innebærer at de publiseres på en liste over selvdeklarerte løsninger administrert av og ført tilsyn med av Norsk kommunikasjonsmyndighet (Nkom)[10]. Listen gir en henvisning til det selvdeklarerte sikkerhetsnivået. Dette gjør at utenforstående kan ha tillit til eID-ene.

Tjenesteeiere må velge hvilket sikkerhetsnivå de mener er nødvendig for å bruke deres tjeneste og eventuelt stille krav om bruk av eID, herunder hvilke eID-er som aksepteres. Dette følger av eForvaltningsforskriften § 4. Tjenesteeier må gjøre en vurdering av risikoen for sikkerhetsbrudd og konsekvenser av dette, og på den bakgrunn velge et passende sikkerhetsnivå. Som veiledning kan en se til beskrivelsen av sikkerhetsnivåene i «*Veileder for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor*», særlig punktet om «Veiledning for valg av sikkerhetsnivå for identifikasjon» og underpunktet «Praktiske eksempler på tjenester som kan benytte de forskjellige sikkerhetsnivåene».

2.2 Hva kan eID brukes til?

En elektronisk ID kan benyttes til flere formål, deriblant for å identifisere seg digitalt eller for å produsere en elektronisk signatur. I punkt 4.4.1 er det en illustrasjon av hvordan eID brukes i offentlige tjenester.

[9] FOR-2019-11-21-1578, https://lovdata.no/dokument/SF/forskrift/2019-11-21-1578
[10] www.nkom.no

2.2.1 Autentisering og innlogging i tjenester

2.2.1.1 ID-porten og Ansattporten

ID-porten muliggjør innlogging til offentlige digitale tjenester og støtter i dag innlogging med autentisering med eID-er på de to høyeste sikkerhetsnivåene. MinID er på det nest høyeste nivået (betydelig), mens eID-ene fra BankID, Buypass og Commfides er på det høyeste nivået (høyt).

Våren 2022 startet Digitaliseringsdirektoratet med pilotering av Ansattporten. Det er en innloggingsportal på lik linje med ID-porten, men knytning til ulike autorisasjonskilder som for eksempel Altinn, som kan gi arbeidstaker en rolle basert på sitt arbeidsforhold. I Ansattporten blir slik knytning mellom arbeidsgiver og person gjort etter at vedkommende er autentisert med en eID-løsning.

2.2.1.2 Nærmere om Single-sign-on

ID-porten tilbyr i dag Single-sign-on («engangspålogging»). I denne sammenhengen betyr det at du bruker én innlogging til å logge inn på flere ulike tjenester. Engangspålogging er effektiviserende ved at brukerne unngår å måtte autentisere seg flere ganger for tilgang til ulike tjenester. I et informasjonssikkerhetsperspektiv kan det derimot ansees som en større risiko at brukeren får tilgang til flere tjenester i en og samme innloggingsøkt. Bruk av engangspålogging handler derfor om å finne en balanse, mellom brukervennlighet (færrest mulig innlogginger) og sikkerhet. Tjenesteeier bør foreta en vurdering av behovet for engangspålogging, og kan be om å deaktivere funksjon for engangspålogging dersom det ikke er ønskelig.

Arbeidsgiver bør også være kjent med risikoen, og om nødvendig gjennomføre risikoreduserende tiltak. Av effektivitetshensyn er det i mange tilfeller ønskelig å beholde engangspålogging, og da kan risikoen reduseres ved informasjon, opplæring og oppfølging av de ansatte. Et eksempel kan være tydelige retningslinjer som sier at ansatte må logge av en økt i det de forlater arbeidsplassen, ikke helt ulikt at ansatte skal logge av eller låse en PC.

En eventuell fremtidig løsning i Ansattporten vil også kunne redusere den potensielle risikoen, ved at den ikke gir ansatte tilgang til tjenester en person har tilgang til som privatperson.

2.2.2 Nærmere om «ansatt-eID» og «privat eID»

Markedsleverandørene leverer i dag to ulike produkter innenfor personlige eID-er. Det vi i denne veilederen kaller «privat eID» og «ansatt-eID».

Begrepene privat eID og ansatt-eID er ikke legaldefinert, og veilederen har gitt de et eget innhold. I det følgende vil begrepene forklares slik de benyttes i veilederen.

«Privat eID» er nok det de fleste tenker på når de hører ordet «eID». Dette er en eID som brukeren gjerne har anskaffet uavhengig av et arbeidsforhold fra enten Buypass, Commfides, BankID eller MinID. Dette er en eID på sikkerhetsnivå betydelig eller høyt som ofte benyttes til private formål, men som i mange tilfeller også benyttes i arbeidssammenheng.

Begrepet «ansatt-eID» benyttes i denne veilederen om eID-ordninger fra Buypass, Commfides og BankID som er utstedt etter arbeidsgivers initiativ og som i utgangspunktet er ment for bruk i arbeid. Hvorvidt eID-ene er begrenset til bruk i arbeidet vil fremgå av avtalen mellom eID-leverandøren og avtaleparten somkan være arbeidsgiver og/eller arbeidstaker. I tillegg vil en ansatt-eID ofte inneholde informasjon som kan knytte den ansatte til en virksomhet.

I likhet med privat eID benytter ansatt-eID normalt et personlig sertifikat i bunn. Personopplysningene som ligger i det personlige sertifikatet som benyttes i eID-ene vil derfor ofte være de samme – uavhengig av om det er en privat eID eller ansatt-eID. Ved begge løsninger blir du

identifisert med et personidentifiserende sertifikat som er knyttet til deg personlig.[11] I noen eID-ordninger suppleres det personlige sertifikatet med informasjon om virksomheten du er ansatt i, men ofte vil ikke dette være nødvendig fordi tjenesten du logger inn i håndterer koblingen mellom deg og virksomheten. Se mer om de konkrete opplysningene som behandles i kapittel 4.4.

En ansatt-eID trenger dermed *ikke* å inneholde et «*virksomhetssertifikat*» i den betydning at du identifiserer deg som en virksomhet (juridisk person) eller som ansatt i en virksomhet.

Selv om ansatt-eID i noen tilfeller ikke vil ha noen særlige tekniske forskjeller som skiller den fra en privat eID, kan ansatt-eID oppleves av brukeren som noe adskilt fra sin private eID. Dette fordi ansatt-eID ofte er anskaffet eller betalt av arbeidsgiver, administreres via arbeidsgiver, og gjerne skiller seg visuelt fra den ansattes private eID. Arbeidsgiver vil også kunne ha utvidede rettigheter og forpliktelser når det gjelder utstedelse og administrasjon av eID til sine ansatte, slik som revokering (tilbakekalling) av eID-ene. Arbeidsgiver vil med andre ord ha en mer tydelig og definert rolle for håndteringen av en ansatt-eID.

Arbeidsgiver kan vurdere tiltak for at en «privat eID» skal være mer lik en «ansatt-eID» for arbeidstaker. For eksempel ved å påta seg et betalingsansvar for utstyret som benyttes i forbindelse med den private eID-en. I vurderingen av om en eID-løsning kan tas i bruk i offentlig forvaltning er det ikke avgjørende om det kalles «privat eID» eller en «ansatt-eID». Det må foretas en konkret vurdering i hvert enkelt tilfelle, se mer om denne vurderingen i kap. 4-6. Selv om det må bero på en konkret vurdering, vil det normalt ansees å være innenfor styringsretten å pålegge bruk av en eID som administreres, anskaffes og betales av arbeidsgiver, hvilket ofte er beskrivelsen av en ansatt-eID. Det forutsettes at den ansatte er gitt tilstrekkelig informasjon, og at øvrige vilkår for bruken er oppfylt, se sjekklisten i kapittel 7.

- Les mer om styringsretten i kapittel 5.
- Les mer om hvordan det er hensiktsmessig å tilrettelegge for bruk av eID i arbeidet, herunder gjennom dialog og avtale om rammene for anskaffelsen og bruken, se kap. 5.2 og 5.3.

Arbeidsgiver bør også være oppmerksom på at en privat eID normalt ikke kan begrenses til bruk i arbeidet. Motsatt vil en ansatt-eID som er utstedt til bruk i forvaltningen, normalt kunne begrenses til slik bruk.[12] Dersom arbeidsgiver ønsker å anskaffe en eID som den ansatte skal benytte i forvaltningen må det innhentes samtykke fra den ansatte før utstedelse av eID-en.[13] Dette kan skje i forbindelse med at man må informere og involvere den ansatte i anskaffelsesprosessen, se også kapittel 4.

Det finnes flere ulike eID-er, både innenfor private eID- og ansatt-eID-ordninger. Det er opp til virksomheten og de ansatte å vurdere hvilken løsning som er best egnet i deres konkrete tilfelle.

2.2.3 Elektronisk signatur

Elektronisk signatur er en løsning for å signere digitalt. Slik som for håndskrevne signaturer kan det benyttes til å signere dokumenter og være med på å bevise at partene hadde til hensikt å forplikte

[11] (nedtrekkbart felt til web) I praksis er begrepsbruken noe inkonsekvent. Begrepene «personlig sertifikat» og «personidentifiserende sertifikat» brukes om det samme; Et sertifikat med informasjon som kan identifisere en fysisk person. Også begrepet «personsertifikater» benyttes, blant annet i Veileder til eForvaltningsforskriften: https://www.regjeringen.no/contentassets/be9697d7e68041e29ffca576c331b4b0/efvf_del3.pdf

[12] eForvaltningsforskriften § 19

[13] eForvaltningsforskriften § 18

seg til en avtale. Ved bruk av elektronisk signatur i ansattforhold må man også være oppmerksom på at innehaver av eID-en, altså personen som har signert dokumentet, kan representere en virksomhet.

I prinsippet kan signaturen din være like bindende om den er skrevet for hånd eller avgitt elektronisk, og en signatur skal ikke forskjellsbehandles utelukkende fordi den er elektronisk, jf. eIDAS artikkel 25 (1). Det finnes derimot ulike grader av sikkerhet i en elektronisk signaturløsning, altså hvor sikker du kan være på at noe er elektronisk signert av rette vedkommende.

En elektronisk signatur som innebærer bruk av en eID på nivå betydelig eller høyt regnes normalt som sikker, og vil typisk oppfylle krav til notoritet og sporbarhet samtidig som den bidrar til å hindre at dokumentet kan endres i etterkant. I dag benyttes gjerne en eID for å signere et dokument sikkert i en signaturløsning. Både eID-ene fra Commfides, Buypass og BankID kan benyttes for å produsere en signatur.[14] For nærmere om begrepet 'sporbarhet', se Veileder for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor.

Virksomheten bør ta med i sin behovsanalyse hvilket konkret behov de har for elektronisk signering, og hvilke eID-ordninger som kan brukes for å gjennomføre signeringen.

Ettersom en elektronisk signatur gjerne forutsetter bruk av eID fra markedsløsningene – så vil vurderingene i denne veilederen langt på vei være sammenfallende mellom bruk av eID til innlogging/autentisering og til elektronisk signering.

2.3 Hvordan får du en eID?

En eID på sikkerhetsnivå høyt kan anskaffes gjennom private eID-leverandører som BankID, Buypass eller Commfides. Ved førstegangsutstedelse må brukeren per i dag møte personlig og vise frem gyldig legitimasjon. I praksis gjennomføres ID-kontroll gjennom en tjeneste fra Posten, i bankfilial eller via arbeidsplassen. Det er mulig å få utstedt flere eID-er til ett og samme fødsels- eller d-nummer, men koblingen mot identiteten skal være entydig. eID-ene vil ofte vil være bundet til en bestemt autentiseringsfaktor, slik som en bestemt mobiltelefon, en chip i et smartkort eller et SIM-kort.

Figur 1: Utstedelse av en eID på sikkerhetsnivå høyt

Selv om eID er enkelt å få utstedt for de fleste, er det likevel enkelte brukergrupper som har utfordringer. Det kan for eksempel være utfordringer med å få utstedt eID på nivå høyt til utenlandske borgere som følge av krav til identitetskontrollen og knytning til norsk identitetsnummer. Disse begrensningene i hvilke brukergrupper som kan få eID på nivå høyt, bør arbeidsgiver ha med seg ved valg av tjeneste.

[14] I Veileder for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor er det forklart hvordan elektronisk signatur kan sikre sporbarhet for godkjenning av et dokument. Det henvises dit for ytterligere informasjon.

2.3.1 Kort om virksomhetssertifikater

Denne veilederen omtaler ikke autentisering av virksomheter. Arbeidsgiver gjøres likevel oppmerksom på at det finnes såkalte virksomhetssertifikater som er knyttet til organisasjonsnummer i stedet for den enkelte ansatte. Merk at ikke alle tjenester støtter bruk av virksomhetssertifikat og krever personlig innlogging. Se Altinn: https://www.altinn.no/hjelp/profil/avanserte-innstillinger/hva-er-virksomhetssertifikat/

Digitaliseringsdirektoratet har en egen veileder for virksomhetsautentisering, som finnes her https://www.digdir.no/datadeling/veileder-virksomhetsautentisering/2435

2.4 Utfordringer ved bruk av eID i arbeidsforhold i dag – Funn fra behovsanalysen

I forbindelse med arbeidet med ny strategi for eID i offentlig sektor[15] er det gjennomført behovsanalyser som blant annet omhandler bruk av eID i arbeidsforhold. Behovsanalysene viser at noen brukere reagerer på at de må benytte sin egen private eID og mobiltelefon for å kunne autentisere og logge seg inn i jobbsammenheng, og viser til at det er prinsipielt utfordrende om ansatte selv må bære kostnadene for å kunne utføre arbeidet sitt, slik som gjerne forutsettes ved bruk av egen mobiltelefon eller annet utstyr eid av arbeidstakeren.

Det oppleves også utfordringer knyttet til signering av avtaler i forbindelse med tjeneste- og varekjøp i offentlig sektor. I dag gjennomfører enkelte ansatte i offentlig sektor signering av avtaler med privat eID, altså som privatperson, uten at det er en direkte knytning til rollen den offentlige ansatte har i virksomheten.

I andre sammenhenger har det vært stilt spørsmål om bruk av privat eID innebærer en økt risiko for den ansatte som privatperson. For eksempel om den ansatte er personlig ansvarlig ved tap av privat utstyr, eller dersom eID-en blir utsatt for misbruk. Det er også et spørsmål om personopplysningsbehandlingen, herunder hvilke opplysninger som behandles og av hvem.

Formålet med denne veilederen er å gi informasjon og veiledning slik at virksomhetene kan møte disse utfordringene på best mulig måte.

[15] Forslag til ny strategi for eID i offentlig sektor ble sendt på alminnelig høring 21. juni 2022

3 Regler og krav for bruk av eID

3.1 Lover og regler som gjelder spesielt for eID

3.1.1 eIDAS-forordningen[16] (eIDAS)

eIDAS er en EU-forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det europeiske indre marked, vedtatt i 2014. Norge har gjennomført eIDAS-forordningen i norsk rett ved Lov om elektroniske tillitstjenester i 2018. eIDAS-forordningen gir felles regler for eID i hele Europa. Hovedformålet med eIDAS er å harmonisere regelverket i EU, og dermed legge til rette for bruk av eID over landegrenser.

3.1.2 Lov om elektroniske tillitstjenester[17]

Lov om elektroniske tillitstjenester med forskrifter regulerer eID og andre tillitstjenester. Loven gjennomfører eIDAS i norsk rett og etablerer blant annet selvdeklarasjonsordninger og tilsyn. Gjennomføringsrettsakter til eIDAS er fastsatt som forskrift til lov om elektroniske tillitstjenester[18]

3.1.3 Selvdeklarasjonsforskriften[19] og identifikasjonsnivåforskriften[20]

I forbindelse med gjennomføringen av eIDAS i norsk rett, ble det utarbeidet en forskrift om selvdeklarasjon av ordninger for elektronisk identifikasjon med hjemmel i Lov om elektroniske tillitstjenester (Selvdeklarasjonsforskriften). Den beskriver krav for å oppfylle norske sikkerhetsnivå.

Selvdeklarasjonsforskriften gjenbruker kravsettet fra identifikasjonsnivåforskriften med noen norske tilpasninger, hvor det mest sentrale er kravet til entydig knytning til norsk fødsels- og d-nummer (nasjonal identifikator).

Identifikasjonsnivåforskriften er Kommisjonens gjennomføringsforordning (EU) 2015/1502 til eIDAS-forordningen. Forskriften definerer de tre sikkerhetsnivåene: «Lavt», «betydelig» og «høyt» og beskriver hvilke krav som må være oppfylt for å oppnå det aktuelle nivået. Den enkelte eID-leverandør avgjør hvilket sikkerhetsnivå de ønsker å oppnå for deretter å kunne selvdeklarere sin eID-løsning på dette nivået. Se kapittel 2.1.

3.1.3.1 Veileder for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor[21]

Nytt regelverk for eID og elektroniske tillitstjenester gjorde det nødvendig å revidere Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, samt oppheve Kravspesifikasjon for PKI i offentlig sektor. Veileder for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor skal nå bidra med veiledning i overenstemmelse med nytt regelverk for eID.

3.2 Lover og regler som påvirker bruk av eID i offentlig forvaltning

3.2.1 Arbeidsmiljøloven

Arbeidsmiljøloven av 2005 (aml.) har som formål å sikre et arbeidsmiljø som gir grunnlag for blant annet trygge ansettelsesforhold. Arbeidsmiljøet skal holde en velferdsmessig standard som til enhver tid er i samsvar med den teknologiske og sosiale utvikling i samfunnet, gjøre tilpasninger for den

[16] https://lovdata.no/static/NLX3/32014r0910.pdf (norsk oversettelse)
[17] https://lovdata.no/dokument/NL/lov/2018-06-15-44
[18] https://lovdata.no/dokument/SF/forskrift/2019-11-21-1577
[19] https://lovdata.no/dokument/SF/forskrift/2019-11-21-1578
[20] Forskrift om tillitstjenester for elektroniske transaksjoner § 6
[21] https://www.digdir.no/samhandling/veileder-identifikasjon-og-sporbarhet-i-elektronisk-kommunikasjon-med-og-i-offentlig-sektor/2992

enkelte arbeidstaker ut ifra konkrete behov, og bidra til et inkluderende arbeidsliv, jf. formålsbestemmelsen § 1-1.

Selve anskaffelsen og bruken av eID er ikke konkret regulert i arbeidsmiljøloven, men mer overordnede regler om informasjon til ansatte, slik som i arbeidsmiljøloven § 4-2, er av betydning. I tillegg danner loven et viktig bakteppe. Blant annet vil den ovennevnte formålsangivelsen og forskriftsbestemmelser med hjemmel i loven kunne påvirke de rettslige vurderingene for bruk av eID i arbeidssammenheng.

3.2.1.1 Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale

Arbeidsmiljøloven gir hjemmel til mer detaljerte bestemmelser i forskrift om bruk av elektronisk utstyr på arbeidsplassen. Deriblant forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale som er hjemlet i aml. § 9-5.

Forskriften gir arbeidsgiver en innsynsrett på nærmere bestemte vilkår i arbeidstilknyttet epostkasse og annet elektronisk utstyr som omfattes av forskriften. Begrepet «utstyr» må trolig forstås vidt, slik at ulike former for kommunikasjonsløsninger omfattes, deriblant informasjon som er lagret i applikasjoner.

Forskriften omfatter ikke eID-en i seg selv, men kan i konkrete tilfeller omfatte utstyr der informasjon om eID og bruken av denne er lagret.

3.2.2 Statsansatteloven

Statsansatteloven av 2017 gjelder der staten er arbeidsgiver og supplerer reglene i arbeidsmiljøloven for ansatte i statlig sektor. Arbeidsforholdet til ansatte i kommunal og privat sektor er fullt ut regulert i arbeidsmiljøloven.

3.2.3 Personopplysningsloven og GDPR

Personopplysningsloven trådte i kraft 20. juli 2018, og gjennomfører EUs personvernforordning i norsk rett (General Data Protection Regulation – GDPR). GDPR gir en rekke grunnleggende prinsipper for behandlingen av personopplysninger,[22] som også gjelder for arbeidsgivers behandling av ansattes personopplysninger.

Arbeidsgiver kan kun behandle personopplysninger om ansatte for et uttrykkelig angitt formål som er saklig begrunnet i virksomheten, og det må foreligge et rettslig grunnlag for den aktuelle bruken av personopplysningene.

Arbeidsgiver må utøve styringsretten i overensstemmelse med personopplysningslovens regler. Dersom behandlingen av personopplysninger ikke er tillatt etter GDPR, så vil arbeidsgiver ikke kunne påberope seg styringsretten som grunnlag for pålegg rettet mot den ansatte.

3.2.4 Forvaltningsloven

Forvaltningsloven gir generelle regler om behandlingsmåten i den offentlige forvaltning, deriblant elektronisk kommunikasjon med og i forvaltningen. Forvaltningsloven er hjemmelslov for eForvaltningsforskriften og setter rammene for forskriftens virkeområde.

3.2.4.1 eForvaltningsforskriften[23]

eForvaltningsforskriften gjelder i likhet med forvaltningsloven både statlig, kommunal, regional og lokal forvaltning, og kommer til anvendelse med mindre annet er bestemt i lov eller i medhold av lov.

[22] jf. GDPR art. 5

[23] *Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)*, tilgjengelig her.

eForvaltningsforskriften fastlegger rammene for elektronisk kommunikasjon i forvaltningen og mellom forvaltningen og private parter. Veileder til eForvaltningsforskriften finnes på regjeringen.no.

3.2.5 Skadeerstatningsloven

Skadeerstatningsloven av 1969 har regler om erstatning for skade på person eller ting. Den inneholder også regler for arbeidsgivers ansvar for arbeidstaker, jf. § 2-1. Regelen er omtalt nærmere i kapittel 4.3.

3.3 Regler som kan ha overføringsverdi, herunder bruk av telefoni og elektroniske kommunikasjonstjenester for statlige ansatte

Statens personalhåndbok av 2022 gir retningslinjer til statlige arbeidsgivere, og regulerer adgangen virksomhetene har til å utstyre de ansatte med elektroniske kommunikasjonstjenester. Det vises herunder til administrative bestemmelser om elektroniske kommunikasjonstjenester, jf. pkt. 10.2.2.

Der den konkrete eID-en forutsetter anskaffelse av eller bruk av kommunikasjonsutstyr slik som mobiltelefon, så kan det være relevant se hen til reglene i Statens Personalhåndbok.

4 Dette bør arbeidstaker være kjent med

4.1 Hvorfor bruker vi eID? Kort om eID sin rolle i elektronisk samhandling i offentlig sektor

I dagens samfunn blir stadig flere tjenester digitalisert, og det er blitt vanlig å signere dokumenter og å identifisere seg elektronisk for å få tilgang til tjenester. Virksomheter har derfor et økende behov for at ansatte har tilgang til og kan bruke en elektronisk ID.

Ansatte benytter som regel en bruker-ID forvaltet av arbeidsgiver på arbeidsplassen. Denne bruker-ID-en består gjerne av et brukernavn og passord, og benyttes for å logge inn på en PC eller interne systemer. I tillegg har mange ansatte en privat eID som benyttes til personlige tjenester typisk innen skatte-, finans- og helseområdet. En slik eID vil være mye sikrere enn bare en bruker-ID med et brukernavn og passord. Se nærmere omtale av hva en eID er i kapittel 2. I noen sammenhenger benyttes en eID på arbeidsplassen fordi det er behov for at den ansatte identifiserer seg elektronisk på en sikker måte.

4.2 Arbeidstakers behov for enkel og forståelig informasjon om hva det innebærer å bruke eID i arbeidssammenheng

Det eksisterer ikke et helhetlig tilbud for opplæring og veiledning for anskaffelse og bruk av eID for offentlige ansatte. Mange ansatte vil derfor ha behov for informasjon om eID, for å forstå hva bruken innebærer. I kapittel 2 i veilederen sies det noe om eID generelt, deriblant om bruksområder for eID, risiko, sikkerhetsnivåer og hvordan en eID utstedes.

I kapittel 2.4 er det beskrevet noen gjennomgående utfordringer knyttet til bruk av eID i arbeidssammenheng. De enkelte arbeidstakerne kan derimot ha ulike utfordringer knyttet til bruk av eID. Utfordringene kan være unike for arbeidstakeren, være sektorspesifikke eller gjelde for en bestemt gruppe. Flere av utfordringene kan løses ved at arbeidsgiver gir tilstrekkelig informasjon til arbeidstaker. Det er arbeidsgivers ansvar å informere arbeidstaker om det som er relevant og nødvendig for tilrettelegging for bruk av privat eID i arbeidssammenheng. Både arbeidsmiljøloven og personopplysningsloven (personvernforordningen) krever at arbeidsgiveren aktivt informerer sine ansatte.

Denne delen av veilederen søker å gi nødvendig informasjon som arbeidstakeren bør være kjent med, og som arbeidsgiver kan formidle til arbeidstakeren.

4.3 Informasjon om risiko, ansvarsfordeling og andre forhold mellom arbeidsgiver og arbeidstaker

En arbeidstaker må få informasjon om hva det innebærer å bruke eID i arbeidssammenheng, både i de tilfeller hvor arbeidstaker bruker sin private eID eller har fått tildelt en ansatt-eID av arbeidsgiver.

I dette underkapittelet gis en oversikt over hvilken informasjon som bør formidles til arbeidstakeren. Blant annet hvordan risiko og ansvar fordeles mellom arbeidsgiver og arbeidstaker, og behandlingen av den ansattes personopplysninger.

Det er viktig at arbeidsgiver gir tilstrekkelig og forståelig informasjon til arbeidstaker før løsningene tas i bruk.

Ved *anskaffelse og bruk* av eID bør du som arbeidstaker få vite følgende:

- Hva bruken av eID innebærer for den enkelte arbeidstaker, og om bruk av eID i arbeidssammenheng medfører noen **tilleggsrisiko**[24] for den enkelte arbeidstaker. Det er ikke uvanlig at ny teknologi møtes med en viss skepsis og bekymring, ei heller konseptet om å identifisere seg elektronisk. Selv om dette over tid nok er blitt moden teknologi, vil en del bekymringer kunne henge igjen. Noen av disse kan være mer eller mindre berettigede, mens andre ikke er det.
    - Generelt er det en viss risiko uavhengig av hvilken eID-ordning som velges, i det man aldri kan være helt sikker på at opplysninger som behandles digitalt ikke utsettes for sikkerhetsbrudd.
    - Dagens løsninger på sikkerhetsnivå betydelig og høyt gjennomgår grundig internrevisjon og er underlagt et eksternt tilsynsregime. Overordnet tilsier den høye utbredelsen av eID at det er løsninger som brukerne stoler på og ønsker å benytte. Forutsetningen for bruk av eID på jobb er at de ansatte mottar tilstrekkelig informasjon, inkludert informasjon om eventuell risiko og ansvarsfordeling (se også kapittel 5.2 og 5.3).
- Ved spørsmål om hvilken **tilleggsrisiko** det utgjør å benytte eID *i forbindelse med arbeidet*, må risikoen knyttes til forhold som er relatert til arbeidet.
    - Arbeidsrelaterte forhold kan være sikkerhetsbrudd på arbeidsgivers systemer, ID-misbruk fra andre ansatte, eller uaktsom deling av tilgangskoder.
    - For ansatte kan det for eksempel utgjøre en risiko hvis de forlater arbeidsplassen uten å låse PC-en. Et lignende eksempel er risikoen forbundet med at flere personer jobber på delte enheter. Hvis en ansatt logger på gjennom ID-porten og glemmer å logge ut, vil den som kommer etterpå kunne bruke den pågående sesjonen og få uberettiget tilgang til ulike tjenester.
    - Andre risikofaktorer knyttet til arbeidet er frakt og oppbevaring av utstyr som benyttes til eID og generelt økt bruk av eID-en.
    - Den eventuelle tilleggsrisikoen ved å ta i bruk eID i arbeidssammenheng kan reduseres ved gode interne retningslinjer, samt informasjon, opplæring og oppfølging av de ansatte.
    - Arbeidstakere må skille mellom opplevd risiko og faktisk risiko. De fleste har i dag en eID, og bruk av eID i arbeidet utgjør normalt liten tilleggsrisiko, sett i forhold til bruken i hjemmet og ellers.
    - For mer informasjon om risikoen ved «engangsinnlogging» se kapittel 2.2.1.2. Se også Datatilsynets nettsider for mer informasjon om identitetstyveri generelt, og om sterk autentisering.
- **Ansvar og plikter** i forbindelse med bruk av eID-en, oppbevaring av kodebrikker og annet utstyr knyttet til bruk av eID-en i arbeidssammenheng. Dette inkluderer ansvarsfordelingen mellom arbeidstaker, arbeidsgiver og eventuelt eID-leverandøren.
    - Ansattes forpliktelser etter brukeravtalen med eID-leverandøren
        - Ved bruk av eID vil den ansattes konkrete forpliktelser overfor eID-leverandøren normalt fremgå av en brukeravtale. Den ansatte må overholde disse forpliktelsene.
        - Et eventuelt personlig tap som den ansatte lider i forbindelse med bruk av eID-en i arbeidet, kan likevel tenkes å bli arbeidsgivers anliggende. Et eksempel er hvis det stilles krav til informasjonssikkerheten i

[24] (Skal inn i trekkspill-boks)

brukeravtalen. I slike tilfeller er det nærliggende at virksomheten tar del i dette ansvaret og sørger for tiltak for å unngå brudd på sikkerheten til eID-en til den ansatte, jf. også virksomhetens forpliktelser etter eforvaltningsforskriften § 15 flg.
        - Ved bruk av ansatt-eID vil det enten være en brukeravtale mellom den ansatte og eID-leverandøren direkte, eller en avtale med eID-leverandøren som går via arbeidsgiver.[25] I avtalen bør det normalt fremgå hvilket ansvar og plikter den ansatte har.
        - Ved behov kan det avtales mellom arbeidsgiver og arbeidstaker hvilken bruk av eID-en som er tillatt i arbeidssammenheng og hvilken bruk av eID-en som ligger utenfor rammene av arbeidsforholdet. Se nærmere omtale av dette i kapittel 5.2.2.2.

    - <u>Arbeidsgivers ansvar</u>
        - En offentlig virksomhet kan i egenskap av å være arbeidsgiver bli ansvarlig for arbeidstakers bruk av eID, ettersom arbeidsgiver svarer for skade som voldes forsettlig eller uaktsomt av arbeidstaker under arbeidstakers utføring av arbeid, jf. skadeserstatningsloven § 2-1 («arbeidsgiveransvaret»). En kan for eksempel se for seg at arbeidstaker uaktsomt benytter en annens eID når flere personer jobber på delte enheter.
        - Arbeidsgivers ansvar vil måtte bero på en konkret vurdering av omstendighetene. I vurderingen skal det tas hensyn til om «de krav skadelidte med rimelighet kan stille til virksomheten eller tjenesten, er tilsidesatt». Virksomheten vil ikke måtte svare for skade som skyldes at arbeidstakeren går utenfor det som er rimelig å regne med etter rammene for arbeidsforholdet.
        - Såfremt du som arbeidstaker benytter eID-en etter beste evne og til å utføre dine pålagte arbeidsoppgaver, skal det mye til før det oppstår et tilfelle hvor det er aktuelt med personlig ansvar for den ansatte.[26]

- **Informasjon om restriksjoner** knyttet til bruk av eID-en.[27] Dette kan inkludere informasjon om egen og andres mulighet til å suspendere eller stenge eID-en, for eksempel ved misbruk eller avslutning av arbeidsforholdet. Arbeidsgiver kan som utgangspunkt *ikke legge restriksjoner* på arbeidstakers bruk av en privat eID, selv om den benyttes i arbeidet.
- **Informasjon om kostnader ved bruk av eID i arbeidet** og **kostnadsfordelingen** mellom arbeidsgiver og arbeidstaker. Dette gjelder også for anskaffelse og bruk av utstyr knyttet til den eID-en som blir brukt i arbeidssammenheng.
    - Her finnes det flere ulike løsninger som må avklares konkret, enten med den enkelte ansatte eller kollektivt.

[25] For eksempel en egen avtale mellom eID-leverandøren og virksomheten (arbeidsgiver), hvor det også innhentes en godkjenning fra sluttbrukeren (den ansatte).
[26] *(Nedtrekkbar tekst til web)* For omfanget av arbeidsgiveransvaret se for eksempel Rt. 2008 s. 755 avsnitt 52, og Rt. 2015 s. 475 avsnitt 80 flg. Et eksempel på hvor grensen for arbeidsgivers ansvar skal trekkes opp finnes i HR-2017-2292-A.
[27] (*Nedtrekkbar tekst til web*) Utstyr som er innkjøpt for arbeidsgivers regning, er normalt arbeidsgivers eiendom med mindre annet er avtalt. På lik linje som med annet utstyr, må arbeidsgiver kunne sette retningslinjer for bruk av eID-ordninger de selv har anskaffet, herunder ansatt eID med tilhørende utstyr. En slik ansatt eID vil i mange tilfeller også inneholde et sertifikat som er ment for bruk i tjeneste for forvaltningen, og skal derfor ikke benyttes for andre formål, jf. eForvaltningsforskriften § 19 første ledd.

- Den ansatte bør få informasjon om arbeidsgiver vil dekke kostnader til anskaffelse av en eID og/eller tilhørende nødvendig utstyr. For eksempel anskaffelse av mobiltelefon eller smartkort der det er nødvendig for bruk av eID i arbeidsforholdet. (Se også kap. 5.2.2 for mer informasjon om hva arbeidsgiver bør vurdere i denne sammenheng.)
- Det bør også gis informasjon om eventuell **kompensasjon** for det tilfellet at arbeidstaker ønsker å benytte en eksisterende eID i arbeidet, som ikke innebærer noen nyanskaffelser for arbeidsgiver. Selv om det ikke er noen generell regel for slik kompensasjon, så vil ansattes bruk av privat eID normalt kunne være en fordel for arbeidsgiver. Avhengig av omstendighetene ved det konkrete arbeidsforholdet kan det antas at dette er noe arbeidstaker vil forvente kompensasjon for.

- For bruk av eID på arbeidsplassen kreves det at virksomheten har god generell informasjonssikkerhet. Det er viktig med bevissthet rundt **informasjonssikkerhet** og **ansvarsfordeling ved bruk/innføring av eID**. Dette innebærer også krav til at behandlingsansvarlig gjennomfører tekniske og organisatoriske sikkerhetstiltak.[28] (For mer informasjon om informasjonssikkerhet se Digdirs nettsider)
- Informasjon om behandling av **personopplysninger** (se kap. 4.4 for mer utfyllende informasjon)
- Hvilken **opplæring** og **oppfølging** de ansatte vil få

4.4 Nyttig for arbeidstaker å vite om personvern

Arbeidsgiver skal informere arbeidstaker om behandlingen av personopplysninger som skjer ved bruk av eID-ordninger i arbeidssammenheng. Ved innsamling av personopplysninger krever personvernforordningen art. 12-14 at behandlingsansvarlig skal gi konkret informasjon til den det er registrert opplysninger om – i dette tilfellet den ansatte. Denne informasjonen skal fremstilles på en «*kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk*» (personvernforordningen, art. 12(1)). Det anbefales også som beste praksis at det gis mer informasjon enn det som er fastsatt i personvernforordningen art. 13 og 14. Det bør gis en kortfattet og skriftlig forklaring til ansatte om hva behandlingen av personopplysningene innebærer, i tillegg til de kravene som ligger i personvernforordningen.

- Se Datatilsynets nettsider for mer informasjon om den behandlingsansvarliges informasjonsplikt under personvernforordningen.

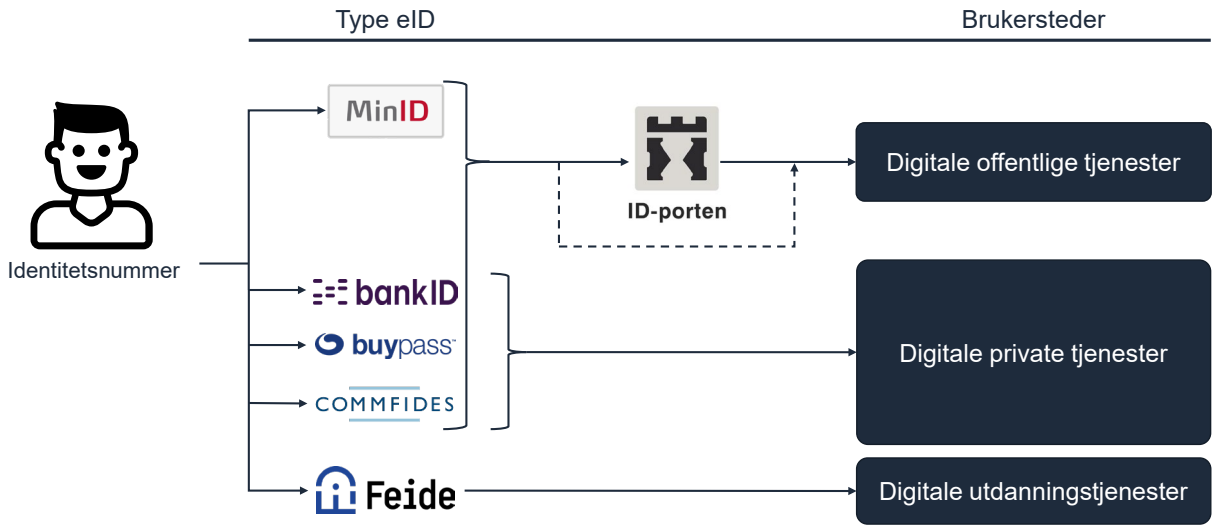
Ved bruk av privat eID for identifikasjonsformål innebærer behandlingen av personopplysninger normalt sett en overføring av navn og fødselsnummer til og mellom de aktørene som har behandlingsgrunnlag. Dette gjelder også der eID blir brukt i arbeidssammenheng. (Se kap. 4.4. for mer informasjon om personvern, og kap. 6.3.7 for informasjon om særlig bruk av fødselsnummer.)

4.4.1 Hvilke personopplysninger behandles og hvorfor?

eID-ordninger behandler personopplysninger som navn, fødselsnummer og eventuelt andre opplysninger slik som adresse og telefonnummer. Fødselsnummer benyttes for å opprette en entydig knytning til en person i Folkeregisteret, slik at en person kan bli unikt identifisert. Dette fjerner risikoen for identitetsforveksling.

[28] Personvernforordningen, art.32.

Det er flere aktører i «eID-økosystemet» som behandler disse opplysningene, for det overordnede formål å bekrefte at du er den du utgir deg for å være. I det følgende vil de ulike aktørene og flyten for personopplysningsbehandlingen gjennomgås.



Figur 1: Overordnet eksempel på hvordan eID-er brukes i dag

Eksempel: Bruk av journalsystem i Oslo kommune, driftet av Norsk Helsenett

1. Oslo kommune benytter et journalsystem som driftes av Norsk Helsenett. I systemet ligger det i tilgangskontrollen at *ansatt X* skal ha tilgang til visse ressurser. I utførelsen av sine arbeidsoppgaver er det nødvendig for ansatt X å gå inn i journalsystemet.
2. Oslo kommune har derfor et legitimt behov for at ansatt x skal presist og sikkert kunne autentisere seg selv.
    - Prosessen ansatt x går igjennom er følgende:
        - Ansatt x går til ID-porten
        - Ansatt x autentiserer seg med en eID (enten det er en ansatt-eID eller en privat eID)
            - Dette medfører kall frem og tilbake til den valgte eID-leverandøren, for eksempel Commfides, Buypass eller BankID.
            - Kallet forteller ID-porten at: Ja, denne personen er den han utgir seg for å være.
        - ID-porten sender da informasjon til Norsk Helsenett om at denne personen er autentisert.
        - Basert på policyene i tjenesten til Norsk Helsenett blir også ansatt x autorisert til å aksessere gitte ressurser.
    - Rollene kan tenkes å være som følger: [29]

[29] Dette er en forenklet fremstilling. Under omstendighetene og for deler av prosessen vil ulike aktører også kunne ansees å være databehandler. Dette gjelder for eksempel Digdir. Se nærmere om Digdirs rolle ifbm. behandling av personopplysninger i ID-porten: https://samarbeid.digdir.no/digital-postkasse/bruksvilkar-offentlige-kunder/70#24_behandling_av_personopplysninger_ , punkt 1.7 og 2.4.

- Oslo kommune er behandlingsansvarlig for opplysningene om ansatt x som behandles i forbindelse med utførelsen av arbeidsoppgaven, herunder innloggingen.
- Digitaliseringsdirektoratet er behandlingsansvarlig for personopplysninger som behandles i ID-porten.
- eID-leverandøren er behandlingsansvarlig for personopplysninger som behandles ved bruk av deres eID..
- Norsk Helsenett er databehandler for Oslo kommune for journalsystemet.

4.4.1.1 Markedsløsningene (angitt som «Type eID» i figur 2 over)

Behandling av personopplysninger i forbindelse med utstedelse og bruk av eID kan variere noe mellom de forskjellige leverandørene i markedet. For hvilke eksakte opplysninger som behandles henvises det til de forskjellige leverandørenes egne brukeravtaler og personvernerklæringer.

Overordnet vil følgende personopplysninger behandles i forbindelse med eID:

- Som et minimum behandles ditt unike identitetsnummer (fødselsnummer eller D-nummer), fornavn og etternavn ved utstedelse og bruk av eID. Dette gjelder både for privat og ansatt-eID.
- Det varierer hvorvidt informasjon om telefonnummer og epostadresse logges ved bruk av privat eID, men informasjonen blir behandlet ved utstedelse hos alle leverandørene.
- Praksis for behandling av opplysninger om nasjonalitet og språkpreferanse varierer mellom leverandørene.
- Ved utstedelse og bruk av ansatt-eID behandles gjerne informasjon om virksomheten du er ansatt i, for eksempel arbeidsgivers organisasjonsnummer.

eID-leverandørene er behandlingsansvarlige for de personopplysningene som er nødvendige for å administrere sine eID-ordninger.

4.4.1.2 ID-porten

Ved autentisering og innlogging i ID-porten er Digitaliseringsdirektoratet behandlingsansvarlig. I denne forbindelse lagrer og videreformidler Digitaliseringsdirektoratet opplysninger om fødselsnummer, sikkerhetsnivå for gjennomført autentisering, språkvalg og hvilken eID som ble benyttet for autentiseringen. Disse opplysningene blir lagret i ett år. ID-porten bruker også fem forskjellige typer informasjonskapsler i forbindelse med autentisering. Disse blir automatisk slettet når du lukker nettleseren din.[30] Digitaliseringsdirektoratet er behandlingsansvarlig for disse opplysningene.

ID-porten fører en samlet logg over brukernes autentiseringer uavhengig av om det er privat bruk eller autentiseringer gjennomført i arbeidssammenheng. Opplysningene sikrer sporbarhet og notoritet for de enkelte påloggingene. I tilfelle det oppstår misbruk av eID-en vil loggen kunne bidra til å ivareta brukerens sikkerhet, ved at urettmessige innlogginger avdekkes. Opplysningene er bak innloggingsmur og er ikke tilgjengelig for arbeidsgiver. Loggen krever innlogging med eID og er derfor under brukerens kontroll.

[30](lenke til) https://samarbeid.digdir.no/digital-postkasse/bruksvilkar-offentlige-kunder/70#64_behandling_av_personopplysninger_ punkt 2.4 og https://eid.difi.no/nb/sikkerhet-og-informasjonskapsler/personvern-og-informasjonskapsler

4.4.1.3 Tjenesteeier (angitt som «Brukersteder» i figur 2 over)

Tjenesteeieren, det vil si de som har ansvar for den konkrete tjenesten man logger seg inn i (for eksempel skatt eller helsetjenester), er behandlingsansvarlig for opplysninger som blir utlevert fra ID-porten i forbindelse med autentisering av brukere. Tjenesteeier må også ha lovlig grunnlag for behandling av personopplysninger (personopplysningsloven §1, jf. GDPR artikkel 6), inkludert for behandling av fødselsnummer (personopplysningsloven § 12).

5 Dette bør arbeidsgiver vurdere – Bruk av eID i et arbeidsrettslig perspektiv

I tråd med den økte digitaliseringen har det blitt vanligere å identifisere seg og å signere dokumenter elektronisk, og i dag bruker mange ansatte en eID for dette formålet. Ved bruk av tjenester som krever eID på et bestemt sikkerhetsnivå vil arbeidsgiver kunne ha et saklig behov for at ansatte benytter slik eID i utførelsen av sitt arbeid.

I vurderingen av om den ansatte skal bruke eID i arbeidsutførelsen, bør virksomheten kartlegge behovet for at de ansatte benytter dette verktøyet. Videre bør det innhentes informasjon som gjør det enklere å foreta vurderinger om valg av eID-løsning og tilhørende utstyr, samt risikovurderinger.

Det kan være fornuftig av arbeidsgiver å avtale rammene for bruk av eID i arbeidet med de ansatte, deriblant anskaffelsen, eller om det er ønskelig å bruke en eksisterende løsning. Dette omtales nærmere i kapittel 5.2.

Det er ingen konkret hjemmel i lov eller forskrift som pålegger anskaffelse og bruk av eID i et arbeidsforhold. Ofte vil det heller ikke foreligge en konkret eller kollektiv avtale om bruk av eID i arbeidet. Da er det naturlig at bruk av eID i et arbeidsforhold tar utgangspunkt i arbeidsgivers rett til å lede, organisere, fordele og kontrollere arbeidet, heretter kalt «styringsretten».

Arbeidsgiver som vurderer å benytte eID for ansatte i virksomheten i medhold av styringsretten, bør være kjent med følgende utgangspunkter:

- Anvendelse av styringsretten må vurderes konkret innenfor rammene av den enkelte ansattes arbeidsforhold. Arbeidsavtalen setter rammene for vurderingen, se nærmere i kapittel 5.2.1. Omfanget av styringsretten vil også bero på en nærmere vurdering av arbeidsgivers behov for et bestemt pålegg og tilgjengelige alternativer. Ettersom vurderingen må være konkret, kan det ikke generelt konkluderes med at et pålegg ligger innenfor eller utenfor styringsretten.
- De konkrete omstendighetene ved arbeidsforholdet som omtalt under kapittel 5.1-5.3 (særlig kapittel 5.2.1 - 5.2.3) vil innvirke på vurderingen av inngrepet overfor den ansatte. For eksempel vil det være mindre inngripende om arbeidsgiver kompenserer den ansatte økonomisk for anskaffelse eller bruk av eID.
- Selv om det må bero på en konkret vurdering vil det i mange tilfeller ligge utenfor arbeidsgivers styringsrett å pålegge den ansatte å benytte sin private eID med tilhørende privat utstyr, dersom de ikke ønsker dette selv.
- Det er uansett en forutsetning for anvendelse av styringsretten at personvernreglene er overholdt (se kapittel 6).
- Det er også en forutsetning at arbeidsgiver har gjort arbeidstaker kjent med alle relevante opplysninger om bruk av eID i arbeidsforholdet (se kapittel 4).
- For alternativer til privat eID som forutsetter bruk av privat utstyr, se kapittel 2.2.2. Her gis informasjon om ansatt-eID og privat eID besørget av arbeidsgiver. Informasjonen her kan bidra til vurderingen av fordeler og ulemper ved de alternativene som finnes.
- Nærmere veiledning for vurderingen følger av kapittelet ellers med en sjekkliste i kapittel 5.4.

5.1 Kan arbeidsgiver benytte styringsretten for å pålegge bruk av privat eID?

Det er ingen konkret hjemmel i lov eller forskrift som pålegger anskaffelse og bruk av eID i et arbeidsforhold. For virksomhetene vil det ofte være et spørsmål om arbeidsgiver kan benytte styringsretten for å pålegge bruk av eID.

Styringsretten vil her som ellers være begrenset av lov, forskrift, tariffavtale, eventuelle kollektive avtaler og arbeidsavtalen, og omtales gjerne som en type restkompetanse. Arbeidsgiver bør derfor orientere seg om rettsutviklingen og eventuelle regulatoriske endringer som kan påvirke adgangen til å bruke styringsretten.

Styringsretten begrenses også av mer allmenne saklighetsnormer. Dette innebærer at utøvelse av arbeidsgivers styringsrett stiller visse krav til saksbehandlingen. Det må foreligge et forsvarlig grunnlag for avgjørelsen, som ikke må være vilkårlig, eller basert på utenforliggende hensyn, jf. bl.a. avgjørelsen i Rt. 2001 s. 418 (Kårstø). For å sikre en forsvarlig saksbehandling bør arbeidsgiver gjøre arbeidstaker kjent med alle relevante opplysninger om bruk av eID i arbeidsforholdet (se kapittel 4).

Vurderingen av om det foreligger et saklig behov for pålegg overfor den ansatte gjennomføres med utgangspunkt i vedkommendes arbeidsoppgaver, stilling og andre relevante forhold slik som samfunnsutviklingen. Arbeidsgiver vil i sin alminnelighet kunne ha et saklig behov for at de ansatte identifiserer seg i forbindelse med arbeidet. Et mer tradisjonelt eksempel er bruk av pass i forbindelse med en jobb som involverer mye internasjonal reiseaktivitet. Etter hvert som samfunnet er blitt mer digitalisert har eID i mange tilfeller blitt en forutsetning for digital samhandling, og det vil kunne være nødvendig at den ansatte identifiserer seg digitalt på en sikker måte. Dersom arbeidstaker etter en konkret vurdering trenger en eID for å kunne gjennomføre sine arbeidsoppgaver, vil bruk av eID kunne være saklig begrunnet i arbeidsgivers virksomhet.

Overordnet kan det skilles mellom de tilfeller der det oppnås enighet mellom arbeidsgiver og arbeidstaker om en frivillig ordning, og de tilfellene der det er uenighet om ulike forhold. Dersom arbeidstaker ikke selv ønsker det, må arbeidsgiver vurdere nærmere om styringsretten gir grunnlag for et ensidig pålegg. Generelt er det viktig at arbeidsgiver er oppmerksom på at adgangen til å pålegge bruk av private eiendeler i arbeidssituasjonen, for eksempel eID med tilhørende privat kodebrikke eller mobiltelefon, synes å være snever. Det antas derfor at arbeidsgiver må ha gode grunner for at et slikt pålegg ansees å ligge innenfor styringsretten. Se nærmere om fremgangsmåten i slike tilfeller i sjekklisten i punkt 5.4, særlig steg 3.

Motsatt synes det i utgangspunktet ikke å være noe i veien for en frivillig ordning som innebærer bruk av en privat eID med tilhørende utstyr, forutsatt at den ansatte er tilstrekkelig informert og øvrige regler er overholdt, deriblant kravene i personopplysningsloven. Som følge av ubalansen i styrkeforholdet mellom arbeidsgiver og ansatt skal det imidlertid noe til før en ordning ansees å være frivillig. Et eksempel der frivilligheten forsøkes ivaretatt er at arbeidsgiver tilbyr anskaffelse av en eID først, men den ansatte ønsker å benytte sin private eID. Mange ansatte opplever det som enkelt og effektivt å benytte en eID-løsning de allerede har erfaring med. Det bør derfor også legges til rette for at de som ønsker det kan fortsette med en slik ordning. Rammene for bruk av privat eID bør da avtales nærmere, se kapittel 5.2.

5.2 Hva bør avtales mellom arbeidsgiver og arbeidstaker?

5.2.1 Arbeidskontrakten eller annen avtale

Det kan være fornuftig at arbeidsgiver og arbeidstaker avtaler hvordan eID skal benyttes i arbeidet.

Arbeidsgiver bør drøfte behov og den konkrete bruken av eID i arbeidsforholdet med arbeidstakerne og deres representanter, og verneombudet kan tas med på råd i planleggingen. Drøftingene bør foregå så tidlig som mulig, slik at arbeidstakerne har en reell mulighet til å komme med eventuelle innvendinger og innspill. Målet er at partene kommer fram til løsninger som i størst mulig grad begrenser eventuelle ulemper for arbeidstakerne.

Det sikrer forutsigbarhet og trygghet om arbeidsgiver og arbeidstaker avtaler konkrete regler for bruk og anskaffelse av eID. Dette kan for eksempel skje i avtaler med den enkelte, kollektive avtaler, eller i internt reglement som utarbeides av virksomheten. For de som allerede er ansatt vil det være et spørsmål om partene bør avtalefeste eksisterende eller fremtidig bruk av eID i arbeidet.

Relevante punkter kan være:

- Retningslinjer for bruken.
- Kostnadsfordelingen knyttet til bruk og anskaffelse av eID, herunder også spørsmålet om kompensasjon ved bruk av arbeidstakers private utstyr.
- Ansvarsfordelingen mellom arbeidsgiver/arbeidstaker knyttet til eventuell tilleggsrisiko ved bruk av privat eID i arbeid.

Ved utformingen av slike bestemmelser bør arbeidsgiver være oppmerksom på rammene for hva som kan avtales for eksempel om bruk av privat utstyr i arbeidet.[31] Ettersom det ikke foreligger noen plikt til å ha en privat eID i dag, bør det som et utgangspunkt ikke pålegges anskaffelse av en slik eID dersom ikke den ansatte selv ønsker dette. Alternativet kan da være at arbeidsgiver besørger en eID til den ansatte, se nærmere om eID besørget av arbeidsgiver i kap. 2.2.2.

5.2.2 Tilgang til relevant tilleggsutstyr

For å benytte en eID i arbeidet trenger de ansatte tilgang til en «*besittelsesbasert autentiseringsfaktor*». Dette er en autentiseringsfaktor som den ansatte skal bevise at den er i besittelse av («noe du har»),[32] og som er i form av en fysisk ting som kan kommunisere med eID-ordningen. Dette kan for eksempel være et smartkort, en mobiltelefon eller en kodebrikke.[33]

Arbeidsgiver må foreta en konkret vurdering av hvilket utstyr som er nødvendig for at arbeidstakeren skal kunne gjennomføre sine arbeidsoppgaver, herunder også hvilken eID og tilhørende besittelsesbaserte autentiseringsfaktorer som skal anvendes.

Overordnet synes det i norsk arbeidsrett å være en nokså pragmatisk tilnærming til bruk av privat utstyr, og det forutsettes ofte at dette er noe partene avklarer i forbindelse med inngåelse av arbeidsforholdet. Det er nok likevel en forventning i mange arbeidsforhold om at arbeidsgiver stiller nødvendig utstyr til disposisjon, deriblant teknisk utstyr som bærbar PC og mobiltelefon. Det er derimot ikke en konkret lovfestet regel at arbeidsgivere skal skaffe utstyret som kreves for at en arbeidstaker skal kunne utføre sitt arbeid.

Det vil trolig innvirke på inngrepets styrke under styringsretten om den ansatte får besørget nødvendig utstyr av arbeidsgiver eller om dette må betales med egne midler, eventuelt om

[31] (nedtrekkbart felt til web). Blant annet vil arbeidsgiver normalt ikke kunne begrense bruken av en privat eID og tilhørende utstyr til tjenstlige formål.
[32] Se kapittel 2
[33] (nedtrekkbart felt til web). Fokuset i dette kapittelet vil være den fysiske tingen som benyttes til å autentisere brukeren og som kan medføre merkostnader for brukeren. ID-elementet i eID-en er sammenlignbart med et fysisk ID-dokument, og bruken av dette innebærer normalt ikke merkostnader for sluttbruker (den ansatte).

arbeidstaker kompenseres for bruken av arbeidstakers private utstyr. [34] Se nærmere om kostnadsfordelingen under.

5.2.2.1 Kostnadsfordelingen

Generelt kan det være hensiktsmessig om partene avtalefester om utstyret som skal benyttes helt eller delvis skal anskaffes og betales av arbeidsgiver.[35]

Den ansattes bruk av privat eID vil normalt innebære en fordel for arbeidsgiver, som kan skape en forventing hos arbeidstakeren om kompensasjon.[36] Hvorvidt kompensasjon er rimelig kan derimot avhenge av flere forhold, deriblant eventuelle bruks- eller anskaffelseskostnader i det konkrete tilfellet, hvem som bærer risikoen for utstyret, og størrelsen på den samlede økonomiske belastningen for den ansatte.[37]

Selv om det er nødvendig at eID benyttes i arbeidet, vil det ikke nødvendigvis være behov for bruk av bestemt utstyr. Arbeidsgiver har i utgangspunktet et teknologinøytralt valg innenfor rammene av de ulike eID-leverandørenes tilbud. For eksempel er det ikke nødvendig at en eID-løsning er tilknyttet en mobiltelefon, den kan også være knyttet til normalt billigere løsninger, slik som Smartkort eller være en integrert del av ansattkortet. Hvilket utstyr som eventuelt skal tilstås den enkelte arbeidstaker vil bero på en helhetlig vurdering av de økonomiske konsekvensene ved bruk av de ulike eID-ordningene. Selv om en autentiseringsfaktor isolert sett er dyrere, så kan anskaffelse og administrasjon av billigere autentiseringsfaktorer likevel vise seg å utjevne de totale kostnadene.

For det tilfellet at det skal anskaffes utstyr til bruk i arbeidet bør arbeidsgiver foreta en vurdering av hvilke skatteregler som kommer til anvendelse.

5.2.2.2 Risiko og ansvar

Dette underkapittelet vil ha fokus på den eventuelle tilleggsrisikoen som påføres arbeidsgiveren ved at ansatte benytter eID i arbeidet.

Innledende vil arbeidsgiver ha et ansvar for å overholde krav til informasjonssikkerheten, og gjennomføre egnede sikkerhetstiltak for bruk av eID i arbeidet, jf. punkt 5.3. Videre må arbeidsgiver ta høyde for at den ansatte kan gjøre feil i forbindelse med bruk av eID i tjenesten. Det vises til gjennomgangen i kap. 4.3 og redegjørelsene for «**tilleggsrisiko**», «**Ansvar og plikter**» - deriblant

---

[34] (nedtrekkbart felt til web)

[35] (nedtrekkbart felt til web) Avtalefesting av eventuell kompensasjon til den ansatte, og størrelsen, bidrar til å oppfylle kravet om at arbeidsavtalen skal angi eventuelle tillegg og andre godtgjørelser som ikke inngår i lønnen, sml. Henning Jakhelln, Arbeidsrettslige studier bind II, 2000, s. 1133

[36] (nedtrekkbart felt til web) I informasjonsinnhentingen til veilederen fremkom blant annet at Norsk Sykepleierforbund (NSF) har lagt en slik løsning til grunn; Den enkelte ansatte gis nødvendig utstyr av arbeidsgiver eller får dekket merkostnaden som følge av eventuell bruk av sin privat eID for arbeidsgiver.

[37] (nedtrekkbart felt til web). Et eksempel som ikke er direkte overførbart, men likevel kan gi noe veiledning ved pålegg som innebærer utlegg for ansatte, finner vi i dom fra Borgarting lagmannsrett (LB-2017-11661). Her hadde Utenriksdepartementet pålagt de ansatte å påta seg et personlig økonomisk ansvar overfor tredjemenn for utgifter til tjenestereiser, og bestille reisene med privat kredittkort.
I den konkrete vurderingen, viser lagmannsretten til at arbeidsgiver hadde iverksatt tiltak for å avdempe den økonomiske belastning som ordningen kunne ha for medarbeiderne. Dette endret likevel ikke det faktum at pålegget var inngripende overfor arbeidstaker, i det pålegget innebar at den enkelte medarbeider ble økonomisk ansvarlig overfor tjenesteyteren og at ordningen forutsatte bruk av private debet- eller kredittkort som igjen kunne sammenblande private midler og arbeidsgivers penger.
Lagmannsretten tok utgangspunkt i at et slikt pålegg måtte ha rettslig grunnlag – enten i tariffavtale, arbeidsavtalen eller styringsretten, og kom til at det ikke var tilfellet. Lagmannsretten mente at pålegget lå utenfor rammene av det arbeidsgiver kan bestemme i kraft av styringsretten.

arbeidsgiveransvaret i skadeerstatningsloven § 2-1. Arbeidsgiver kan også bli erstatningsansvarlig i medhold av GDPR artikkel 82, som gir enhver person som har lidt skade adgang til å kreve erstatning fra den behandlingsansvarlige som har forvoldt skaden.[38]

Gitt at arbeidsgiver er erstatningsansvarlig etter en nærmere vurdering av arbeidsgiveransvaret i skadeerstatningsloven § 2-1 eller som behandlingsansvarlig etter GDPR artikkel 82, kan arbeidsgiver måtte svare for skaden.

Arbeidsgivers ansvar etter skadeerstatningsloven § 2-1 omfatter som hovedregel ikke skade arbeidstaker volder utenfor tjenesten. En handling som har rimelig og naturlig sammenheng med tjenesten kan likevel omfattes. Det kan derfor være et behov på arbeidsgiversiden for å trekke opp skillelinjene mellom tjenstlig bruk av eID som har en naturlig sammenheng med arbeidsforholdet, og bruk eller handlinger knyttet til eID som faller utenfor arbeidsgivers ansvarssfære. Det vil også være en fordel for arbeidstaker, om det klart fremgår hva arbeidsgiver vil være ansvarlig for i forbindelse med bruk av eID. Dette kan oppleves betryggende og sikrer samtidig forutsigbarhet.

Arbeidsgiver bør i den sammenheng være oppmerksom på at det klare utgangspunktet vil være at de ikke kan legge begrensninger på bruken av en privat anskaffet eID. De ansatte vil kunne bruke denne til egne formål.

En ansatt-eID som er anskaffet av arbeidsgiver kan derimot normalt begrenses til tjenstlig bruk. Dette har sammenheng med at eID-en er anskaffet av eller via arbeidsgiver, og knytter seg til utstyr som er eid av arbeidsgiver. Et alminnelig utgangspunkt kan være at utstyr som er innkjøpt for arbeidsgivers regning forblir arbeidsgivers eiendom og leveres tilbake til arbeidsgiver ved fratredelse, eller når behovet for tjenesten ikke lenger er til stede. Ytterligere støtte for at arbeidsgiver kan begrense en ansatt-eID til tjenstlig bruk finnes i eForvaltningsforskriften § 19 første ledd. Her fastsettes at sertifikat eller passord/PIN-koder som er ment for bruk i tjeneste for forvaltningen, ikke skal benyttes for andre formål.

Ved bruk av ansatt-eID bør arbeidsgiver, på bakgrunn av den eID-ordningen som er valgt, gjennomføre tiltak for å begrense muligheten for at arbeidstakere benytter eID-en uberettiget og til andre formål enn det som er bestemt. Egnede tiltak kan være både av teknisk og organisatorisk art, f.eks. informasjon, instrukser og opplæring.

5.3 Informasjonssikkerhet

5.3.1 Overordnede regler for informasjonssikkerhet og risikovurderinger

eForvaltningsforskriften har som formål å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Forskriften gjelder for elektronisk saksbehandling og kommunikasjon i forvaltningen når ikke annet er bestemt i lov eller forskrift, og gjelder også for bruk av eID.

Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi), jf. § 15 første ledd.

I den utstrekning det er relevant for sikkerhetsstrategien bør det inntas prosedyrer for anskaffelse, bruk, oppbevaring og sikring av signaturfremstillingsdata og passord/PIN-koder knyttet til det personlige sertifikatet, jf. § 15 fjerde ledd bokstav a. Dette gjelder også for bruk av eID og tilhørende utstyr. Hva som bør omtales i sikkerhetsstrategien har også en side til GDPR artikkel 32, som pålegger

[38] (nedtrekkbart felt til web) Utgangspunktet er at personer som handler under en arbeidsgivers (den behandlingsansvarliges) instruksjonsmyndighet, blir identifisert med den behandlingsansvarlige. Se blant annet Prop. 56 LS (2017–2018) s. 145, jf. Ot.prp.nr.92 (1998–1999) s. 135.

arbeidsgiver som behandlingsansvarlig å «gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen».

5.3.2 Særlig om bruk av personlig sertifikat i offentlig forvaltning

eForvaltningsforskriften oppstiller regler for forvaltningens bruk av «personlige sertifikater», som er en av komponentene i både privat eID og ansatt-eID. Det stilles krav til at slike sertifikater skal «godkjennes» av forvaltningsorganet, jf. § 19 annet ledd.

Forskriften stiller ingen nærmere krav til denne godkjennelseshandlingen. En tolkning av konteksten og formålet ved bestemmelsen tilsier at det er tilstrekkelig med en form for godkjenning av sertifikatutsteder, herunder eID-leverandøren. Arbeidsgiver bør derfor synliggjøre at de godkjenner ønskede eID-leverandører, for eksempel ved eksplisitt å godkjenne selvdeklarerte løsninger på sikkerhetsnivå «høyt» på Nkom sin publiserte liste.

5.4 Sjekkliste for arbeidsgiver

<u>Steg 1</u>

- Kartlegg behovet og hvilke konkrete arbeidsoppgaver som skal løses ved bruk av eID og/eller elektronisk signatur.
    - Innhent informasjon om hvilke eID- og signatur-løsninger som finnes og vurder om de kan dekke virksomhetens behov. Bli kjent med fordeler og ulemper ved de ulike løsningene.
    - Finn ut hvor mange og hvilke ansatte som vil ha behov for å bruke eID og/eller elektronisk signatur som del av sine arbeidsoppgaver.
    - Avklar om det er ansatte som vil ha utfordringer med å skaffe eID på nivå høyt og om det finnes løsninger på dette.[39] En utfordring kan for eksempel være manglende fødselsnummer eller D-nummer, jf. selvdeklarasjonsforskriften § 19.
- Inngå dialog med ansatte og/eller deres tillitsvalgte som skal benytte eID og/eller elektronisk signatur.
    - Informer de ansatte om hva de bør være kjent med ifbm. bruk av eID i arbeidet. Se kapittel 4.
    - Avklar om den ansatte allerede har en eID og om de ønsker å benytte denne.
    - Vurder om bruken innebærer arbeidsorganisatoriske utfordringer. Her er det spesielt av betydning om den ansatte må benytte privateid utstyr i arbeidet, hvorvidt dette eventuelt skal kompenseres, og hvordan risikoen og ansvaret fordeles.
- Ta hensyn til likebehandling. Sjekklisten er utformet med tanke på førstegangsanskaffelse av eID. Realiteten er at mange benytter eID i arbeidet allerede. Det kan være fornuftig med en gjennomgang av sjekklisten så langt det passer, og påse at de som allerede bruker eID ikke utilsiktet behandles annerledes enn de som i fremtiden skal ta eID i bruk eller de som har innvendinger mot bruken.

<u>Steg 2</u>

- Vurder om bruken av valgt eID-løsning er i overenstemmelse med personvernreglementet, se kapittel 6.

[39] I utkastet til ny eID strategien er det beskrevet grupper med ulike utfordringer forbundet med å skaffe eID på høyere sikkerhetsnivå. Se for eksempel under mål 3.1.
https://www.regjeringen.no/contentassets/2756b7cebb38484e96840333a1919c51/utkast-til-ny-strategi-for-eid-i-offentlig-sektor-hor-l84994.pdf

- Vurder om bruken av valgt eID-løsning er i overenstemmelse med eForvaltningsforskriften, se kapittel 5.3 for hvilke krav som må være oppfylt.
- Vurder hva som eventuelt bør avtalefestes mellom arbeidsgiver og arbeidstaker, jf. kapittel 5.2. Avtaler mellom arbeidsgiver og arbeidstaker bør være skriftlige.

Steg 3: Vurdering av styringsretten - forutsatt bruk av privat eID

- Spørsmålet er om styringsretten kan benyttes til å pålegge bruk av privat eID. Ettersom styringsretten må utøves innenfor rammene av det enkelte arbeidsforholdet, vil det alltid måtte bli en konkret vurdering. Se kapittel 5.1 for en nærmere redegjørelse.

I det følgende er en sjekkliste om hvilke punkter som arbeidsgiver bør gjennomgå i sin vurdering.

- Arbeidsgiver bør orientere seg om rettsutviklingen. Er det f.eks. kommet nye regler eller praksis av betydning for bruk av eID i arbeidsforholdet?
- Undersøk om det er avtalefestet noe i tariffavtale, kollektive avtaler eller ansettelseskontrakten som direkte eller indirekte angår bruk av privat eID i arbeidet.
- Vurder om styringsretten kan gi grunnlag for pålegg om bruk av arbeidstakers private eID. Som et utgangspunkt kan det skilles mellom de tilfeller arbeidstaker ønsker å benytte sin private eID i arbeidet, og de tilfeller arbeidstaker ikke ønsker dette:

    - Dersom bruken baseres på arbeidstakers ønske om å bruke privat eID i arbeidet.
        - Vurder om partene er kommet frem til en tilstrekkelig frivillig ordning gjennom dialog, hvor det er tatt hensyn til maktubalansen.
        - Påse at punktene i steg 1 og 2 er oppfylt, deriblant at bruken av privat eID er i overenstemmelse med personvernreglementet og eForvaltningsforskriften. At arbeidstaker er tilstrekkelig informert, og gjort kjent med hva det innebærer å bruke eget utstyr, herunder om bruken skal kompenseres, samt håndtering av tilleggsrisiko og ansvarsfordeling mellom arbeidsgiver og arbeidstaker.
        - Gitt at punktene over er oppfylt vil det normalt ikke være noe i veien for en løsning som innebærer bruk av privat eID i et arbeidsforhold.
    - Dersom arbeidstaker ikke ønsker å benytte privat eID i arbeidet
        - Dersom det ikke er enighet om en frivillig ordning om bruk av privat eID i arbeidet, må det først identifiseres hva uenigheten går ut på, og om uenigheten kan avhjelpes.
        - Hvis uenigheten ikke kan avhjelpes kan det vurderes om det er grunnlag for et eventuelt pålegg i kraft av styringsretten. Ofte vil det være et spørsmål om arbeidsgiver kan kreve at en arbeidstaker benytter sine private eiendeler eller verktøy i arbeidssituasjonen. Dersom arbeidstaker nekter bruk av slik privat utstyr, bør arbeidsgiver være tilbakeholden med å anvende styringsretten og vurdere andre alternativer.
        - At den ansatte ikke ønsker å benytte private eiendeler, er imidlertid ikke alltid avgjørende. Om det er grunnlag for et pålegg om bruk av privat eID i slike tilfeller vil blant annet kunne bero på følgende momenter:
            - Tidsnød som arbeidsgiver ikke med rimelighet kunne forutse i forbindelse med utføringen av en oppgave, og som gjør det utfordrende å finne alternativer til bruk av privat eID.

- Det vil antakeligvis være et merkbart skille mellom pålegg om anskaffelse av en ny eID og pålegg om bruk av en eID den ansatte allerede har, hvor det førstnevnte tilfellet normalt er mer inngripende.
- Samfunnsutviklingen. Deriblant hvor vanlig det er med bruk av privat eID i arbeidsforhold, normer i den aktuelle sektoren, og hvilke forventinger det er til at arbeidsgiver sørger for en eID til sine ansatte.
- Stillingen og forventningen til stillingen. Er en privat eID noe arbeidstakeren bør forvente å bidra med inn i arbeidsforholdet?
- Det konkrete inngrepet overfor den ansatte, herunder hvilke løsninger som foreslås i forbindelse med besørgelse av utstyr og kompensasjonsordning.

6 Dette bør arbeidsgiver vurdere – Personvernet til arbeidstaker

Arbeidsgiver bør være kjent med følgende personvernrettslige utgangspunkter ved bruk av eID for ansatte i virksomheten:

- Arbeidsgiver vil normalt være behandlingsansvarlig for personopplysningsbehandlingen i forbindelse med gjennomføringen av en arbeidsoppgave, slik som innlogging i en tjeneste for å lese sikre meldinger eller autentisering for signering av et dokument.
- Det anses normalt å ligge innenfor formålet at privat eID benyttes som identifikasjonsmiddel mer generelt, også i arbeidsøyemed.
- Behandlingsgrunnlag vil ofte være arbeidsgivers berettigede interesse, jf. GDPR art. 6 (1) bokstav f. Arbeidsgiver må vurdere om det foreligger en berettiget interesse og dokumentere vurderingen. Det finnes alternative behandlingsgrunnlag som arbeidsgiver konkret må ta stilling til om kommer til anvendelse. Behandlingsansvarlige skal alltid velge det behandlingsgrunnlaget som best balanserer partenes interesser.
- De fleste eID-ordninger for privatpersoner og ansatte (privat eID og ansatt-eID) benytter personidentifiserende sertifikater, som medfører at det stort sett er samme personopplysninger som behandles i forbindelse med bruk, deriblant fødselsnummer.

De ulike utgangspunktene over vil etter omstendighetene kunne endre seg. I dette kapittelet vil vi gå nærmere inn på de ulike personvernsaspektene rundt roller og ansvar, formålsvurderingen, valg av behandlingsgrunnlag og personvernkonsekvenser for den enkelte.

6.1 Roller og ansvar

I kapittel 5 har vi tatt utgangspunkt i rollene i arbeidslivet fra et arbeidsrettslig perspektiv. Der er innbyggeren en ansatt og den offentlige etaten en arbeidsgiver. I dette avsnittet skal vi se på rollene i et personvernrettslig perspektiv.

I personvernforordningen er det flere roller vi må forholde oss til, men i denne veilederen konsentrerer vi oss om

- «den registrerte»
- «behandlingsansvarlig»
- «mottaker»
- «databehandler»

Med «den registrerte» menes en spesifikk ansatt.

Etter personvernforordningen artikkel 4 (7) er en «behandlingsansvarlig» (…) den som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes». Definisjonen kan passe både til arbeidsgiver, et offentlig organ som arbeidsgiver må forholde seg til, eID-leverandøren og ID-porten - avhengig av hvilken behandling det er snakk om.

Et scenario er at en ansatt som logger seg inn på en offentlig tjeneste med sin private eID for å utføre arbeidsoppgaver som er pålagt fra arbeidsgiver. Her vil det forekomme flere behandlinger av personopplysninger, blant annet gjennom ansattes valgte eID-løsning, gjennom ID-porten og hos den offentlige tjenesten bruker trenger å logge seg inn hos. Det vil være fire separate aktører som er behandlingsansvarlige for hver sin bruk, og må oppfylle de krav som følger av personopplysningsregelverket. Se eksempelet i kapittel 4.4.1. og kapittel 4.4.1.1 flg. for informasjon om hvilke personopplysninger som behandles.

«Mottaker» vil i mange tilfeller være en annen behandlingsansvarlig som ikke innhenter personopplysninger fra den registrerte.

«Databehandler». I det tilfellet en part behandler personopplysninger på vegne av en annen part (behandlingsansvarlig) vil det foreligge et databehandlerforhold som krever at det inngås en databehandleravtale mellom partene, jf. personvernforordningen artikkel 28 nr. 3.

6.1.1 Arbeidsgivers behandlingsansvar ved bruk av eID

Arbeidsgiver vil kunne ha et eget behandlingsansvar ved bruk av eID i arbeidsforholdet. En vurdering av arbeidsgivers behandlingsansvar må gjøres i den konkrete saken, og det må legges vekt på hvor stor rolle arbeidsgiver har i prosessen.

Vurderingsmomenter er her:

- Bestemmer arbeidsgiver formålet (hensikten) med behandlingen? (Bestemmer arbeidsgiver at den ansatte skal logge seg inn i tjenesten?)
- Bestemmer arbeidsgiver hvilke midler (metode) som brukes? (Bestemmer arbeidsgiver hvor og på hvilken måte den ansatte skal logge seg inn?)[40]
- Behandles personopplysningene på arbeidsgivers vegne? (Gjøres innloggingen som ledd i arbeidsoppgavene til den ansatte?)

Arbeidsgiver bør være oppmerksom på at de normalt vil være behandlingsansvarlig for personopplysningsbehandlingen i forbindelse med gjennomføringen av en arbeidsoppgave.

6.2 Er det i overenstemmelse med formålet å bruke eID i arbeidet?

Før det kan behandles personopplysninger, må behandlingsansvarlig definere et eller flere klart formulerte formål. Formålet for arbeidsgiver vil nok i de fleste tilfeller være krav om sikker identifisering som ledd i utføringen av en arbeidsoppgave. Dette omfatter blant annet å dele personopplysninger med ID-porten og den tjenesten som aksesseres.

Videre er det et prinsipp at personopplysninger ikke skal viderebehandles på en måte som er uforenlig med formålet de opprinnelig ble innhentet for, jf. personvernforordningen artikkel 5 nr. 1 bokstav b. Det påhviler arbeidsgiver som behandlingsansvarlig å foreta en vurdering av

[40] (nedtrekkbart felt til web) Her er det også et moment at arbeidsgiver etter eForvaltningsforskriften § 19 annet ledd godkjenner bruk av det personlige sertifikatet til eID-leverandøren, jf. kap. 5.3.

formålsangivelsen til den konkrete eID-leverandøren, og påse at sikker identifisering i arbeidsforholdet ikke er uforenlig med det oppgitte formålet.

Digdir har gjort en vurdering av formålet for bruk av eID basert på opplysninger fra eID-leverandørene og de formålsbeskrivelsene som ligger tilgjengelig ute på nett. Det er gjennomgående nokså generelle formålsbeskrivelser av eID som et digitalt identifikasjonsmiddel.[41] Dette tilsier at den private eID-en kan benyttes til å identifisere brukeren digitalt i ulike sammenhenger, også som ledd i utførelsen av en arbeidsoppgave. Det forutsettes at det foreligger en saklig grunn for identifiseringen i arbeidsoppgavene som er tillagt arbeidstaker,[42] og at det ikke fremgår konkrete begrensninger i formålsangivelsen til eID-leverandøren som tilsier at eID-en ikke kan benyttes i et arbeidsforhold.

6.3 Behandlingsgrunnlag

Behandling av personopplysninger forutsetter at behandlingsansvarlig på forhånd har identifisert et behandlingsgrunnlag for hver enkelt behandling. All behandling av personopplysninger må ha et grunnlag i GDPR art. 6 nr. 1 bokstav a til f.

GDPR Art. 6 nr. 1 er derfor i alle sammenhenger en uttømmende liste over mulige behandlingsgrunnlag. Behandling av særlige kategorier personopplysninger må i tillegg, for å være lovlig, tilfredsstille minst ett av vilkårene i art. 9 nr. 2.

Grunnlagene i GDPR er ikke listet opp i prioritert rekkefølge. I veilederen derimot, vil vi behandle de behandlingsgrunnlagene som er mest nærliggende å benytte seg av først, slik at man antar bokstav f som mest aktuell, men at det kan være supplerende rettsgrunnlag som gjør bokstav e og c aktuelle i de konkrete omstendighetene.

Dersom det ikke foreligger behandlingsgrunnlag etter GDPR art. 6 bokstav f eller alternative behandlingsgrunnlag for den konkrete behandlingen, vil heller ikke styringsretten kunne anvendes for å pålegge bruk av privat eID (se kap. 5.1. flg.).

6.3.1 Berettiget interesse

Behandlingsgrunnlag etter GDPR art. 6 nr. 1 bokstav f innebærer en nærmere interesseavveining av de forhold som begrunner behandlingen sett i forhold til hensynet til den registrerte. Behandling etter bokstav f er lovlig dersom *«behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger».* Behandlingsansvarlig må kunne dokumentere vurderingen.

Vi antar at dette vil være et naturlig behandlingsgrunnlag for de fleste arbeidsgivere. Arbeidsgiver må derfor vurdere følgende tre krav; *det må foreligge et saklig formål*,[43] *behandlingen må være nødvendig for å ivareta dette formålet* og *til slutt må det foretas en interesseavveining der den ansattes interesser balanseres mot behandlingsansvarliges eller tredjeparts interesser.*

I GDPR artikkel 6 nr. 1 siste ledd er det inntatt en særskilt begrensning som innebærer at art. 6 nr. 1 bokstav f ikke kan benyttes som behandlingsgrunnlag for behandling av personopplysninger som ledd i offentlig myndighetsutøvelse. Offentlige virksomheter anses ikke å utøve offentlig myndighet når de opptrer som arbeidsgiver. Begrensningen kommer normalt ikke til anvendelse ved bruk av eID

[41] (nedtrekkbart felt til web) Det kan derimot være spesifikke formålsbegrensninger ved den enkelte eID. Dette vil eventuelt fremgå av brukervilkårene for denne ordningen.
[42] (nedtrekkbart felt til web) Personvernforordningen artikkel 5 nr. 1 b, jf. Artikkel 6 nr. 4 a-e.
[43] Se kapittel 6.2.

i offentlig forvaltning, ettersom offentlige virksomheter i denne sammenheng opptrer som arbeidsgivere for sine ansatte.

Bruk av eID har med samfunnsutviklingen blitt en grunnpilar for samhandling i digitale tjenester. En offentlig ansatt må med ulik frekvens og avhengig av stillingen regne med å måtte identifisere seg digitalt, og på en sikker måte, under utførelsen av sine arbeidsoppgaver. Dette vil i mange tilfeller være et saklig formål for å behandle personopplysninger.

Arbeidsgiver må videre foreta en konkret vurdering av om arbeidsoppgavene til den enkelte gjør det *nødvendig* å benytte eID med den underliggende persondatabehandlingen det medfører. Det kan for eksempel være behov for å identifisere seg mot en bestemt tjeneste i arbeidet, og eID ansees ofte som et egnet og nødvendig middel for å oppnå det formålet.[44]

Selv om behandlingen av personopplysninger ved innlogging med eID anses som nødvendig for å oppnå et saklig formål, må det foretas en interesseavveining - der ansattes interesser, rettigheter og friheter veies opp imot virksomhetens berettigede interesser for å behandle opplysningene til ovenfor nevnte formål. I den sammenheng bør en merke seg at sikker og entydig digital identifisering kan være i både virksomhetens og den ansattes interesse - av hensyn til informasjonssikkerhet, datakvalitet og for å sikre at rett ansatt gis riktig tilgang.

GDPR art. 6 nr. 1 bokstav f må videre ses i sammenheng med art. 21, som gir den registrerte rett til å protestere mot bestemte former for behandling etter dette behandlingsgrunnlaget. Den ansatte må også informeres om retten til å protestere.

Dersom den ansatte motsetter seg behandlingen som forutsettes ved bruk av eID, kan behandlingen likevel igangsettes dersom det foreligger tvingende berettigede grunner, som går foran den registrertes interesser, rettigheter og friheter. I dette ligger at ved en eventuell protest fra den registrerte må det foretas en ny vurdering, ikke helt ulik den som foretas etter GDPR art. 6 nr. 1 bokstav f. At det kreves «tvingende» berettigede grunner, tilsier at terskelen i denne omgang er høyere.

---

[44] (Nedtrekkbart felt til web) Vi kan her se på to typetilfeller: 1) Der sikkerhetsnivået bestemmes av en ekstern tjenesteeier, og 2) Der sikkerhetsnivået bestemmes av arbeidsgiver.

1) *Sikkerhetsnivået er bestemt av ekstern tjenesteeier*. Vurderingen av om det er nødvendig med bruk av eID på sikkerhetsnivå «betydelig» eller «høyt» kan sees i sammenheng med behovet for å benytte bestemte tjenester som krever disse sikkerhetsnivåene i arbeidet. I en del tilfeller vil ikke arbeidsgiver kunne påvirke sikkerhetsnivået til en tjeneste, eller med rimelighet kunne sies å ha tilgang til gode alternative tjenester. Bruk av eID vil da ofte være nødvendig.

2) *Sikkerhetsnivået er under* a*rbeidsgivers kontroll*. Dersom arbeidsgiver kan bestemme sikkerhetsnivået i tjenesten den ansatte skal identifisere seg mot, må arbeidsgiver gjøre en vurdering av om det er nødvendig med eID på et bestemt sikkerhetsnivå. I disse tilfellene kan man vurdere om formålet om sikker nok identifisering av den ansatte kan oppnås med andre midler, for eksempel brukernavn og passord, og at bruk av eID ikke alltid er nødvendig.

Typetilfellene over er ikke ment å være uttømmende og det finnes flere ulike scenarioer som berettiger bruk av eID i arbeidet. Arbeidsgiver som behandlingsansvarlig må i alle tilfeller ha foretatt en nødvendighetsvurdering av om arbeidsoppgavene til den enkelte forutsetter bruk av eID (og tilhørende behandling av personopplysninger).

En tvingende berettiget interesse kan kanskje være at behovet for sikker identifisering er så stort at det ikke kan tilfredsstilles på annen måte enn ved bruk av eID, og at den tilhørende behandlingen av personopplysninger dermed er berettiget.

I korthet vil GDPR art. 6 nr. 1 bokstav f i mange tilfeller kunne være behandlingsgrunnlag for det begrensede sett av personopplysninger som er nødvendige for bruk av eID, forutsatt at tiltaket gjennomføres på en måte som er saklig og forholdsmessig for den enkelte og etter en forsvarlig vurdering og prosess hos arbeidsgiver.

Dersom en ansatt motsetter seg behandling av personopplysningene av tilstøtende grunner til selve behandlingen, for eksempel bruk av private eiendeler i arbeidssammenheng, vises det videre til behandlingen av dette temaet under kapittel 5. Arbeidsgiver kan i slike tilfeller vurdere andre alternativer. Se også kapittel 2.2.2, og sjekklisten i kapittel 7 (steg 2).

6.3.2 Nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet

GDPR artikkel 6 nr. 1 bokstav e angir at behandling av personopplysninger er lovlig, dersom behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt.

Som et utgangspunkt ansees utøvelse av offentlig myndighet å forutsette bruk av den myndigheten organet er gitt i eller i medhold av lov (supplerende rettsgrunnlag). Myndighetsutøvelsen kan også følge av annet supplerende rettsgrunnlag enn lovpålegg, herunder nasjonale rettsregler som pålegger organet plikter.

Det utøves normalt ikke offentlig myndighet når offentlige organer opptrer som arbeidsgiver, og i disse tilfellene er alternativet i artikkel 6 nr. 1 bokstav e ikke et anvendelig behandlingsgrunnlag.

Det finnes tilfeller der artikkel 6 nr. 1 bokstav e med supplerende rettsgrunnlag kan være behandlingsgrunnlag for ansattes opplysninger, og dette må arbeidsgiver vurdere i det konkrete tilfellet. Tilsvarende som for de behandlingene som er dekket av art. 6 nr. 1 bokstav f, må bestemmelsen ses i sammenheng med art. 21. Det vil si at den registrerte må gis informasjon om behandlingen og om retten til å protestere mot denne.

6.3.3 Nødvendig for å oppfylle en rettslig forpliktelse

Art. 6 nr. 1 bokstav c gir rettslig grunnlag for å behandle personopplysninger dersom det er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige.

Dette kan for enkelte oppgaver og behandlingsansvarlige vurderes som behandlingsgrunnlag. Dette gjelder der behandlingsansvarlig gjennom lov, forskrift eller på andre måter gjennom nasjonal rett er pålagt oppgaver som tydelig forutsetter behandling av ansattes personopplysninger, jf. tilsvarende redegjørelse for «supplerende rettsgrunnlag» i punkt 6.3.2.

Det finnes tilfeller der artikkel 6 nr. 1 bokstav c med supplerende rettsgrunnlag kan være behandlingsgrunnlag for ansattes opplysninger, og dette må arbeidsgiver vurdere i det konkrete tilfellet.

6.3.4 Samtykke

Artikkel 6 nr. 1 bokstav a stiller som vilkår at den registrerte har «samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål».

Samtykke fra den registrerte er «enhver frivillig, spesifikk, informert og utvetydig viljestyring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende».[45] I denne sammenhengen er det særlig hvorvidt samtykket er gitt frivillig som er det avgjørende. Situasjonen må være slik at det i realiteten er mulig å gi et samtykke av fri vilje.

Samtykke er som utgangspunkt ikke egnet som behandlingsgrunnlag dersom det er usannsynlig at samtykket er reelt frivillig. For eksempel er det ikke en reell frivillighet når skatteetaten behandler personopplysningene til en skattebetaler.

Når det gjelder ansattes bruk av personopplysninger i sin eID etter instruks fra arbeidsgiver, vil utgangspunktet være relativt likt. Arbeidsgiver vil ha en styringsrett og instruksjonsmyndighet over hvordan den ansatte utøver arbeidet sitt. Dette må sees i sammenheng med den generelle maktubalansen mellom partene. Samlet sett vil det være utfordrende å oppfylle kravet om reell frivillighet.

Vår anbefaling er at arbeidsgiver ikke baserer seg på samtykke som behandlingsgrunnlag for ansattes personopplysninger.

6.3.5 Nødvendig for å oppfylle en avtale

Art. 6 nr. 1 bokstav b gir rettslig grunnlag for å behandle personopplysninger dersom behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås.

Generelt ansees ikke art. 6 nr. 1 b som et spesielt godt rettslig grunnlag for behandling av personopplysninger i arbeidsforhold. Det er utfordrende å nå opp til terskelen om direkte og objektiv forbindelse mellom behandlingen av personopplysninger og oppfyllelse av arbeidskontrakten, og det er en maktubalanse mellom partene.[46]

Videre bør arbeidsgiver være obs på at det sjelden vil være en farbar vei å basere seg på "samtykke" i arbeidskontrakten for overskytende behandling som ikke omfattes av bokstav b, ettersom en raskt støter på problemer rundt art. 7 nr. 4 og kravet om frivillighet, jf. også punkt 6.3.4.

6.3.6 Nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser

Art. 6 nr. 1 bokstav d gir grunnlag for å behandle personopplysninger når det er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser.

Vi antar at denne vil være lite relevant som et generelt behandlingsgrunnlag for personopplysninger som deles ved bruk av eID i ansattsammenheng.

6.3.7 Særlig om bruk av fødselsnummer

Av personopplysningslovens § 12 følger det at «Fødselsnummer og andre entydige identifikasjonsmidler kan bare behandles når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering».

Vi kan som utgangspunkt anta at i systemer som arbeidsgiver har kontroll over som for eksempel ansattes PC og Microsoft 365, vil ikke fødselsnummer være nødvendig fordi det er andre gode metoder for å identifisere personen. Derimot, når den ansatte skal logge inn i for eksempel Altinn, NAV og Skatteetaten, krever disse løsningene entydig identifisering med personlig innlogging.[47] Det

[45] pvf. artikkel 4 nr. 11
[46] Se mer i EDPB guideline 2/2019, og uttalelser fra tidligere Article 29 Working Party i (WP 114)
[47] Se også om skillet mellom innlogging med virksomhetssertifikat og personlig sertifikat i kap. 2.3.1.

samme gjelder for helsepersonell som generelt jobber i en sektor der det ofte er krav til identifisering i tjenestene som benyttes. I mange tilfeller vil arbeidsgiver ha et saklig behov for sikker identifisering og behandling av fødselsnummer fordi ansattes eID er nødvendig for å oppnå identifiseringen. Se også punkt 6.3.1.

6.4 Personvernkonsekvenser

For alminnelig autentisering med eID er det et nokså begrensede sett av personopplysninger som behandles, se kapittel 4.4.1.

Det påhviler behandlingsansvarlig likevel en plikt til å kartlegge den konkrete persondatabehandlingen som gjennomføres og om det foreligger noen relevant risiko. I den sammenheng er det naturlig og samtidig vurdere eventuelle personvernulemper.

Enkelte relevante risikofaktorer kan være:

- At eID-en (mis)brukes av andre som har eller får tilgang til samme enhet som den ansatte,
- Tap av utstyr. Risikoen kan normalt begrenses ved at det kreves en kode for at utstyret kan tas i bruk for autentisering.
- Det vises til redegjørelsen for tilleggsrisiko ellers i kapittel 4.3.
- I tillegg bør det vurderes om det foreligger konkrete risikofaktorer eller personvernulemper i det enkelte arbeidsforhold.

For spørsmålet om det kreves en Data Protection Impact Assesment (DPIA) er vurderingstemaet om behandlingen utgjør en «*høy risiko for fysiske personers rettigheter og plikter*», jf. GDPR art. 35 nr. 1. I den vurderingen må det også sees hen til hvilke personopplysninger som behandles, jf. vurderingen ellers i denne delen. Forutsatt alminnelig aktsom bruk av eID-en, vil det i forbindelse med autentiseringen normalt ikke foreligge risikofylt persondatabehandling for individet i slik grad at kravet til DPIA utløses.

6.5 Andre rettigheter etter GDPR

Personvernforordningen gir den registrerte en del rettigheter knyttet til den behandlingen av personopplysninger som foretas. Det er viktig at den behandlingsansvarlige sørger for at de er i stand til å ivareta de registrertes rettigheter. Dette kan gjøres ved at den behandlingsansvarlige har retningslinjer for hvordan organisasjonen håndterer de registrertes forespørsler samt de frister mv. som gjelder ved oppfyllelse av rettighetene. En detaljert beskrivelse av den registrertes rettigheter i forbindelse med behandling av personopplysninger kan leses på Datatilsynet sine nettsider.

6.6 Sjekkliste

- Definer virksomhetens rolle, se kapittel 6.1. Det forutsettes at arbeidsgiver normalt er behandlingsansvarlig for autentisering som ledd i utførelsen av en arbeidsoppgave.
- Angi formålet ved behandlingen.
- Undersøk om det finnes brukervilkår knyttet til den eID-ordningen din organisasjon velger som tilsier at den ikke kan brukes slik dere ønsker.
- Sørg for å tilrettelegge slik at den ansatte kan bruke sine rettigheter knyttet til den behandlingen av personopplysninger som foretas.
- Foreta en kartlegging av den konkrete persondatabehandlingen som gjennomføres og om det foreligger noen relevant risiko.
- Har dere som behandlingsansvarlig gjort en vurdering av behandlingsgrunnlaget for bruk av eID på arbeidsplassen? GDPR art. 6 bokstav f er identifisert som et aktuelt

behandlingsgrunnlag, men det kan også finnes alternative eller supplerende behandlingsgrunnlag som er bedre egnet for den konkrete behandlingen, jf. kapittel 6.3.

- Gitt at GDPR art. 6 bokstav e eller f er behandlingsgrunnlag må den ansatte informeres om sine rettigheter etter GDPR art. 21.
    - Under vurderingen av GDPR art. 6 bokstav f bør følgende vurderes, og vurderingen må kunne dokumenteres:
        - Er det en saklig grunn basert på arbeidstakers arbeidsoppgaver for bruk av eID på sikkerhetsnivå «betydelig» eller «høyt»?
        - Ansees bruk av eID som nødvendig eller finnes det andre alternativer som med rimelighet kan oppfylle samme formål?
        - Foreta en interesseavveining av inngrepet overfor den enkelte, veid opp mot behovet for å gjennomføre behandlingen. Under både nødvendighetsvurderingen og interesseavveiningen er det relevant å trekke inn valget mellom privat ID og ansatt-eID. Er det foretatt en personvernvurdering av fordeler og ulemper ved de ulike eID-ordningene for virksomheten og de ansatte? Blant annet:
            - De konkrete forskjellene ved bruk av privat ID og alternative løsninger slik som ansatt-eID, jf. kap. 2.2.2 flg.
            - Eventuell risiko og personvernulemper for den ansatte.
            - Hvorvidt den ansatte protesterer mot behandlingen.

7 Sjekkliste (Overordnet)

Steg 1

Kartlegging og informasjonsinnhenting

1. Fortrinnsvis før eID tas i bruk i arbeidssammenheng, bør arbeidsgivere vurdere:

- Nødvendighetsvurdering
    - Er bruk av eID på aktuelt sikkerhetsnivå berettiget ut ifra et reelt behov (nødvendig)?
- Risikovurderinger og gjennomgang av informasjonssikkerheten
    - Undersøk risiko for sikkerhetsbrudd, herunder svindel, tap/misbruk av utstyr og tilgangskoder, bruk av engangspålogging, angrep mot virksomhetens IKT-systemer mv. Hvilken risiko innebærer bruken av eID i virksomheten?
    - Bør bruk av eID være forankret i virksomhetens strategi, jf. eForvaltningsforskriften § 15?

Steg 2

2. Valg av løsninger:

Overordnet bør det tas stilling til om det skal anvendes privat eID - eventuelt med tilpasninger for bruk i arbeidsforholdet, eller om det skal benyttes en ansatt-eID. Se nærmere om begrepene i kapittel 2.2.2.

I tillegg til risikovurderingen i steg 1, bør denne vurderingen blant annet adressere følgende punkter:

- Økonomiske hensyn
    - Kostnad for anskaffelse av eID og tilhørende nødvendig utstyr.
    - Kartlegging av hvor mange ansatte som trenger eID. Herunder hvor mange med eksisterende privat eID som de ønsker å benytte i arbeid.
    - Hvor omfattende og tidkrevende blir en eventuell omlegging, sett opp mot risikoen ved bruk av eksisterende system og løsninger.
- Effektivitetshensyn
    - Tidsbesparelsen ved å ta i bruk eksisterende private eID-ordninger, fremfor å anskaffe nye ansatt-eID-er.
- Juridiske vurderinger
    - Gjennomfør steg 1 i sjekklisten for den arbeidsrettslige vurderingen, se kap. 5.4.
    - Er det ønskelig å sette begrensninger for bruken av eIDen som benyttes i arbeidet? I så tilfelle kan det vurderes en ansatt-eID, jf. kap 5.2.2.2.
    - Gjennomfør sjekklisten for den personvernrettslige vurderingen, se kap. 6.6 – som blant annet oppstiller vurderingstema for valget mellom ansatt-eID og privat eID. Enkelte av vurderingene må foretas etter konkret eID-ordning er valgt (Steg 3).
    - De arbeids- og personvernrettslige vurderingene vil gi et godt grunnlag for å vurdere hvilken løsning som bør velges. Om nødvendig kan det foretas en konsekvens- og risikovurdering ved ikke å tilby en ansatt-eID.

Steg 3

3.1 Ved valg av en Privat eID:

- Arbeidsrettslig vurdering:
    - Gjennomfør steg 2 og 3 i sjekklisten for den arbeidsrettslige vurderingen, kapittel 5.4
- Personvernrettslig vurdering:
    - Gjennomfør relevante tilleggsvurderinger for bruk av valgt privat eID etter sjekklisten i kapittel 6.6, deriblant konkrete vurderinger rundt behandlingsgrunnlaget, og konkret risiko.

3.2 Ved valg av en Ansatt-eID:

- Arbeidsrettslige vurdering:
    - Gjennomfør steg 2 i sjekklisten for den arbeidsrettslige vurderingen, kapittel 5.4. Steg 3 forutsetter bruk av privat eID, men kan gjennomføres så langt det passer. I sin alminnelighet vil det ansees å ligge innenfor arbeidsgivers styringsrett å utstyre sine ansatte med en ansatt-eID som arbeidsgiver administrerer, anskaffer og betaler for.
- Personvernrettslig vurdering:
    - Gjennomfør relevante tilleggsvurderinger for bruk av valgt ansatt-eID etter sjekklisten i kapittel 6.6, deriblant konkrete vurderinger rundt behandlingsgrunnlaget, og konkret risiko.
    - I noen grad vil vurderingene være sammenfallende med vurderingen av privat eID. Et tilleggsmoment er at ansatt-eID generelt innebærer et sterkere skille mellom den profesjonelle og private sfære.

8 Hvordan bruke denne veilederen?

Veilederen består av to hoveddeler. Del 1 (kapittel 5 og 6) gir informasjon og vurderinger arbeidsgiver bør ha med seg i beslutningsprosessen. Del 2 (kapittel 4) forklarer hvilken informasjon som bør gis til arbeidstaker. Det er også utarbeidet en sjekkliste som arbeidsgiver kan følge.

Veilederen har også en del som beskriver mer utdypende om hva en eID er og hvordan dette reguleres generelt. Videre er det utarbeidet en begrepsliste med forklaringer om hvordan de ulike begrepene skal forstås i denne veilederen. Til sist vil det komme en samleside med ofte stilte spørsmål.

For beslutningstakere som skal foreta mer grundige vurderinger anbefales det å gjennomgå informasjonen i veilederen, deriblant:

- Fra del 1 - kap. 5 og kap. 6 (eller «*for arbeidsgiver*» i webutgaven)
- Fra del 2 - kap. 4 (eller «*for arbeidstaker*» i webutgaven)
- Deretter følge sjekklistene. Sjekklistene er ikke ment som fasit, men en anbefaling om fremgangsmåte i forbindelse med bruk av eID i arbeidssammenheng, herunder en trinnvis fremstilling med de hensyn og vurderinger som ansees aktuelle.

Det er ikke nødvendigvis meningen at brukere skal lese hele veilederen fra A til Å. Ulike deler av veilederen vil være mer eller mindre relevante avhengig av de forskjellige arbeidsforholdene, avtalene og praksisen rundt bruken av eID som finnes i dag.

Ved konkrete spørsmål om bruk av eID i arbeidet, kan sende dette via tilbakemeldingsmekanismen nederst på siden. Utvalgte spørsmål som ansees å ha generell rekkevidde vil kunne inntas sammen med en besvarelse på siden for «Spørsmål og svar».

9 Spørsmål og svar

(Vil oppdateres etter publisering med innkomne spørsmål og svar.)