Byrådsavdeling for finans

Oslo

Notat

Til: Sølve Monica Steffensen
Fra: Byrådsavdeling for finans

Vår ref. (saksnr.):	Saksbehandler:	Dato:
22/4876 - 22	Geir Faremo, 958 13 943	24.01.2023

Oslo kommunes høringssvar på veileder for bruk av eID for ansatte i offentlig forvaltning.

Oslo kommune viser til Kommunal- og distriktsdepartementets (KDD) brev av (02.12.2022) der departementet ber om tilbakemelding på utkast til veileder for bruk av eID for ansatte i offentlig sektor.

Oslo kommune har i et tidligere høringsbrev (19.08.2022) pekt på at dette (Hva er "dette"? eID for ansatte generelt eller utarbeidelse av denne konkrete veilederen?) er et godt initiativ og at kommunen støtter dette. I dette svaret peker Oslo kommune på problemstillingen med ansattes bruk av (privat?) eID, altså noe dette utkastet til veileder skal svare på.

KDDs utkast til veileder gir en inngående innføring i ulike forhold knyttet til bruk av eID i arbeidssammenheng, og ser ut til å svare på de fleste av spørsmålene kommunen som arbeidsgiver har knyttet til ansattes bruk av eID.

Dette er et krevende område, og - selv om veilederen er god - gir den likevel ikke tydelige svar i alle sammenhenger. Det er fortsatt flere avklaringer som må gjøres av arbeidsgiver, og som foreliggende veileder ikke besvarer

Innspill til veilederen fra Oslo kommune

Veilederen kan bli enda tydeligere på en del arbeidsrettslige forhold
Det er flere områder som er uklart i veilederen mht. til arbeidsrettslige problemstillinger og som med fordel kan spisses:.

Arbeidsrettslige forhold knyttet til bruk av eID må vurderes konkret. I foreliggende utkast til veileder er det uklart for Oslo kommunen hvilke eventuelle rettslige utfordringer som kan oppstå, veilederen kunne gjerne omhandlet dette noe mer.

Hvorvidt arbeidsgiver kan pålegge bruk av privat eID innenfor styringsretten er uklart.
Veilederen kan med fordel være tydeligere her.

Av KDDs utkast til veilederen fremgår det at det "generelt er 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". Veilederen bør være mer tydelig på hvor grensene for denne styringsretten går.

Drøfting av behov og konkret bruk av privat eID i arbeidsforhold må vurderes i hvert tilfelle. Likeledes om dette forutsetter avtaler med den enkelte eller kollektive avtaler. Veilederen viser i pkt. 5 til et vidt spekter av vurderinger for bruk av eID i et arbeidsrettslig perspektiv. Hvilke tiltak som er aktuelle er det vanskelig å si noe om før vi vet hvilke arbeidsprosesser i kommunen som forutsetter bruk av privat eID.

Hvordan ivareta like vurderinger knyttet til styringsretten
Utkastet til veileder legger opp til at hver enkelt organisasjon selv skal vurdere om det kan pålegges bruk av eID for ansatte. Det kan derfor fort gjøres forskjellige vurderinger i ulike virksomheter. For å motvirke dette vil det vært nyttig at veilederen inkluderer noen gode eksempler på slike vurderinger som virksomhetene kan benytte.

Veilederen bør også omtale eID for de med utenlandsk bakgrunn
Dette berører først og fremst de som bruker kommunens tjenester, men kan nok berøre enkelte ansatte også etter hvert som bruken av eID i forvaltningen øker. Dette vil skape ytterligere behov for utvikling av en egen eID løsning for ansatte.

Veilederen bør si noe om en ansatt med flere roller eller stillinger
Det er viktig at eID for ansatte klarer å håndtere flere roller og/eller ansattforhold i en kommune. Hvordan dette løses bør beskrives i veilederen.

Konsekvent begrepsbruk knyttet til personvern:

Personopplysningsloven, personvernreglementet, GDPR og personvernforordningen benyttes om hverandre. Oslo kommune anbefaler at veilederen konsekvent bruker ett av disse begrepene.

GDPR og personvernforordningen benyttes om hverandre ved angivelse av konkrete lovbestemmelser. Oslo kommune anbefaler konsekvent bruk av begrepet «GDPR»

Bestemmelser i GDPR nevnes på ulike måter, for eksempel GDPR art. 6 (1) og GDPR art. 6 nr. 1. Vi anbefaler konsekvent bruk av en betegnelse

2.2.2

I kapittel 2.2.2 har utkastet til veileder en nærmere redegjørelse produktene privat-eID og ansatt-eID. I denne sammenheng burde det også vært nevnt at ansatt-eID generelt innebærer et sterkere skille mellom den profesjonelle og private sfære. Dette er et såpass viktig moment at det bør nevnes i dette kapittelet.

2.4 utfordringer ved bruk av eID i arbeidsforhold

I andre avsnitt under dette punktet drøftes problemstillingen mht. rolleuklarhet i bruk av personlig eID i arbeidsforhold. Denne omtalen er begrenset til tjeneste- og varekjøp i offentlig sektor. Dette er bare ett av mange eksempler på den rolleuklarheten som oppstår når personlig eID benyttes i jobbsammenheng. Dvs. utfordringen med at når man bruker en personlig eID så agerer man i egenskap av privatperson / borger, ikke som ansatt. Etter Oslo kommunes vurdering kan veilederen gjerne gå lenger mht, å problematisere dette.

Kap. 3.2.3:

I første avsnitt vises det til personvernprinsippene, jf. GDPR art. 5, og at disse også gjelder for arbeidsgivers behandling av ansattes personopplysninger. Det savnes en nærmere redegjørelse av disse prinsippene samt en vurdering av disse sett opp mot behandling av personopplysninger ifm. bruk av eIDi (Dette burde også legges inn som punkt i sjekklisten).

Kap. 4:

Oslo kommune anbefaler KDD å se nærmere på hvorvidt innholdet i dette kapittelet samsvarer med navnet på kapitlet.

Videre anbefaler vi å flytte teksten under kap. 4.4 til kap. 6, jf. informasjonsplikt ved behandling av personopplysninger (her bør veilederen påpeke at ivaretakelse av denne plikten er avgjørende for at arbeidstaker kan ivareta øvrige rettigheter.)

Kap. 4.3: tilleggsrisiko, andre kulepunkt

Her nevnes risikoene ved bruk av personlig eID på delte enheter, som er betydelige. Bør det være en tydelig anbefaling om at dette ikke skal forekomme? Erfaringen fra Oslo kommune er at forsøk på å innføre denne typen løsninger har ført til bekymringsmeldinger fra de ansatte, som igjen har medført at løsningene har måtte bygges om.

Kap. 4.4.1.2:

I Kapittel 4.4.1.2 redegjøres det for hvilke personopplysninger som lagres i ID-porten, og hvem som er behandlingsansvarlig for dem. I dette punktet om ID-porten savner vi en kort innledning om hva ID-porten er, og hva slags tjenester denne fellesløsningen dekker. Det er ikke alle virksomheter som er kjent med dette.

Kap. 5:

Av dette kapittelet (side 24) fremgår det ikke hvilken konkret hjemmel i lov eller forskrift som pålegger anskaffelse og bruk av eID i et arbeidsforhold. eForvaltningsforskriften har bestemmelser om forvaltningsorgans anskaffelse og bruk av sikkerhetstjenester, herunder

virksomhetssertifikater i kapitlene 4-6. Veilederen bør også ha en gjennomgang av disse bestemmelsene. Veilederen omhandler arbeidsgivers muligheter til å bruke styringsretten til å pålegge ansatte å bruke privat eID på side 24, 25 og 30-31(sjekklisten). Oslo kommune opplever også at vurderingene som er gjort på sidene 24 og 25 virker strengere enn det som fremgår av fremgangsmåten i sjekklisten på sidene 30-31. Det vil være en fordel om veilederen er konsekvent.

Kap.5.4:

Kapittel 5.4 inneholder en sjekkliste for arbeidsgiver. Steg 1 i sjekklisten har punkter om kartlegging av behovet og hvilke oppgaver som skal løses ved bruk av eID og/eller elektronisk signatur og om behovet for dialog med ansatte /tillitsvalgte når dette skal innføres i virksomheten (Merknad: riktig forstått?). Siden det finnes flere ulike leverandører av eID-er, både innenfor private eID- og ansatt-eID-ordninger, se kapittel 2.2.2, burde det fremgå eksplisitt i sjekklistens steg 1 at virksomheten, og de ansatte, må foreta en vurdering av hvilken løsning som er best egnet for å ivareta deres konkrete behov.. I tillegg bør veilederen opplyse om at ansatt-eID generelt vil innebære et sterkere skille mellom den profesjonelle og private sfære, ref. side 40. (ref. Også tilsvarende under pkt. 5.4.) Veilederen har også en sjekkliste i kapittel 7 som er overordnet. Når arbeidsgiver skal gjøre sine vurderinger, må man forholde seg til begge sjekklistene. Oslo kommunen opplever at dette kan bidra til å gjøre prosessen mer tungvint, og at det derfor ville være mer brukervennlig om veilederen kun hadde én sjekkliste.

Kap. 6:

Etter Oslo kommunes vurdering er ikke overskriften på dette kapittelet Ikke helt treffende. Vi foreslår at at KDD heller vurdere tittelen «Arbeidstakers rettigheter etter GDPR» (ref. punkt over – få inn beskrivelse/redegjørelse av informasjonsplikten her) (Merknad: her er det et eller annet som mangler i den siste linjen dvs. det som står i parentes.

Kap. 6.1:

I avsnitt 4 i kapittel 6.1 omhandler det scenarioet at en ansatt logger seg innpå en offentlig tjeneste med sin private eID for å utføre arbeidsoppgaver pålagt fra arbeidsgiver. Det står videre at det i denne sammenheng vil være fire separate aktører som er behandlingsansvarlige for hver sin bruk, og som må oppfylle de krav som følger av personopplysningsregelverket. I avsnittet nevnes det tre eksempler, den ansattes valgte eID-løsning, ID-porten og den offentlige tjenesten som brukeren logger seg inn hos. Dette tilsvarer også aktørene gjennomgått i kapittel 4.4.1.1 flg. Om det er en fjerde aktør bør også denne nevnes i dette avsnittet. Om det er arbeidsgiver som er den fjerde aktøren, bør veilederen gjøre rede for arbeidsgivers rolle i dette scenarioet og hvilke personopplysninger arbeidsgiver eventuelt har behandlingsansvar for.

Kap. 6.2 - 6.6

Kapitlene 6.2 – 6.6 gir en gjennomgang av hvordan man skal gå frem når man som behandlingsansvarlig skal behandle personopplysninger. Etter Oslo kommunes vurdering synes

det som at disse kapitlene gir veiledning for de tilfellene hvor arbeidsgiver har et behandlingsansvar ved den interne bruken av eID i arbeidsforholdet, og ikke det tilfellet når den ansatte logger seg inn på en privat eller offentlig tjeneste. I så fall bør veilederen opplyse om dette, f.eks. med en avsluttende setning i kapittel 6.1.1.

Bruk av begrepet tjenestebruker / bruker

Det følger av KDDs forslag at i veilederen brukes begrepet «Privat eID» om eID-er på høyt sikkerhetsnivå betydelig og høyt «som ikke utelukkende er ment for bruk i arbeid». Det fremstår her som at privatpersoner har anskaffet privat eID, f.eks. BankID for fortrinnsvis å bruke det i sitt arbeid. Realiteten er at privatpersoner har anskaffet seg privat BankID for å håndtere sine private banktjenester. De siste par årene har dette blitt utvidet til å omfatte privatpersonens personlige signatur på digitale plattformer. Enhver bruk av privat eID vil være knyttet til privatpersonen, uansett om hen benytter seg av en tjeneste for å kunne utføre sine arbeidsoppgaver på best mulig måte. Siden det ikke finnes noen legaldefinisjon av privat eID, mener Oslo kommune at departementet i denne veilederen ikke bør gi begrepet et eget innhold som i liten grad gjenspeiler realiteten. Veilederen skal gi retningslinjer om bruk av eID for ansatte. I mangel av en legaldefinisjon og andre rettskilder, vil begrepsavklaringen som gis i denne veilederen kunne få betydning utover rettsområdet som veilederen dekker.

Oslo kommunen mener at begrepsbruken i veilederen bør gjenspeile virkeligheten. Kommunen foreslår derfor følgende definisjon av begreper privat eID:I denne veilederen brukes begrepet privat eID om eIDer på sikkehetsnivå betydelig og høyt som er utstedt etter arbeidstakers initiativ og som er ment for privat/personlig bruk.

Bruk av begrepet tjenestebruker / bruker

I utkastet til veileder benyttes begrepet tjenestebruker/bruker om en fysisk person som benytter seg av elektronisk identifikasjon eller tillitstjenste. I denne veilederen vil dette ofte innebære det samme som den ansatte. De ansatte i offentlig forvaltning benytter seg av digitale tjenester både i kraft av seg selv, f.eks. internt i virksomheten, og på vegne av arbeidsgiver. I det siste tilfellet er det i realiteten arbeidsgiveren som er tjenestebruker/bruker. Den ansatte representerer her sin arbeidsgiver. Siden enhver bruk av elektroniske tjenester etterlater seg spor, bør det synliggjøres når en ansatt opptrer på vegne av seg selv, og når den ansatte opptrer på vegne av arbeidsgiver. Tjenestebruker/bruker kan være både en fysisk og en juridisk person, ref. også eIDAS sin definisjon av eID (gjengitt i veilederen).

I beskrivelsen av begrepet bør det derfor gjøres et tydelig skille mellom de situasjonene i et arbeidsforhold hvor den ansatte opptrer på vegne av seg selv, og når hen opptrer på vegne av sin arbeidsgiver.

Tor Fjellstad

konst. seksjonssjef

Geir Faremo

fagsjef