1 Framtidig situasjon

Dette er en beskrivelse av en framtidig situasjon – hvordan det kan se ut når vi har fått en styrket og mer helhetlig tilnærming til informasjonssikkerhet og personopplysningsvern i forvaltningen. Det er en skisse av ønsket framtidig situasjon, hvor hensikten er å vise fram noen av mulighetene som finnes.

1.1 For virksomhetene i forvaltningen

Sikkerhetsnivået er løftet i mange virksomheter i stat og kommune, noe som har gitt **styrket grunnleggende sikkerhet på tvers av forvaltningen**. Ledere i disse virksomhetene er fornøyde og har bedre oversikt og styring enn tidligere. Aktiv styring fører til stadig mer kostnadseffektivt arbeid med informasjonssikkerhet og personopplysningsvern.

Kommuner, fylkeskommuner og statlige virksomheter utvikler brukerrettede, sammenhengende og effektive digitale tjenester. Rammevilkårene for utvikling av tjenester i felles økosystem vektlegger **evne til samarbeid og samstyring**, og bidrar til gjensidig tillit mellom tjenesteeiere som er avhengige av hverandre. Når de samarbeider om sammenhengende tjenester og deler data, benytter de de samme styringsaktivitetene og basisnivåene med sikkerhets- og personverntiltak. De synes derfor det er enklere å samarbeide og samstyre risiko for tjenestene. Godt samarbeid gir bedre sikkerhet og bidrar til redusert ressursbruk på informasjonssikkerhet og personopplysningsvern.

Virksomhetene synes det er **enklere og mer effektivt å anskaffe tjenester** hvor leverandører må bidra til tilstrekkelig informasjonssikkerhet og personopplysningsvern. Næringslivet synes det er enklere å tilpasse og tilby tjenester til offentlig sektor.

Virksomhetene har tilgang til gode **anbefalinger og veiledning som henger sammen**, og er orientert rundt deres perspektiv. De har tilgang på stadig flere **hjelpemidler og støtteprodukter** til bruk i sitt arbeid med informasjonssikkerhet og personopplysningsvern.

Felles anbefalinger fra veiledningsaktørene bidrar til at virksomhetene har gode rammebetingelser for arbeidet med informasjonssikkerhet. Sammen med god veiledning er det **lett å gjøre rett, og ivareta forpliktelser** i ulike regelverk.

Mange virksomheter bruker stegvise resultatorienterte "snarveier" som gjør det **enkelt for dem å få på plass det mest vesentlige**. Det er ikke tilstrekkelig for å oppfylle kravene i alle regelverk, men «snarveiene» gjør det enklere å komme i gang med å få på plass det som er anbefalt. De er spesielt egnet for umodne virksomheter som synes det er vanskelig å ha

helhetlig, selvstendig styring, slik regelverkene pålegger dem. En slik "snarvei", som hjelper virksomhetene med å få på plass grunnleggende sikkerhetstiltak, er illustrert i denne figuren:

Figur 1 – Virksomhetene får hjelp til å finne svar på sentrale spørsmål

Et perspektiv på framtidig situasjon for virksomhetene er illustrert i vedlegget *Nå og i framtiden*.

1.2 Felles anbefalinger

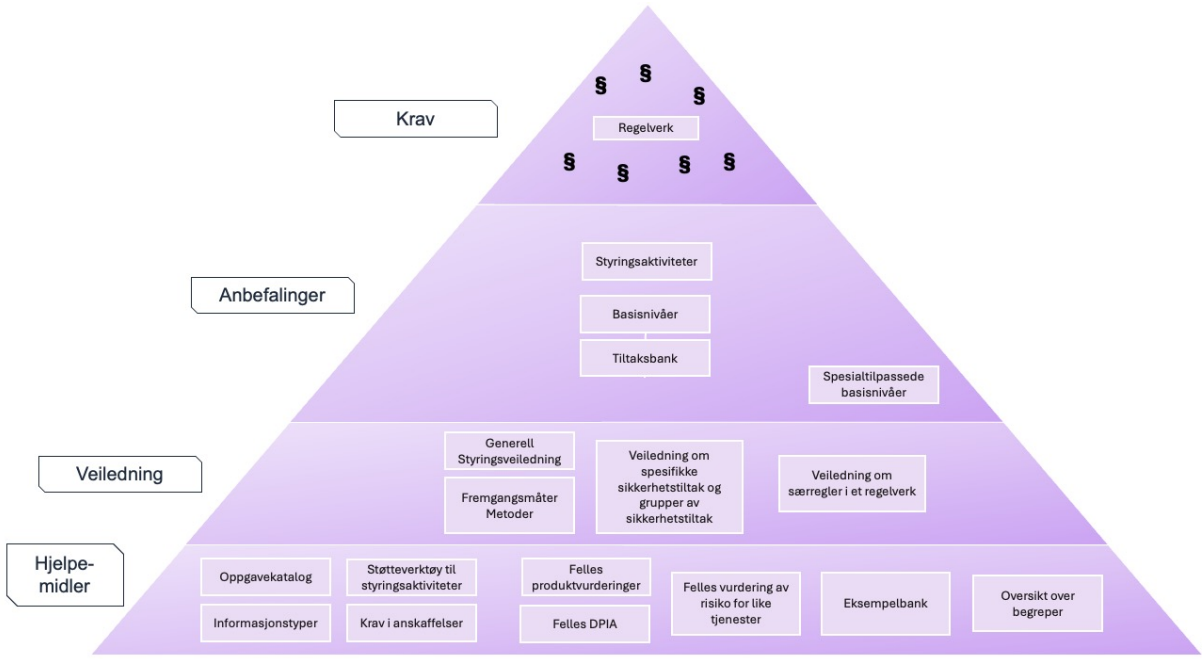
Det er publisert felles anbefalinger til offentlige virksomheter om hva de bør ha på plass for å være i stand til å ha god styring av informasjonssikkerhet og personopplysningsvern, og ha et tilstrekkelig og forsvarlig sikkerhetsnivå for sine oppgaver og tjenester.

Virksomhetene får felles anbefalinger om styringsaktiviteter, sikkerhetstiltak og personverntiltak. Det er anbefalt at alle offentlige virksomheter

- har disse styringsaktivitetene
- tar utgangspunkt i basisnivåene når de skal etablere sikkerhetstiltak for sine oppgaver og tjenester
- benytter tiltaksbanken ved valg av ytterlige sikkerhetstiltak

1.3 Anbefalinger, veiledning og hjelpemidler

Det er lett å se sammenhengen mellom felles anbefalinger og utfyllende veiledning. Veiledning henviser til anbefalingene, og veiledningsaktørene forklarer hvilke deler av det som er anbefalt de veileder om. Det er tydeligere hva som er anbefalt, og hvilken veiledning som er til hjelp for å få det til i praksis.



Figur 2 – Felles anbefalinger henger godt sammen med veiledning og hjelpemidler (se større figur i vedlegg)

Veiledning er enten generell, eller spesielt rettet inn mot etterlevelse av krav i ett bestemt regelverk – men benytter alltid anbefalingene som samlende punkt for virksomhetene. Dette gjør virksomhetene i bedre stand til å arbeide helhetlig og etterleve alle regelverk.

Veiledning, hjelpemidler og støtteverktøy henger godt sammen og hjelper virksomhetene til å få ting til i praksis. Det er tydelig for brukerne hva som er særskilt for enkelte regelverk eller veiledningsaktørers ansvarsområder.

Det er lett for brukerne å finne frem i anbefalinger, veiledning og hjelpemidler. Der finner brukerne den informasjonen og hjelpen de trenger i sin situasjon.[1]

1.4 For veiledningsaktørene

Veiledningsaktørene har samordnet seg. De har endret måten de arbeider på for å tilrettelegge for styringsevne og tilstrekkelig informasjonssikkerhet og personopplysningsvern i offentlige virksomheter. De har tilpasset eksisterende produkter og utviklet nye produkter for ulike målgrupper.

Det er ikke lenger vanntette skott mellom veiledningsaktørene og deres ulike veiledningsprodukter. De har utviklet og lansert **felles anbefalinger** og sørget for god sammenheng i anbefalinger, veiledning og hjelpemidler orientert rundt brukernes behov.

[1] Hvordan man praktisk skal få dette til er ikke utredet. Det kan være mulig å lage løsninger med referanser/lenker og metadata, eller det kan være mulig å samle så mye som mulig på ett sted.

1.4.1 Samordning og styring

Veiledningsaktørene har etablert en styringsmodell for å utvikle de felles anbefalingene og skape god sammenheng med veiledning og hjelpemidler. Styringsmodellen er forankret i hver organisasjon, og det er godt samarbeid og god kommunikasjon og på tvers av veiledningsaktørene.

Samordnet innsats sørger for at fagspesifikk veiledning fra ulike veiledningsaktører samsvarer med, og tilbyr god hjelp til å følge, de felles anbefalingene.

Nye måter å samarbeide om produkter til nytte for virksomhetene i forvaltningen, fører til jevn utvikling av hjelpemidler og støtteprodukter i tråd med hvor det er størst behov for hjelp.

1.4.2 Forvaltning av felles anbefalinger

Føringer gis og beslutninger tas om forvaltningen av de felles anbefalingene. Dette utføres av et styringsråd med representanter fra departementer med ansvar for området, statlige myndigheter og KS.

Utviklingsprosessene er så transparente som mulig, og er strukturert på en måte som gir forutsigbarhet for brukerne. Endringer sendes på åpne innspillsrunder. Nye versjoner kunngjøres i god tid før de overtar for de gamle. Virksomheter i forvaltningen og næringsliv kan melde inn forslag til endringer. Interessenter blir aktivt involvert i videreutvikling og endringer.

Basisnivåer og tiltaksbank kommer i oppdaterte versjoner på en forutsigbar, periodisk måte. Det kommer som regel nye versjoner annethvert år. Tekniske sikkerhetstiltak blir oppdatert i takt med teknologiutviklingen. Anbefalinger om styringsaktiviteter har mindre behov for endringer på kort sikt, men blir forbedret og justert basert på innspill fra interessenter.

1.4.3 Enklere og mer effektivt

Veiledningsaktørene synes det er lettere å se ansvarsavgrensningene seg imellom, og enklere å samordne veiledning. Det er enklere å identifisere hvor det er udekket behov for hjelp til virksomhetene. De synes det er lettere å tilpasse[2] spesiell veiledning om de tingene som ikke er dekket av generell veiledning[3].

---

[2] Ulik veiledning kan tilpasses virksomheters størrelse og kompetanse, slik at det er lett å tilegne seg den kunnskapen som er nødvendig for å etterleve alle regelverk på en effektiv og forsvarlig måte.

[3] For eksempel generell veiledning om hvordan man kan gå fram for å gjennomføre styringsaktiviteten «vurdering av risiko», og spesiell veiledning om særkrav til «vurdering av risiko» i virksomhetssikkerhetsforskriften til sikkerhetsloven.

Samordning har ført til mindre dobbeltarbeid og at flere drar lasset sammen. Samordning har også redusert den totale arbeidsbelastningen på veiledningsaktørene.

1.4.4 Evalueringer og tilsynsvirksomhet

Virksomheter som driver tilsyn, inkludert mange av veiledingsaktørene, har nå bedre oversikt over hva som normalt må til for å etterleve de funksjonelle regelverkene. Der det er relevant, bruker tilsynsmyndighetene de felles anbefalingene når de forbereder tilsyn.

De som evaluerer tilstanden i forvaltningen, bruker de felles anbefalingene til å utarbeide hva de skal evaluere tilstanden på.

1.5 Offentlige anskaffelser

Offentlige virksomheter anskaffer produkter og tjenester som benyttes til informasjonsbehandlingen i oppgavene og tjenestene de har ansvaret for. Å ivareta dette på en god måte er også en del av arbeidet med å styre risiko for oppgavene og tjenestene.

Virksomhetene har oversikt over behov for informasjonssikkerhet og personopplysningsvern i sine oppgaver og tjenester, inkludert spesifikke sikkerhets- og personverntiltak som er nødvendige for å håndtere risiko på en god måte. Deler av disse behovene dekkes gjennom krav til leverandører av tjenester, inkludert digitale tjenester.

De felles anbefalingene brukes til å stille krav til leverandører – noe som gir effektiviseringsgevinst for begge parter. Det bidrar også til bedre oversikt og kontroll over verdikjedene.

- Basisnivåene brukes til å stille krav til sikkerhets- og personverntiltak, og til å gå opp ansvaret for disse tiltakene mellom kunde og leverandør
- Beskrivelse av styringsaktivitetene brukes til å stille krav til leverandører når det er behov for samhandling mellom kunde og leverandør i slike prosesser
- Leverandører av konsulenttjenester tar utgangspunkt i anbefalingene når de hjelper virksomhetene
- Deler av anbefalingene er tatt inn som krav i Statens standardavtaler (SSA)

1.6 Etterlevelse av regelverk

Regelverk forutsetter fortsatt at virksomhetene har evne til å utrede egne behov og tilpasse til sin størrelse, egenart og risiko. Det er nødvendig for at arbeidet er formåls- og kostnadseffektivt[4] i hver enkelt virksomhet.

Virksomhetene har bedre evne til å ha oversikt over og ivareta mange ulike hensyn: sin egen leveranseevne og økonomi, personvernet til de de behandler opplysninger om, egne ansatte,

[4] Både oppnå det man skal og ha en fornuftig ressursbruk for å oppnå det.

andre virksomheter, samfunnssikkerhet og nasjonal sikkerhet. Dette må de ha evne til fordi regelverk stiller krav til informasjonssikkerhet både eksplisitt og implisitt.[5] Like hensyn reguleres fortsatt noe ulikt. Regelverk har ulike formål, og er opptatt av ulike årsaker til hendelser, og å unngå ulike typer konsekvenser av dem.[6]

Kravene i mange regelverk kan oppsummeres slik:

- jobb risikobasert, integrert i øvrig styring av virksomheten
- ha tilstrekkelig arbeid med informasjonssikkerhet
- etabler egnede tiltak for å redusere risiko og oppnå et tilstrekkelig og forsvarlig sikkerhetsnivå

Til tross for ulikheter i forskjellige regelverk, så gjennomfører virksomhetene aktiviteter og etablerer tiltak som imøtekommer krav i flere forskjellige regelverk samtidig. Styringsaktivitetene er i all hovedsak de samme på tvers av virksomhetene. Tiltakene i basisnivåene passer for alle oppgaver og tjenester, for stort sett alle hensyn som skal ivaretas. Noen særkrav i regelverk ivaretar virksomhetene spesielt – for eksempel detaljer i gjennomføring av noen styringsaktiviteter, eller spesifikke sikkerhetstiltak de må etablere.

Ettersom det virksomhetene må gjøre for å etterleve disse regelverkene ofte er ganske likt, så abstraherer de felles anbefalingene delvis bort kompleksiteten i regelverkene, og gir virksomhetene et solid grunnlag for å ivareta alle sine forpliktelser. De forenkler også arbeidet for de virksomhetene som fortsatt har problemer med å få på plass et grunnleggende sikkerhetsnivå.

Forvaltningen av felles anbefalinger sørger for at de alltid er i henhold til eksisterende og kommende regelverk. Dermed er de nyttige for virksomhetene som skal etterleve endrede og nye regelverk.

1.7 Begrepsoversikt

Felles anbefalinger har fremtvunget avklaringer om bruk av en del sentrale begreper. Veiledningsaktørene har ryddet i begrepsbruken, og begreper i de felles anbefalingene samsvarer med begreper veiledningsaktørene bruker i sin veiledning.

---

[5] Krav til styring og kontroll, eller internkontroll, i økonomiregelverket i staten og kommuneloven stiller implisitt krav til informasjonssikkerhet for oppgavene og tjenestene virksomhetene har ansvaret for. eForvaltningsforskriften til forvaltningsloven, lov om nasjonal sikkerhet (sikkerhetsloven) og lov om digital sikkerhet er eksempler på regelverk med eksplisitte krav til informasjonssikkerhet.

[6] Det at ulike perspektiver gir ulikt fokus er beskrevet her: https://www.digdir.no/informasjonssikkerhet/ulike-perspektiver-gir-ulikt-fokus/2279

Det er likevel fortsatt slik at

- begreper benyttes ulikt i en lang rekke regelverk, og det vil være slik i overskuelig framtid.
- internasjonale standarder og referanseverk bruker begreper ulikt.
- det er flere fagområder med ulik historie involvert, og fagmiljøer bruker begreper ulikt.
- det er vanskelig å enes om felles beskrivelse av begreper på tvers av fagområder og -miljøer.

Virksomheter og veiledningsaktører har tilgang til en oversikt over begreper hentet fra krav, anbefalinger og veiledning. Oversikten er samlet i en database og er tilgjengelig for oppslag og søk på nett.

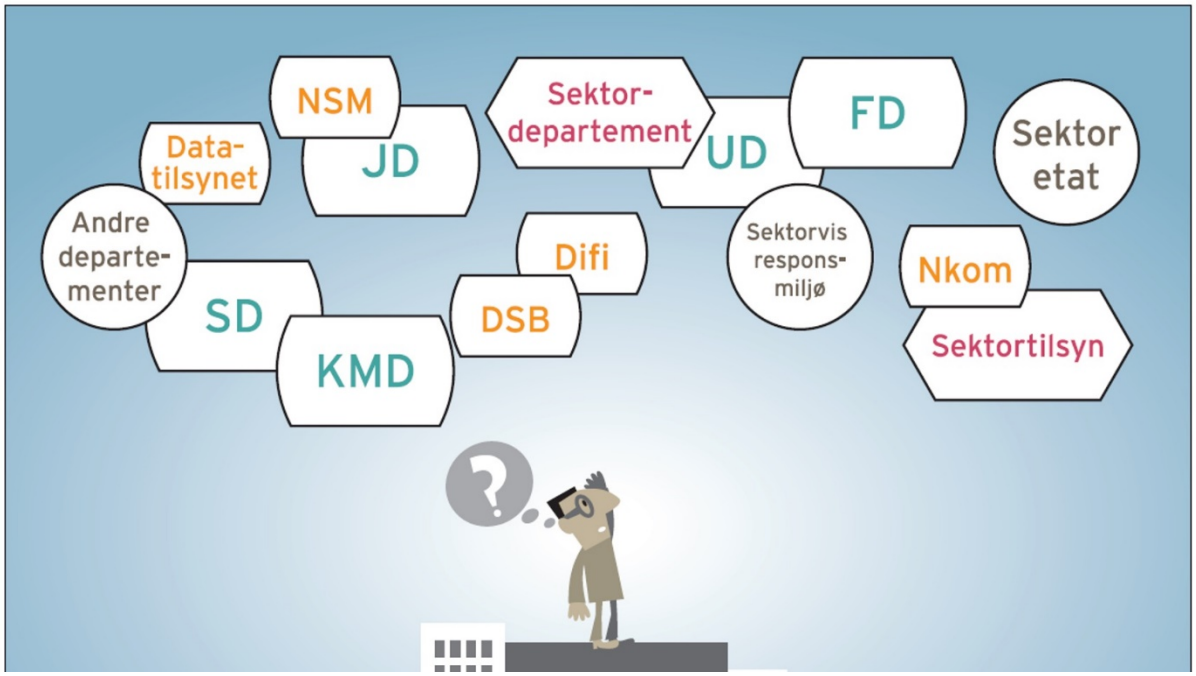
Oversikten er til hjelp for å forstå terminologi og bli oppmerksom på når det finnes flere beskrivelser av samme begrep. Oversikten gjør det også enklere å finne en beskrivelse man kan bruke i den situasjonen man er i. Et eksempel er forskjellen på innholdet i begrepet «informasjonssystem» i lov om nasjonal sikkerhet (sikkerhetsloven) og NIS-direktivet fra EU, som ligger til grunn for lov om digital sikkerhet.

Veiledningsaktørene forklarer begrepsbruken i veiledningen sin, spesielt begreper som kan ha litt ulik bruk andre steder, slik at det blir lett for brukerne å forstå begrepsbruken og sammenhenger på tvers av regelverk.

Veiledningsaktørene bruker begrepsoversikten når de forvalter eller utvikler veiledning. Over tid bidrar det til mer lik begrepsbruk, redusert begrepsforvirring og demper tendensen til å lage nye, unike beskrivelser i forskjellige sammenhenger.

1.8 Nå og i framtiden

1.8.1 Nå — figur fra NOU 2018:14



1.8.2 I framtiden