POLITIET

Strategi for fremtidig IKT-funksjon i politiet

Sammendrag

Versjon 1.0
Dato: 25.05.2018

1 Innledning

IKT-funksjonen[1] i politiet har gjennomgått store endringer de siste årene. Det er gjennomført en profesjonalisering gjennom etablering av IKT-avdelingen i Politidirektoratet og Politiets IKT-tjenester (PIT) som felles leverandør av IKT-tjenester. Lokale IKT-medarbeidere og IKT-løsninger i distriktene er overført til PIT for å gi bedre organisering og styring av hele IKT-funksjonen. Dagens IKT-funksjon er imidlertid fortsatt organisert som en tradisjonell IKT-virksomhet og anvender tradisjonelle metoder for prosjektgjennomføring og utvikling og forvaltning av politiets IKT-løsninger.

De siste årene er det gjennomført store og viktige tiltak for sikre og forbedre politiets IKT-infrastruktur og tilpasse IKT-løsningene til ny distrikts- og organisasjonsstruktur som følge av Nærpolitireformen. I hele perioden er det også levert endringer og ny funksjonalitet både via prosjekter og løpende forvaltning. Som Digitaliseringsstrategien påpekte er det imidlertid fortsatt et stort behov for å modernisere politiets eksisterende IKT-løsninger (ta inn etterslepet fra 2000-tallet) og for å utvikle nye digitale løsninger for å forbedre og effektivisere politiets oppgaveløsing.

De siste 20 årene har ikke utviklingen av politiets IKT-løsninger fulgt noen helhetlig plan eller arkitektur basert på en samlet forståelse av politiets behov for IKT-løsninger. Utviklingen har vært preget av at større og mindre funksjonelle behov har blitt løst ved å videreutvikle eksisterende applikasjoner eller ved å etablere nye enkeltløsninger. Dette har ført til at politiet nå har et fragmentert informasjons-, applikasjons- og teknologi- og infrastrukturlandskap som ikke støtter morgendagens behov.

"Strategi for fremtidig IKT-funksjon i politiet" har tatt utgangspunkt i virksomhetsstrategien "Politiet mot 2025" og Digitaliseringsstrategien, med de målene og ambisjonene som beskrives mot 2020 og 2025. Rask utvikling av sikre digitale løsninger vil være svært viktig for politiets evne til å realisere disse målene og ambisjonene. Fremover vil utvikling av digitale løsninger være enda tettere koblet mot virksomhetsutvikling i politiet enn i dag. Denne strategien er utformet for å gi en tydelig retning for politiets utvikling av digitale løsninger fremover og derigjennom bidra til raskere digitalisering og oppnåelse av virksomhetsstrategiens mål.

2 Politiets behov

Politiets virksomhetsstrategi og digitaliseringsstrategi stiller store krav til politiets utnyttelse av informasjon og teknologi. Virksomhetsstrategien utrykker at forebygging og etterretning er sentralt og skal gjennomsyre politiets måte å jobbe på slik at vi kan være **i forkant av kriminaliteten**, levere **tilgjengelige polititjenester med høy kvalitet** og være tilstede og skape **trygghet i det digitale rom**. For å klare dette må vi være **et moderne og kompetent politi**. Kriminelle nettverk og miljøer er innovative og med nye digitale muligheter har dette akselerert. Dette er en kontinuerlig utfordring for politiet. For å ligge i forkant må politiet derfor være nytenkende og innovative.

Alle deler av virksomhetsstrategien er avhengig av gode digitale løsninger for å kunne realiseres, men spesielt behovene knyttet til det å være "I forkant av kriminaliteten" og å skape "Trygghet i det digitale rom" stiller krav til politiets digitale løsninger som skiller seg fra det mange andre virksomheter står overfor. Dette er behov som det i liten grad kan kjøpes ferdige IKT-løsninger til i markedet og som markedet generelt har lite kompetanse på. Dette er i kjernen av politiets virksomhet og dermed områder der politiet selv må ha kompetanse og kapasitet til å utvikle digitale løsninger. "Tilgjengelige polititjenester med høy kvalitet" og "Et moderne og kompetent politi" er også utfordrende, men behovene her minner mer om behovene hos andre virksomheter og er også bedre kjent i markedet.

Politiet vil ikke kunne realisere målene og ambisjonene i virksomhetsstrategien innenfor eksisterende økonomiske rammer, hvis vi fortsetter vår IKT-utvikling slik vi gjør i dag. Politiets behov krever en helhetlig plan og tilnærming for utvikling av digitale løsninger. Dette gjelder både hva politiet skal ha av digitale løsninger i fremtiden og hvordan IKT-funksjonen skal levere disse. For å kunne lage gode,

[1] Med "IKT-funksjon" menes "de deler av politiet som er involvert i utforming, utvikling, videreutvikling, forvaltning og drift av politiets IKT-løsninger", dette inkluderer også prosesseiere og fagmiljøer i politiet

fremtidsrettede digitale løsninger må vi begynne å se alle delene av IKT-løsningene våre i sammenheng – ikke fortsette å løse behovene hver for seg. Dette dreier seg om å styre mer målrettet:

- Hvordan vi organiserer og forvalter **informasjonen** vår
- Hvordan vi deler inn, integrerer og utformer brukerflater for **applikasjonene** våre
- Hvilken **infrastruktur** vi etablerer
- Hvordan vi **sikrer** informasjonen og de digitale løsningene våre.

Vi må også ha en annen tilnærming til hvordan vi leverer IKT-løsninger enn det vi tradisjonelt har hatt. Vi må:

- Styre mer på **ønsket effekt** og mindre på tiltak
- Svare raskere på behov gjennom **hyppigere og mindre leveranser**
- **Utforske muligheter** som ny teknologi gir
- Levere mindre gjennom prosjekt og mer gjennom **kontinuerlig produktutvikling**
- Gjøre **mer selv** på områder som er politiets kjernevirksomhet og bruke markedet smartere
- Utnytte de mulighetene teknologien gir for å **levere IKT-løsninger mer effektivt**.

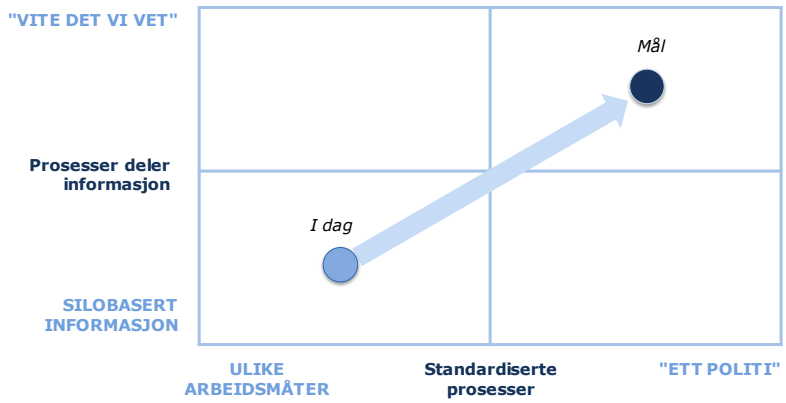
Begrensede ressurser (både mennesker og økonomi) og behov for kontinuitet i politiets tjenester og IKT-løsninger, tilsier at vi må modernisere "arven" og etablere nye digitale løsninger over tid. Samtidig har politiet et høyt ambisjonsnivå mot 2025, noe som ikke gir rom for store prosjekter som mislykkes eller går i feil retning. Vi må altså utvikle våre digitale løsninger etter en "Reguleringsplan for digitale løsninger" og vi må gjøre det på en annen måte enn i dag.

3 Fremtidige digitale løsninger

3.1 Fremtidige digitale løsninger vil drive utviklingen av politiet

Politiet må klare å utnytte datamaskiner til det de er gode til i dag (f.eks. mønstergjenkjenning), ikke bare det de var gode til for 20 år siden. Teknologianvendelsen skal være innrettet mot å forbedre politiets arbeidsprosesser og hvordan informasjon behandles, og den skal baseres på de overordnede behovene som uttrykkes i politiets virksomhetsstrategi.

Et av de viktigste bidragene fra IKT-funksjonen i politiet er å understøtte ønsket om "Ett politi" som løser like oppgaver på samme måte og som har tilgang til politiets samlede kunnskap i oppgaveløsingen.



Figur 1: Retning for digitale løsninger i politiet[2]

Felles digitale løsninger bidrar til standardisering av politiets prosesser og til å gjøre politiets tjenester mer tilgjengelige for innbyggere og virksomheter. Deling av informasjon på tvers av arbeidsprosesser, virksomhetsområder og enheter i politiet vil bidra til at vi kan jobbe enda mer kunnskapsbasert[3], evner å ligge i forkant av kriminaliteten og etterforsker og oppklarer kriminelle forhold.[4] Samtidig skal vi også

[2] Modell fra Weill & Ross, Enterprise architecture as strategy (2006)
[3] Et mer "informasjonsdrevet" politi
[4] Iht. de lover og regler som gjelder for deling av informasjon

sørge for at politiets behov for til dels meget spesialiserte digitale løsninger lar seg levere på en hensiktsmessig måte.

Politiets fremtidige digitale løsninger må ha innebygd noen viktige egenskaper som er sentrale for å møte behovene og realisere målene som uttrykkes i politiets overordnede strategier og føringer. Vi skal derfor:

- Tilrettelegge våre løsninger for samhandling på et **felles sett av informasjon** som kan anvendes på tvers av arbeidsprosesser
- Anvende **prosessautomatisering** til å effektivisere politiets oppgaveløsning og frigjøre tid til oppgaver som krever politikompetanse og tilstedeværelse
- Bruke **mønstergjenkjenning** og **kognitive teknologier** til å styrke vår evne til å ligge i forkant og avklare kriminalitet
- Tilby politiet **mobile løsninger** for å kunne utføre oppgaver der politiet er
- Styrke **selvbetjening** og **digital samhandling** i politiets tjenester
- Skape **notoritet** og ivareta **etterlevelse, informasjonssikkerhet og personvern** i vår behandling av informasjon.

3.2 "Reguleringsplan" for digitale løsninger

Hvis vi skal lykkes med digitalisering og virksomhetsstrategien må alle i IKT-funksjonen "bygge på den samme byen og følge den samme planen". Det betyr at vi må se informasjon, applikasjoner, teknologi og infrastruktur og sikkerhet i sammenheng når vi bygger våre digitale løsninger.

Informasjon

Politiet må øke sin evne til å behandle informasjon digitalt slik at arbeidsprosesser i enda større grad baseres på bl.a. kunnskap om kriminaliteten og for å øke samhandling internt og eksternt. Videre vet vi at den enorme informasjonsmengden som allerede eksisterer i dag vil øke eksponentielt i årene som kommer. Dette vil skape et stort gap mellom hva politiet evner å håndtere og hva vi forventes å håndtere, hvis ikke politiets behandling av informasjon digitaliseres ende til ende. Vi skal derfor:

- **Organisere og forvalte informasjonen** vår på en bedre måte slik at vi kan effektivisere informasjonsbehandlingen og utnytte kunstig intelligens og kognitive teknologier
- **Automatisere prosesser** for å fange, bearbeide og bruke informasjon - tiden vi benytter for å behandle informasjon må **gå mot null** for oppgaver som ikke krever manuell behandling og vurdering
- Legge til rette for et **informasjonsfelleskap** i politiet, hvor informasjon kan utnyttes på tvers av arbeidsprosesser, i tråd med lover og regler.

Applikasjoner

For å kunne behandle de store informasjonsmengdene, utnytte den datakraften som er tilgjengelig, benytte kognitive teknologier og tilby moderne brukergrensnitt må morgendagens applikasjoner planlegges, bygges og samhandle på en annen måte enn i dag – alle må følge den samme "reguleringsplanen". Den enkelte digitale løsning må defineres ut fra en helhet, ikke isolert. Over tid må alle dagens applikasjoner skiftes ut. Vi skal derfor:

- Ha et **helhetlig målbilde** for politiets applikasjonslandskap og applikasjoner
- Dele inn i **mindre komponenter** og gjøre endringer over tid
- Etablere en **arkitektur** som øker samhandling og deling av informasjon på en effektiv måte på tvers av applikasjoner og arbeidsprosesser
- Sikre at **brukeropplevelsen** står sentralt – grensesnitt skal tilpasses bruk og utstyr
- Sikre **kontinuitet** for politiets tjenester.

Teknologi og infrastruktur

For å kunne realisere fremtidig informasjons- og applikasjonslandskap gjennom en ny leveransemodell for IKT-funksjonen, må politiet ha en teknisk infrastruktur som gjør det mulig med kontinuerlig utvikling og produksjonssetting av ny funksjonalitet. Dette fordrer evne til å utnytte moderne plattformtjenester og skyteknologi. Politiet klarer ikke å utnytte de fordelene teknologien gir i utvikling og drift med applikasjoner på gammel teknologi og arkitektur – det representerer også en sikkerhetsrisiko. I tillegg må politiet ha en moderne infrastruktur for å kunne samhandle effektivt og benytte applikasjoner på tvers av arbeidssteder og ulikt klientutstyr.

Vi skal derfor:

- Modernisere **infrastrukturen for samhandling og tilgjengeliggjøring av applikasjoner** til sluttbrukere – dagens Origo-løsning dekker ikke politiets behov for samhandling, bruk av internett og tilgjengeliggjøring av applikasjoner
- Etablere en **skybasert infrastruktur for utvikling og drift av applikasjoner** – videreføre arbeidet med Organa-plattformen
- Etablere **infrastruktur for bruk i etterforskning og oppgaver**. Dette har vi ikke i dag, politidistrikter og særorgan løser det selv.
- Fortsette med å etablere **basis infrastruktur for oppbevaring og sikring, nettverk, prosessering og lagring** av applikasjoner og informasjon, både i privat, offentlig og allmenn sky.

Sikkerhet

En god sikkerhetsarkitektur skal sørge for evnen til å motstå digitale angrep og legge til rette for at sikkerhet blir ivaretatt på en balansert og riktig måte gjennom hele livsløpet til våre digitale løsninger. Politiets tekniske sikkerhetsarkitektur må gjenspeile *policy for klassifisering og verdivurdering*. Når informasjonen har blitt verdivurdert og klassifisert skal den sikres. Nødvendige sikringsnivå defineres ut fra risikonivå og da hovedsakelig basert på verdinivå. Vi skal derfor etablere en **helhetlig sikkerhetsarkitektur** som definerer nødvendige sikringsnivåer for å beskytte politiets digitale verdier

4 Fremtidig leveransemodell

I dag leveres IKT-løsninger og funksjonalitet gjennom tradisjonelle prosjekter eller gjennom mindre endringer og forbedringer i forvaltning av IKT-løsningene. Begge leveransemåtene har en sekvensiell tilnærming[5] med siloer og overleveringssteg mellom behovsspesifisering, utvikling, testing, lansering og drift – dette er ressurskrevende og tar lang tid.

Politiet har et stort innovasjonspress der vi raskt må reagere på endringer og trender både i det fysiske og i det digitale rom. For å realisere politiets komplekse behov og bygge fremtidsrettede digitale løsninger må veien fra idé til utvikling og utprøving derfor være kort og gjennomføres kontinuerlig, slik at vi raskt kan dra nytte av den læringen som gjøres.[6] Med dagens teknologi og metoder er det nå mulig å levere funksjonalitet kontinuerlig gjennom mindre og hyppigere leveranser, slik det også gjøres i virksomheter som lykkes med digitalisering.

Dette krever en endring i hvordan politiet utvikler og leverer digitale løsninger. For å levere digitale løsninger på en måte som er best tilpasset den enkelte oppgavens størrelse, egenart og kompleksitet må politiet ha en leveransemodell som omfatter både kontinuerlige leveranser og dagens mer tradisjonelle prosjekter. Over tid skal stadig mer leveres som kontinuerlige leveranser iht. DevOps-modellen. Denne måten å levere på gjelder ikke bare for IKT-løsningene – det strekker seg langt inn i hvordan politiet utvikler sine tjenester og arbeidsprosesser og har stor betydning for samarbeidet mellom brukerne, prosesseier og IKT-funksjonen. Dette vil også føre til endringer i hvordan vi sikrer arbeidstakernes medbestemmelse i den utviklingen som skjer. Vi vil ta utgangspunkt i dagens modell for forvaltningsleveranser når vi utvikler en modell for kontinuerlige leveranser i politiet.[7] Ved å gå mot en leveransemodell basert på DevOps ønsker vi å oppnå følgende effekter:

- **Kortere tid** fra identifisert behov til levert verdi for bruker
- Økt fokus på brukernes **reelle behov**
- Bedret **kvalitet og informasjonssikkerhet** i digitale løsninger
- Økt evne til å **respondere på behov** fra samfunnet
- Mindre administrasjon og **mer verdi for brukerne** for hver investert krone
- **Redusert risiko** for å bomme på målene.

[5] Også kalt en "plan-build-run"-leveransemodell
[6] Denne leveransemodellen kalles "DevOps". DevOps skiller seg fra tradisjonelle prosjekter ved at det gjennomføres små og hyppige leveranser og med en tett dialog mellom brukere, utviklere og de som drifter IKT-løsningen. I en DevOps-modell gis et helhetlig leveranseansvar til ett tverrfaglig produktteam som spesifiserer, utvikler, tester og drifter en løsning.
[7] Denne DevOps-baserte leveransemodellen vil måtte utvikles over tid i tråd med metodeutviklingen på IKT-området

Produktutvikling og kontinuerlige leveranser basert på DevOps skal være førstevalget for utvikling av digitale løsninger i politiet. Det vil likevel finnes områder der tradisjonelle prosjekter iht. politiets prosjektmodell kan benyttes.

Fremtidig leveransemodell deles inn i tre nivåer: 1) Et *porteføljestyre* som beslutter satsingsområder og tildelinger, 2) Et *fremdriftsstyre* som bryter opp tildelingene i initiativer og følger opp den samlede porteføljen, 3) Et praktisk nivå bestående av *prosessteam*, *produktteam* og *lokale innføringsteam* for den enkelte prosess[8], som definerer og leverer konkrete tiltak.

5 Styring av IKT-funksjonen

5.1 Hensikt og mål for fremtidig IKT-funksjon

Hensikten med utviklingen av fremtidig IKT-funksjon og leveransemodell er å oppnå **"Raskere realisering av digitale løsninger for politiet"**. Dette skal vi gjøre på en måte som sikrer at personvern, sikkerhet og andre krav til etterlevelse blir bygd inn i løsningene fra start og løpende ivaretatt gjennom hele livssyklusen. Raskere realisering av sikre digitale løsninger vil bidra til at politiet kan utnytte mulighetene og møte utfordringene som ligger i den voldsomme innovasjonen som skjer på teknologiområdet, og derigjennom realisere politiets virksomhetsstrategi både på kort (2020) og lang sikt (2025). Stabil og sikker drift av politiets IKT-løsninger vil fortsatt være sentralt for IKT-funksjonen. Basert på hensikten har vi definert seks viktige mål med tilhørende prinsipper[9] for IKT-funksjonen fremover:

1. Forbedre politiets tjenester gjennom økt utnyttelse av innovasjon innen teknologi
2. Øke tempo i etablering av digitale løsninger i politiet
3. Sikre kapasitet, kompetanse og fleksibilitet til å håndtere politiets behov
4. Redusere politiets investeringsbehov og øke forutsigbarheten på kostnadsutviklingen
5. Sikre en styrt, effektiv og trygg bruk av markedet
6. Ivareta stabil og sikker drift av digitale løsninger også i fremtidig IKT-funksjon og leveransemodell

5.2 Styringsmodell for IKT

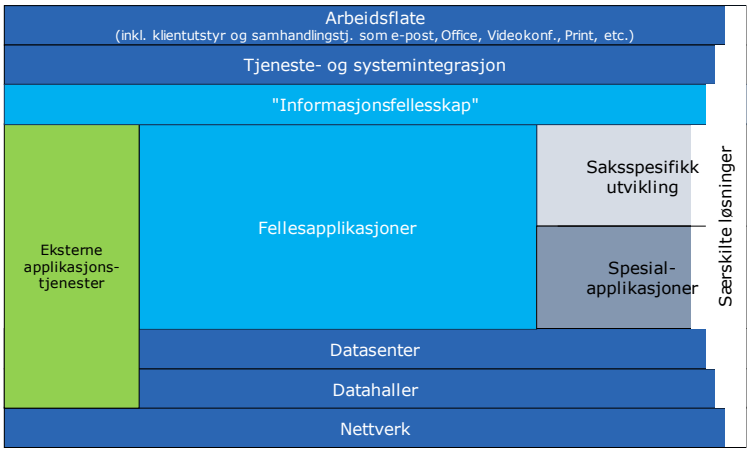
Styringsmodellen for IKT i politiet omfatter all etablering, videreutvikling, forvaltning, drift, support, bruk, avvikling og oppfølging av digitale løsninger som er innenfor politiets/politidirektørens ansvarsområde. Dagens styringsmodell ble sist revidert helhetlig i 2014/15 bl.a. basert på de endringene som ble gjort i Politidirektoratet og etableringen av PIT. Styringsmodellen må nå revideres som følge av denne strategien. Noen viktige prinsipper for styringsmodellen er gjengitt nedenfor:

- Understøtte **ett politi** og utvikling av fellesløsninger
- Omfatte både det som er **felles**, det som er **spesielt**, det som er **saksspesifikt** og det som er **særskilt**
- Sørge for størst mulig grad av **felles IKT-infrastruktur**
- Politidistrikt, særorgan etc. er **brukere** av politiets digitale tjenester, ikke kunder
- **Ikke internhandel** og internfakturering for digitale tjenester
- Ivareta de til enhver tid gjeldende **rammer for informasjonssikkerhet og personvern**.

[8] Med "prosess" menes her en overordnet arbeidsprosess i virksomheten, eksempelvis Straffesaksbehandling
[9] Prinsippene er ikke gjengitt her

5.3 Oppgavefordeling for IKT-løsninger

De digitale løsningene i politiet kan grovt sett deles inn som vist i figuren under. Alle delene er viktige for politiets oppgaveløsing.



Figur 2: Grovinndeling av IKT-løsninger

Felles infrastruktur[10], "informasjonsfellesskap" og fellesapplikasjoner leveres av PIT med underleverandører. Spesialapplikasjoner, saksspesifikk utvikling og særskilte løsninger kan etableres, videreutvikles og driftes av brukerne sin organisasjon, evt. i samarbeid med PIT. Etablering og videreutvikling av fellesapplikasjoner og spesialapplikasjoner skal følge politiets applikasjonslandskap. Det er viktig å utnytte politiets felles infrastruktur maksimalt, derfor skal fellesapplikasjoner, spesialapplikasjoner og saksspesifikke løsninger med tilhørende maskinvare, som hovedregel plasseres i, utvikles og produseres på, integreres med og tilgjengeliggjøres via politiets felles infrastruktur. Kun for særskilte løsninger vil det gis adgang til å avvike fra dette på ett eller flere områder.

5.4 Samhandling

Innovasjon og utvikling i politiet gjennom digitalisering avhenger av tverrfaglig samarbeid. Det må etableres samarbeid og samhandling for all virksomhetsutvikling i politiet. I tillegg til roller og funksjoner som er beskrevet i leveransemodellen kreves et tverrfaglig samarbeid for å:

- Identifisere, beskrive og prioritere behov for å ivareta en helhetlig tilnærming til virksomhetsutvikling
- Drive innovasjon og identifisere mulighetsrom for digitalisering av arbeidsprosesser
- Lage målbilder, veikart og langtidsplaner for å etablere forutsigbarhet
- Utforme beslutningsgrunnlag slik at porteføljestyret kan ta gode beslutninger.

5.5 Finansiering av IKT

Kostnadene til IKT i politiet utgjør litt over 10 % av etatens budsjett.[11] Mye av kostnadene går til eksterne leverandører, nesten 1,4 mrd. NOK i 2017.[12] IKT-kostnadene i politiet fordeler seg på sentrale kostnader og lokale kostnader i politidistrikt og særorgan.

Til tross for at det vil være et stort investeringsbehov knyttet til fornyelse av politiets digitale løsninger, er vurderingen at mye av denne utviklingen kan la seg realisere over tid ved omdisponering av eksisterende rammer slik at politiet får mer IKT for pengene. Det er heller ikke ønskelig å etablere en strategi som har for store avhengigheter til satsingsforslag og tilførsel av ytterligere midler – dette er også i tråd med politiets virksomhetsstrategi. Den største utfordringen med finansiering er det etterslepet politiet har på IKT-området som gjør at politiet fortsatt er avhengig av tilførsel av ekstra midler for å realisere applikasjonslandskapet på viktige områder som f.eks. Straffesak. – hvis ikke vil moderniseringen ta for lang tid.

[10] Nettverk, datahaller, datasenter, arbeidsflate, tjeneste- og systemintegrasjon
[11] Dette er høyere enn hva som disponeres innen enkelte andre offentlige etater (helsesektoren, Nav, m.fl.)
[12] 1364 MNOK iht. PFT sin spend-analyse for 2017 på kategorien IKT

Vi skal derfor:

- Fortsette å **erstatte innleide konsulenter** i PIT og POD med egne ansatte – det vil øke antall ansatte, men redusere kostnadene
- Benytte markedet der det er mulig og hensiktsmessig, til å **jevne ut behovet for reinvesteringer** slik at det blir mer forutsigbart, og **redusere behovet for pukkelinvesteringer** slik at det blir mer håndterbart
- Fortsette med å **budsjettfinansiere PIT** og ikke innføre tjenesteprising og internfakturering. Dagens praksis med underfinansiering av PIT må avsluttes.
- Vurdere om det skal etableres **flere felles IKT-tjenester** til politiet for bedre å møte behovet ute i etaten.[13]

6 Bruk av leverandørmarkedet

6.1 Politiet skal utvikle mer selv med egne ressurser enn i dag

Vi skal styrke politiets evne til å gjøre mer av IKT-utviklingen selv på løsninger som benyttes i politiets kjernevirksomhet. Dette gjelder særlig digitale løsninger innen forebygging, beredskap, straffesaksbehandling og opparbeide kunnskap (etterretning). Dette er strategisk kompetanse for politiet, tjenestene er særegne og det finnes lite ferdig løsninger og lite tilgjengelig kompetanse i markedet. Politiet kan potensielt også utvikle disse digitale løsningene mer effektivt med eget personell i ny leveransemodell.

6.2 Politiet skal bruke markedet smartere

Det er ikke hensiktsmessig, gjennomførbart eller kostnadseffektivt for politiet å ha full kapasitet og kompetanse innenfor alle områder av IKT-funksjonen, og på mange områder eksisterer det kompetanse og løsninger i markedet som politiet kan og bør anvendes. Det er mulig å utnytte leverandørmarkedet bedre enn det politiet gjør i dag. Tidligere analyser[14] viser at bruken av markedet innen applikasjonsutvikling og -forvaltning i stor grad er timebaserte ressurskjøp, noe som indikerer et potensial knyttet til storskaladrift, partnertankegang og større deling av kommersiell risiko. Videre viser analysene at dagens IKT-funksjon har relativt sett mye kapasitet og kompetanse innen ikke-strategiske funksjoner og arbeidsoppgaver og for lite kapasitet knyttet til digital innovasjon, systemutvikling, tjenesteintegrasjon, prosjektledelse, leverandørstyring, virksomhetsarkitektur, kognitive teknologier, dataanalyse og sikkerhet. Det er også muligheter for konsolidering av avtaler og leverandører.[15]

Områder hvor leverandørmarkedet kan bidra til en raskere digitalisering omfatter:

- **Støtte** på innovasjon og kompetanse innen anvendelse av ny teknologi
- **Kapasitet og kompetanse** som øker politiets fleksibilitet til å skalere og nedskalere utviklingsinnsats etter behov
- **Langsiktige partnerskap** på et færre sett av leverandører
- Avtaler og partnerskap som bidrar til å **redusere** politiets **investeringsbehov** og **øke forutsigbarhet** på finansiering ved at leverandører kan bidra med investeringer og storskalafordeler på infrastruktur og applikasjoner.

Så langt som mulig skal politiet unngå å komme i uhensiktsmessige avhengighetsforhold til enkeltleverandører. For tjenester og løsninger som kjøpes i markedet skal det kunne etableres reelle konkurransesituasjoner.

6.3 Sikkerhet må vurderes ved kjøp av tjenester

Politiet har en kritisk funksjon i samfunnet og mange av politiets tjenester skal være tilgjengelige når mye annet i samfunnet ikke fungerer, det gjelder også politiets digitale løsninger og informasjon. Disse må derfor sikres godt. Vi har utarbeidet 10 "føre var"-prinsipper som skal være et utgangspunkt for mer detaljerte verdi- og risikovurderinger ved konkrete tjenestekjøp knyttet til utvikling, drift og forvaltning av politiets IKT-løsninger.[16] De viktigste prinsippene er angitt nedenfor:

[13] Felles IKT-tjenester kan også gi stordriftsfordeler og bidra til mer enhetlig oppgaveutførelse
[14] Bl.a. gjeldende IKT Sourcingstrategi (2013) og realiseringsplaner og mulighetsstudien for IKT Sourcing og finansiering (2017)
[15] Ifm. HSO-fase 1 er applikasjonene som PIT har tatt over fra politidistriktene ikke konsolidert
[16] Risikovurderinger som foretas for det enkelte tjenestekjøp kan tilsi at prinsippene kan avvikes (eksempelvis ved kjøp av skytjenester) dersom restrisiko kan aksepteres

1. De samme sikkerhetsmessige rammene som gjelder for politiet vil gjelde for hele leverandørkjeden
2. Alle politiets data skal lagres og prosesseres i Norge
3. All utvikling, forvaltning og drift av politiets IKT-løsninger skal skje fra Norge
4. Alle som har tilgang til data, drifter, utvikler eller forvalter IKT-løsninger som ansatt i eller etter avtale med politiet, skal ha taushetsplikt, uttømmende og utvidet politiattest og nødvendig sikkerhetsklarering avhengig av hva slags informasjon de har tilgang til
5. Leverandører til politiet på IKT-området kan kun ha ett nivå med underleverandører.

7 Organisering og kompetanse

Vi skal utvikle og levere fremtidsrettede digitale løsninger til politiet og vi skal gjøre det på en annen måte enn vi tradisjonelt har gjort – politiet skal gjøre mer selv, utnytte leverandørmarkedet bedre og ta i bruk kontinuerlige leveranser basert på DevOps som leveransemodell. For å lykkes med dette må vi også se på hvordan vi organiserer IKT-funksjonen og hvilken kompetanse IKT-funksjonen og politiet generelt må ha.

7.1 Organisering av IKT-funksjonen

Organiseringen med Politidirektoratet som premissgiver for IKT-funksjonen og Politiets IKT-tjenester som politiets felles tjenesteleverandør på IKT-området videreføres. Gjennom prosjekt HSO[17]-fase 1 ble lokale IKT-medarbeider og IKT-løsninger i politidistriktene overført til PIT. HSO-fase 2 som omfatter særorganene skal gjennomføres. I tillegg må vi:

- Vurdere POD og PIT sin organisering mhp. hva som bør være funksjonsorganisert og hva som bør være produktorganisert, for å sikre raskere digitalisering av politiet. Dette gjelder for hele verdikjeden fra digitaliseringsbehov oppstår til det er dekket.
- Etablere en kapasitet som skal sørge for at politiet har en systematisk tilnærming til utnyttelse av teknologidrevet innovasjon i politiets oppgaveløsing
- Vurdere organisering av politiets informasjonsforvaltning og dataanalyse for å støtte opp under og forenkle politiets bruk av intern og ekstern informasjon samt sikre etterlevelse av lover og regler. Politiet må øke sin evne til å behandle informasjon digitalt slik at arbeidsprosesser i enda større grad baseres på kunnskap om kriminaliteten og for å øke samhandling internt og eksternt.
- Etablere en kapasitet for sikkerhetsovervåking av politiets digitale løsninger (SOC[18]-funksjon) som sikrer evne til raskt å oppdage sikkerhetshendelser/angrep og til raskt å håndtere hendelser for å redusere/minimalisere skadeomfanget.
- Etablere og drifte Justis-CERT[19]-funksjonen for hele justissektoren.

7.2 Kompetansebehov i IKT-funksjonen

Følgende kompetanseområder anses som spesielt viktig å styrke for å realisere denne strategien og derigjennom realisere politiets virksomhetsstrategi og lykkes med digitalisering av politiet:

- Digital kompetanse i politiet generelt
- Fremtidig leveransemodell
- Innovasjon og tjenesteutvikling
- Informasjonsforvaltning, dataanalyse og innsikt
- Skytjenester og kognitive teknologier
- Systemutvikling
- Bestiller- og leverandørstyringskompetanse
- Tjeneste- og systemintegrasjon
- Informasjonssikkerhet og IKT-sikkerhet.

For å lykkes med digitalisering er vi i tillegg helt avhengig av tverrfaglig samarbeid mellom disse "digitale" kompetanseområdet og dyp kompetanse på politiets arbeidsprosesser og bruk av informasjon og teknologi.

[17] "Helhetlig styring og organisering av IKT i politiet"
[18] Security Operations Centre
[19] Computer Emergency Response Team