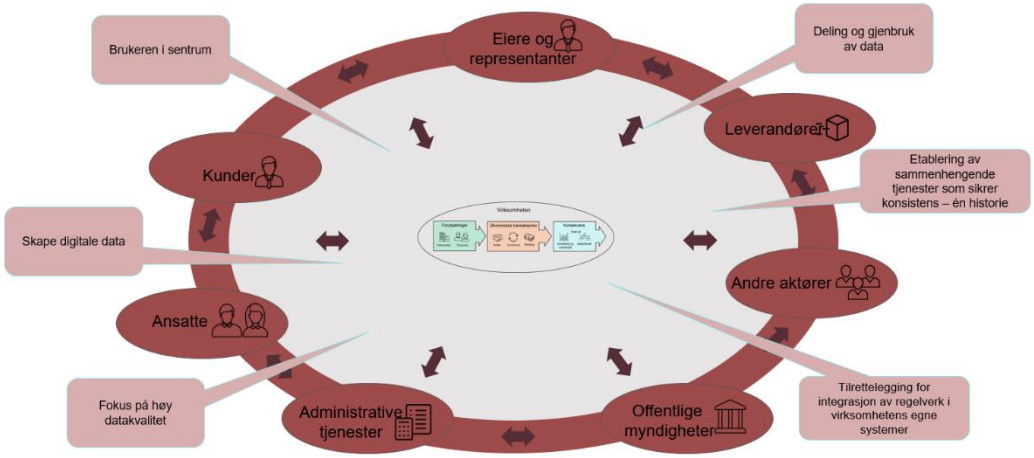


Digitale Økosystemer – hva er det og hvordan jobber vi med det i DigØk initiativet!

Hva er et digitalt økosystem

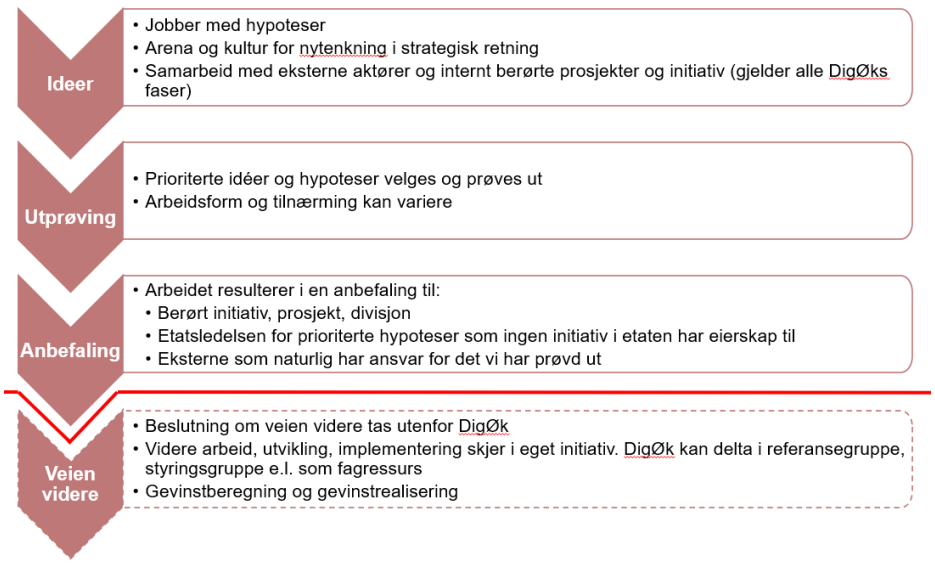
Vår definisjon av et digitalt økosystem er et nettverk av virksomheter og personer som deler og bruker data fra hverandre for å forenkle og/eller forbedre egne prosesser og data. Alle deltakerne samhandler og forteller derfor én historie uavhengig av hvem som «snakker».

Kort om DigØk initiativet

DigØk initiativet ser på hvordan vi kan støtte og legge til rette for at fremtidens digitale økosystem kan benyttes aktivt i gjennomføringen av Skatteetatens samfunnsoppdrag. Utgangspunktet for arbeidet var et tidlig initiativ fra OECD, hvor målet om Compliance by Design lå til grunn. Initiativet er et samarbeid mellom private og offentlige aktører, med forankring i SMSØ (Samarbeid Mot Svart Økonomi) og SIB (Seriøsitet I Byggenæringen). I 2021 har vi i tillegg til å jobbe aktivt med bygg- og anleggsnæringen også jobbet med en arbeidsgruppe i serveringsbransjen som er forankret i trepartssamarbeidet. Målet med arbeidet er å definere problemer, utarbeide løsningsforslag og å teste hvordan økosystemet kan bidra til at det er enkelt å gjøre det riktig for seriøse virksomheter.

DigØk jobber i fellesskap frem forslag og ideer. Det vil si at relevante etater arbeider sammen med arbeidsgiver- og arbeidstakersiden. I tillegg er konkrete virksomheter og systemleverandører invitert inn i samarbeidet.

I 2021 har et av to fokusområder vært arbeidet med sikker identitet på byggeplass. I arbeidet deltar flere private aktører i tillegg til fagforening, Arbeidstilsynet og Statsbygg. Vi har samlet behov og på bakgrunn av disse funnet en relevant prosess for løsningsarbeid og testing. Det lages nå en prototyp, som skal testes på byggeplass.

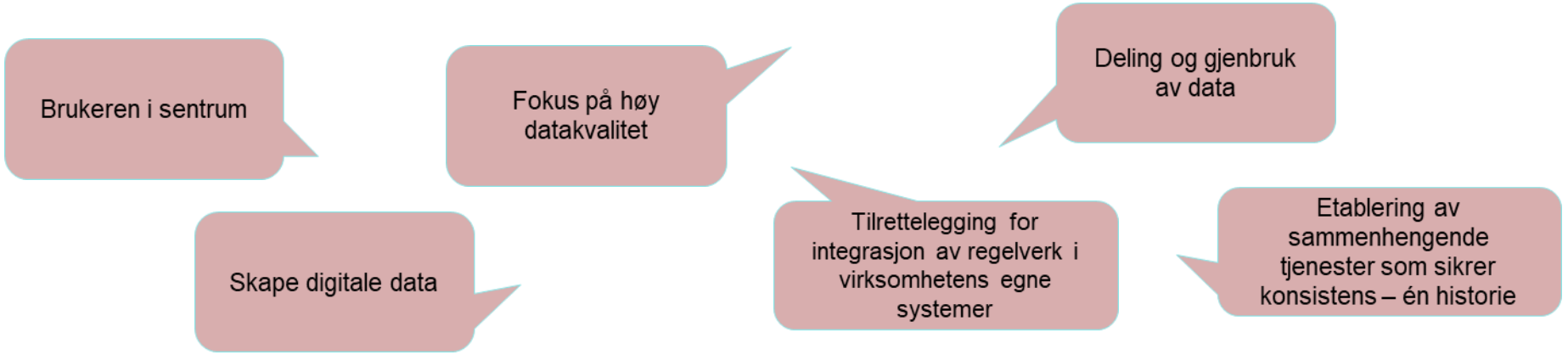


Hvordan jobber vi i DigØk

I DigØk jobber vi aktivt med å finne de gode ideene som gir verdi utover den konkrete problemstillingen vi jobber med. Samarbeidet på tvers i de enkelte arbeidsgruppene gjør at vi får god kunnskap om de relevante behovene som må løses dersom økosystemet faktisk skal ha verdi i et etterlevelsesperspektiv. De digitale økosystemene vil etableres etter hvert, og vi ønsker å skape forståelse for hvordan disse kan brukes for å øke datakvaliteten for relevante brukere.

Vi tester ideene gjennom PoC, prototyper eller i enkelte tilfeller som utviklede testløsninger, men vi har ikke som mål å sette de enkelte ideene i produksjon innenfor initiativet. Vi leverer en ide og en anbefaling til den etat, organisasjon eller aktør som er hensiktsmessig.

Prinsipper vi jobber etter



Gjennom arbeidet har vi funnet seks prinsipper for hva vi tenker er viktig at alltid vurderes i forbindelse med de ideene og initiativene vi jobber med. Dette er viktige mål og ambisjoner for at det potensiale som ligger i teknologiutviklingen skal kunne utnyttes på tvers av samarbeidspartnere og aktører innenfor økosystemet.

Et eksempel på hva vi har gjort - Behov for sikker identitet på byggeplass

Mange av oppgavene på en byggeplass er knyttet til at den enkelte har spesielle kvalifikasjoner. Dersom personen ikke er den han/hun utgir seg for å være vil heller ikke disse kvalifikasjonene kunne verifiseres at personen innehar. Dette kan gjelde alt fra sertifikat for spesielle kjøretøy, sprengning eller beregningsarbeider. Etter byggherreforskriften § 15 skal det føres oversikt over alle som er på en byggeplass i løpet av en dag – oversiktsliste.

For å kunne bruke fremtidens økosystemer aktivt har vi kommet frem til enkelte grunnleggende kjennetegn, knyttet til informasjonselementene som skal deles, som må være oppfylt:

- Data må være digitale

- Dataene må være av høy kvalitet
- Dataenes kvalitet må være kjent for brukeren

Byggeplasser er ikke ensartete, de kan være store med ansvarlige byggherrer som kan etablere omfattende digitale løsninger, men de kan også være små hvor ansvarlige virksomheter ikke har økonomisk eller praktisk mulighet til å ivareta personvern osv. på en god måte. De har likevel alle behov for løsninger som sikrer at behovene over ivaretas.

Med utgangspunkt i disse behovene fant arbeidsgruppen at dersom vi kunne garantere identiteten til de som registreres i oversiktslisten, ville vi ha verifisert identitet for alle på byggeplassen. Det var derfor et godt utgangspunkt for videre arbeid - hvordan kan oversiktslisten digitaliseres på en slik måte at identitet verifiseres.

Arbeidsgruppen var samstemte om at kontroll av biometri er eneste måte å skape data av en så god kvalitet på at de kan legges til grunn både for kontrolletatene, men også for å skape en sikkerhet for byggherren av at de faktisk benytter personer med riktige kvalifikasjoner.

Bruk av biometri stiller i utgangspunktet omfattende krav til personvernhåndteringen. For å omgå disse utfordringene ønsket vi en løsning hvor biometri ikke lagres, men kun representerer et øyeblikksbilde på kontrolltidspunktet.

Ved å bruke det høyoppløselige bildet fra Nasjonalt ID-kort og sammenligne det med et tilsvarende øyeblikksbilde av den ansatte vil det skje en slik verifikasjon. I utgangspunktet var løsningen tenkt benyttet på en inngangsrondell, hvor den ansatte ble nektet adgang dersom verifikasjonen ikke var gyldig. En slik løsning bruker dog så mye datakapasitet at ventetiden for den enkelte ble for lang.

Etter en gjennomgang hvor vi så på relevante alternativer fant vi en løsning hvor den ansatte benytter sin smarttelefon til identifisering opp mot «fysisk» nasjonalt ID-kort. Dette vil ikke bli knyttet til adgangskontrollen, men det skal sendes en melding til den ansatte hvor han/hun bes om å identifisere seg. Denne identifikasjonen gjøres på bakgrunn av informasjon som telefonen leser ut av ID-kortet og sammenligner med personen ved hjelp av telefonens kamerafunksjon. Når ID-kontroll er gjennomført registreres det i oversiktslisten ved at det hukes av for at ID-kontroll er gjennomført. For å sikre at

det ikke sitter personer andre steder klare til å gjennomføre ID-kontrollen vil utsendelsen av meldingen kun treffe personer innenfor et definert geografisk område tilsvarende anleggsområdet.

Forslaget innebærer at biometri/personopplysninger ikke lagres som en konsekvens av denne løsningen. Vi har en sikker identitet for hvem personen er i Norge gjennom kontrollen ved utstedelse, og det er kun mulig å fortelle én historie/være én person når verifikasjonen skjer mot dette kortet.

Selv om kortet per i dag kun er tilgjengelig for norske statsborgere fant arbeidsgruppen det nødvendig å avgrense testen kun til dette ID-dokumentet, da ingen andre dokumenter kan gi så høy sikkerhet for identiteten.

Ved at det tilkjennegis i oversiktslisten om det faktisk er gjennomført en ID-kontroll er det mulig for brukerne av dataene å selv vurdere kvaliteten og hvorvidt dette er informasjon de kan legge til grunn.