BERGEN
KOMMUNE

Bilde: Pexels.com

Temaplan for informasjonssikkerhet og personvern: 2021-2025

Erlend Andreas Horn

Byråd for finans, næring og eiendom

Forord

Byrådet er grunnleggende opptatt av å sikre innbyggernes personvern og at kommunens informasjonssikkerhet tas på alvor. Temaplanen er først og fremst en tematisk plan som skal sikre strategisk utvikling av fagområdene personvern og informasjonssikkerhet i kommunen. Gjennom denne planen lanserer byrådet en egen visjon for arbeidet. Visjonen sier at Bergen kommunes informasjonsforvaltning alltid skal være trygg og tillitsskapende. Visjonen og de fem hovedmålene danner bakgrunnsteppet for den videre innsatsen innenfor informasjonssikkerhet og personvern. Dette er ambisjoner alle ansatte i Bergen kommune skal ha et reflektert forhold til.

Digitaliseringen og ny teknologi endrer måten offentlig sektor produserer tjenester på. Dette skjer når informasjon kobles og settes sammen i digitale verktøy på nye måter. Offentlige tjenester blir mer digitale, og utviklingen vil akselerere fremover gjennom den digitale transformasjonen som pågår i samfunnet. Denne utviklingen skaper merverdi for kommunen og innbyggerne i et informasjonssamfunn. Samtidig endres lokale, nasjonale og globale utfordringer og trusler gjennom bruk av ny teknologi. Bergen og andre kommuner kan bli mer sårbare ettersom de digitaliserer stadig flere viktige prosesser knyttet til infrastruktur, innbyggertjenester, samfunnstjenester og interne prosesser. Sårbarheter kan oppstå både i systemer og knyttet til virksomhetens bruk av teknologi. Slike sårbarheter kan utnyttes gjennom at eksterne aktører ser nye muligheter for å få tak i informasjon de ikke skal ha.

Trusselbildet og teknologiutviklingen påvirker hvordan Bergen kommune forholder seg til omgivelsene sine. Nye sårbarheter som oppstår ved innføring og bruk av ny teknologi stiller nye krav til kommunen som arbeidsgiver, tjenesteleverandør, samfunnsutvikler og myndighetsutøver. Det er viktig at Bergen kommune øker evnen til å oppdage, forhindre og utbedre sårbarheter og trusler mot informasjonssikkerheten og den enkeltes personvern.

Teknologiutviklingen har gitt organisasjoner og enkeltmennesker nye verktøy for å skape, få tilgang til og dele informasjon med andre. Måten Bergen kommune sikrer informasjon, tilrettelegger for åpenhet og ivaretar den enkeltes personvern på, kan ha stor betydning for om innbyggerne har tillit til den informasjonen myndighetene gir. At Bergen kommune har god informasjonssikkerhet og ivaretar de registrertes personvern i tråd med lover, regler og egne prosedyrer er viktigere enn noen gang.

I juli 2018 fikk Norge ny personopplysningslov, og gjennom denne trådte EUs personvernforordning (GDPR[1]) i kraft. GDPR kom som en respons på teknologiutviklingen og behovet for å styrke de registrertes rettigheter i et internasjonalt digitalt informasjonssamfunn. Den økte digitaliseringen har medført forsterkede regulatoriske krav. Det nye lovverket skiller seg

[1] GDPR – General Data Protection Regulation

på enkelte områder fra personopplysningsloven og forskriften fra 2000, med blant annet strengere sanksjonsmuligheter enn tidligere.[2] Samtidig som mye av regelverket i GDPR er en videreføring fra tidligere norsk regelverk, er ikke rettspraksis fullt ut avklart. Over tid ser vi at kommunen utfordres i mange dimensjoner på temaene informasjonssikkerhet og personvern når arbeidsprosesser digitaliseres og systemer fornyes.

Utfordringene har vi sett gjennom flere egne avvik. Hendelsene skiller seg på viktige områder, men har til felles at de er løsninger som har vokst frem som følge av et stort behov i samfunnet eller organisasjonen. Byrådet er opptatt av at Bergen kommune skal jobbe systematisk for å etablere sikre systemer, ivareta et høyt kunnskapsnivå og etablere en informasjonssikkerhetskultur i hele kommunens organisasjon. Det vil skape tillit til at kommunen ivaretar den enkeltes personvern på en trygg måte.

Bergen kommune fikk sin første strategi for informasjonssikkerhet i 2011 og den ble revidert i 2015. I denne temaplanen vender kommunen oppmerksomheten mot hvordan vi samlet skal jobbe med fagområdene informasjonssikkerhet og personvern i tiden fremover. Planen er ment å bidra til å videreutvikle fagområdene, etablere en felles forståelse for fagene samt tilrettelegge for at kommunen skal håndtere den digitale transformasjonen. Bergen kommune skal ha en praksis som følger lov og forskrift, og dermed ivaretar innbyggernes personvern på en trygg og tillitsskapende måte.

All digitalisering i Bergen kommune skal skje på en trygg måte som ivaretar personvernet til ansatte og innbyggere. Teknologi kan utfordre personvernet til den enkelte, samtidig kan den samme teknologien bidra til økt beskyttelse av enkeltmenneskets integritet og privatsfære. I denne planen presenterer byrådet en samlet oversikt over forslag til prioriteringer og tiltak som skal bidra til at kommunen lykkes med å ivareta den enkeltes personvern, samtidig som samfunnets interesser ved å beskytte informasjon ivaretas.

Byråd for finans, næring og eiendom vil takke alle i kommunens organisasjon som har utvist tålmodighet og bidratt i planarbeidet i en ekstraordinær situasjon med Covid-19. Byråden ønsker også å særlig takke de aktørene som har medvirket i den eksterne høringen av planen:

- Datatilsynet
- Trondheim kommune
- Oslo kommune
- Utdanningsforbundet avd. Bergen
- Eldrerådet
- Ungdomsrådet
- Kommunalt råd for personer med funksjonsnedsettelse
- Digitaliseringsdirektoratet

[2] Dataportabilitet og frist for å melde avvik ved brudd på behandling av personopplysninger til Datatilsynet er eksempler områder der GDPR skiller seg fra gammelt regelverk.

Bystyrets vedtak

Bergen bystyre behandlet saken i møtet 24.03.2021 sak 92/21 og fattet følgende vedtak:

1. Bergen bystyre vedtar temaplan for informasjonssikkerhet og personvern 2021-2025 slik den går frem av vedlegg til denne saken.

2. Planen danner grunnlag for prioritering av kommunens innsats på områdene informasjonssikkerhet og personvern. Tiltak som gir økte kostnader, vil bli vurdert i forbindelse med den årlige rulleringen av handlings- og økonomiplaner.

3. Planen rulleres i 2025 eller tidligere ved behov.

Bilde: Unsplash.com

Innhold

1 Om temaplanen

Bilde: Nina Blågestad

1. Om temaplanen

1.1 Planens formål og avgrensninger

Bergen kommune har jobbet mye med å få på plass rutiner, kompetanse og kunnskap om både informasjonssikkerhet og personvern i virksomheten. Samtidig er det et stort potensial for å forbedre måten vi jobber med de to fagområdene. Avvik som har skjedd og utfordringene fremover, gjør at arbeidet med å gjennomføre tiltakene i denne planen må ha svært høy prioritet både i den øverste ledelsen og ute i tjenestene.

Planens formål er å legge til rette for at kommunen bedre kan lykkes med å få på plass egnede organisatoriske og tekniske tiltak som gir tilstrekkelig informasjonssikkerhet. Samtidig skal vi ivareta innbyggernes lovfestede rettigheter. Planen må derfor bidra til å etablere en felles forståelse i virksomheten på tvers av enheter for begge fagområdene, og gi retning for kommunens videre arbeid. Planen er derfor i hovedsak er rettet mot kommunens egen organisasjon. Den legger likevel til grunn at det er den registrerte med sine opplysninger som står i sentrum for arbeidet fremover.

1.2 Utfordringsbildet i Bergen kommune

Systematisk arbeid er en forutsetning for å utvikle gode og sammenhengende offentlige tjenester til innbyggerne. Bergen kommune må øke evnen til å håndtere egne organisatoriske og tekniske utfordringer. Det kan skje gjennom en økt innsats i egen organisasjon og lokalt, regionalt og nasjonalt for å bedre rammebetingelsene for informasjonssikkerhets- og personvernarbeidet.

Fagområdet informasjonssikkerhet har vært gjenstand for flere forvaltningsrevisjoner de siste årene i Bergen kommune.[3] Det har også vært gjennomført egne interne gjennomganger på fagområdene informasjonssikkerhet og personvern. Både revisjonene og de interne gjennomgangene har dokumentert varierende etterlevelse. I ulike sammenhenger har konsernfunksjonen ikke lagt tilstrekkelig til rette for virksomheten. Sammenhengen mellom etterlevelse, tilrettelegging, kompetanse og kapasiteten til å iverksette egnede tiltak for å forhindre brudd på den registrertes personvern er tydelig. Parallelt med arbeidet av denne temaplanen, har det i 2020 pågått en helhetlig gjennomgang av informasjonssikkerhet og personvern i kommunen.[4]

[3] Senere henvisninger til forvaltningsrevisor/revisjon viser til forvaltningsrevisjonen gjennomført i september 2019. I de tilfellene det henvises til flere revisjoner er referansen relevant for revisjoner utført 2019 og 2015.

[4] Se byrådssak 1119/20 for mer informasjon om helhetlig gjennomgang av informasjonssikkerheten og personvernet i Bergen kommune.

Den helhetlige gjennomgangen gir, i tråd med mandat (se byrådssak: 1119/20), en oversikt over mulige sårbarheter. Gjennomgangen gir anbefalinger til tiltak som på kort, mellomlang og noe lengre sikt skal redusere risikoen. Forvaltningsrevisor har i 2019 påpekt mangler eller feil i kommunens etablerte praksis på området. Disse knytter seg til ulike forhold, men kan grovt deles inn i:

- Organisatoriske forhold
- Tekniske forhold
- Kompetanse og kultur

Anbefalingene fra forvaltningsrevisor, helhetlig gjennomgang og det lokale utfordringsbilde blir behandlet fra et strategisk perspektiv i denne planen. Det strategiske perspektivet i planen innebærer at kommunen skal identifisere, prioritere og iverksette de initiativene og prosessene som kan bidra til at kommunen lykkes med arbeidet.

1.3 Byrådets ambisjon, visjon og mål for arbeidet med informasjonssikkerhet og personvern

Byrådets politiske plattform bygger på ambisjonen om at Bergen skal være en god by for alle. Bergen kommunes viktigste oppgave er å tilby gode tjenester av høy kvalitet til innbyggerne. En forutsetning for å nå ambisjonen om at byen skal være god for alle og levere tjenester av høy kvalitet er et systematisk arbeid med informasjonssikkerhet og personvern. Dette arbeidet skal i særlig grad sikre barn og unge på en forsvarlig og proaktiv måte.

Byrådssak 1124/17 «Digitalisering og innovasjon i Bergen kommune» slår i hovedmål 5 fast, at de registrerte i Bergen kommune skal ha et godt personvern og god informasjonssikkerhet. Dette er i tråd med kommuneplanens samfunnsdel «Bergen 2030». Kommuneplanen sier at Bergen skal være en trygg by med god beredskap mot uønskede hendelser. Beredskapsarbeid, informasjonssikkerhet og personvern må sees i sammenheng med hverandre.

For byrådet er det viktig at alle registrerte får oppfylt sine rettigheter gitt gjennom personvernforordningen. Samtidig er det en prioritert oppgave for byrådet å sikre at særlig sårbare registrerte får den beskyttelsen de skal ha gjennom lov- og regelverk. Eldre, pasienter, psykisk syke, barn og unge har behov for sosial beskyttelse fordi de kan være ute av stand til, med enkelhet, å gi sitt samtykke eller motsette seg behandling av personopplysninger eller utøve sine rettigheter. Byrådet forventer at Bergen kommune i strategiperioden skal ha et særlig søkelys på barn og unge, men også andre sårbare registrerte når nye digitale verktøy tas i bruk.

På samme måte er temaplanen for informasjonssikkerhet og personvern forankret i nasjonale føringer, som Regjeringens digitaliseringsstrategi «Én digital offentlig sektor», og internasjonale forpliktelser. Her kan FNs 16. bærekraftsmål «fred og rettferdighet», og delmål 16.3 «fremme rettstaten nasjonalt og internasjonalt, og sikre lik tilgang til rettsvern for alle» nevnes. Dette er mål som Norge har sluttet seg til.

I kommunens nye digitaliseringsstrategi, som legges frem parallelt med denne temaplanen, beskriver byrådet ambisjonene for hvordan Bergen kommune de neste årene skal utvikle seg gjennom en digital transformasjon. Dette innebærer å ta i bruk stordata, og det betyr at måten tjenestene utvikles, driftes og leveres på, vil endre seg fundamentalt i fremtiden.[5] En forutsetning for en slik transformasjon, er imidlertid at informasjonssikkerheten og personvernet ivaretas på en tillitsvekkende måte, i tråd med nasjonale retningslinjer og anbefalinger.

På denne bakgrunn foreslår Byrådet en visjon for kommunens innsats innenfor informasjonssikkerhet og personvern**:**

Bergen kommunes informasjonsforvaltning skal alltid være trygg og tillitsskapende.

Å jobbe systematisk med informasjonssikkerhet og personvern er ikke nytt for kommunen. Gjennom flere år har informasjonssikkerhet og personvern kommet stadig høyere på dagsordenen i kommunen, både i avdelingene og hos de ansatte. Samtidig anerkjenner vi at kommunen har utfordringer knyttet til informasjonssikkerhet og personvern. Virksomheten trenger derfor en intensivert og koordinert innsats på tvers av kommunens organisering.

Hovedmålene bygger på byrådets visjon for fagområdene informasjonssikkerhet og personvern. De har også blitt utviklet med bakgrunn i kommunens behov dokumentert i eksterne gjennomganger, fagmiljøenes vurderinger og dialog med omgivelsene.[6] I tråd med visjonen som er presentert ovenfor, skal kommunen **jobbe etter fem hovedmål:**

1. Bergen kommune skal gi helhetlige og samordnede føringer for arbeidet med informasjonssikkerhet og personvern, som etterleves i hele organisasjonen.
2. Ansatte og innleide skal ha kompetanse til å håndtere personopplysninger, slik at hensynet til informasjonssikkerhet og personvern ivaretas i tråd med gjeldende regler.
3. Bergen kommune skal samarbeide tett med nasjonale og regionale partnere for å styrke informasjonssikkerheten og personvernet, slik at vi tar vare på rettighetene til den enkelte og sikrer samfunnets interesser.
4. All digitalisering og bruk av teknologi i Bergen kommune skal legge til grunn informasjonssikkerhet og personvern i tråd med kommunens arkitekturprinsipper i anskaffelse, innføring, bruk, endring og utfasing.
5. Fundamentet for digitalisering gjennom infrastruktur og systemer skal til enhver tid være oppdatert i henhold til beste praksis for å understøtte informasjonssikkerhet i alle løsninger og tjenester.

[5] Stordata/big data er data som kjennetegnes ved at de samles og lagres i store mengder. Det er i tillegg en variasjon i dataene som samles inn, og de er gjerne tilgjengelig for analyse i sanntid.
[6] Målene er likestilte og er ikke opplistet i prioritert rekkefølge.

2 Introduksjon til fagområdene

Bilde: Pixabay.com

2. Introduksjon til fagområdene

2.1 Forklaring av sentrale begreper

Personopplysninger er alle opplysninger eller vurderinger som direkte eller indirekte kan knyttes til en person slik som navn, adresse, fødselsnummer, telefonnummer, bilnummer, bilder, IP- og e-postadresse, atferdsmønstre med mer.[7] Særlige kategorier av personopplysninger er eksempelvis opplysninger om helseforhold, rasemessig eller etnisk bakgrunn, politisk, filosofisk eller religiøs oppfatning, DNA, seksuelle forhold og medlemskap i fagforeninger.[8]

Med *personvern* menes borgerens rett til et privatliv, og retten han eller hun har til å bestemme over egne opplysninger. Dette prinsippet er nedfelt i Den europeiske menneskerettighetskonvensjonens artikkel 8: «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse». Borgerens integritet er også beskyttet gjennom grunnlovens § 102: «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet.»

For borgerne, den registrerte og behandlingsansvarlig er det sentralt at kommunen har en praksis som hindrer:

- At feil beslutninger tas
- At manglende tilgjengelig informasjon påvirker den registrertes rettigheter
- Informasjonstap
- Brudd på rettigheter og rettssikkerhet
- Omdømmetap
- Økonomiske tap
- Tap av liv og helse
- Krenkelse av integritet

Kommunen forvalter store mengder informasjon om innbyggere, egne ansatte og ulike typer infrastruktur som er av stor betydning for samfunnet. For å ivareta hensynet til både samfunnssikkerhet og personvern er det kritisk at informasjon forvaltes på en slik måte at informasjonens *konfidensialitet*, *integritet* og *tilgjengelighet* sikres i tråd med krav satt i lov, forskrift og kommunens egne vedtak og regelverk.

I faget informasjonssikkerhet er disse tre begrepene selve kjernen i informasjonssikkerhetsfaget, og ut fra kommunens egne behov forklares de derfor nærmere slik:

---

[7] Lov om behandling av personopplysninger artikkel 4 definerer hva som regnes som personopplysninger.

[8] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/spesielt-om-sarlige-kategorier-av-personopplysninger-sensitive-personopplysninger-og-unntak/

Konfidensialitet betyr å sikre at informasjon og informasjonssystemer kun er tilgjengelig for personer, enheter og prosesser som skal ha tilgang.

Integritet betyr å sikre at informasjon og informasjonssystemer er korrekte, gyldige og fullstendige – det vil si å sikre at informasjon og informasjonssystemer ikke kan endres urettmessig eller utilsiktet.

Tilgjengelighet betyr å sikre at informasjon og informasjonssystemer er tilgjengelig og anvendelig innenfor de kravene som er satt om tilgjengelighet.[9]

Digitaliseringsdirektoratet definerer begrepene ovenfor, basert på ISO-27000 serien slik: Arbeidet med informasjonssikkerhet handler om å sikre informasjonsbehandlingen. Det betyr å sikre at informasjon i alle former:

- Ikke blir kjent for uvedkommende (konfidensialitet)
- Ikke blir endret utilsiktet eller av uvedkommende (integritet)
- Er tilgjengelig ved behov (tilgjengelighet)

Informasjonssikkerhetsarbeidet dreier seg om å sikre at den informasjonen kommunen har, ikke er mulig å få tak i for uvedkommende. På samme tid må informasjonen være tilgjengelig for de som skal ha tilgang. [10] Det handler også om at kommunen sikrer virksomhetskritisk informasjon.[11] Riktig bruk av informasjon er nødvendig for at samfunnskritisk infrastruktur som vei, vann, avløp eller bygninger kan løse oppgaver i nød- og krisesituasjoner. Organisasjonen må sikre at de virksomhetskritiske systemene er hardføre nok til å tåle uforutsette hendelser dersom en unormal driftssituasjon oppstår. Kommunen må planlegge for at uforutsette hendelser kan oppstå, som vil kreve en annen kapasitet og bruk enn normalt.

At kommunen sikrer behandling av personopplysninger gjennom egnede tekniske og organisatoriske tiltak er kommunens plikt som *behandlingsansvarlig*. Den behandlingsansvarlige er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. I Bergen kommune er byrådet ansvarlig etter loven. Fullmakter er på vanlig måte delegert til fagbyrådene og videre til kommunaldirektørene i byrådsavdelingene. Som behandlingsansvarlig er man ansvarlig for at personopplysninger håndteres i tråd med reglene i lovverket. Hvis eksterne virksomheter behandler personopplysninger på vegne av Bergen kommune, er kommunen lovpålagt å inngå en databehandleravtale. Kommunen (behandlingsansvarlig) skal i tillegg kontrollere at leverandøren (databehandler) ivaretar god informasjonssikkerhet, og at kravene i personopplysningsloven er ivaretatt.

[9] I tillegg til disse tre kravene omtales prinsippet om robusthet i behandlingssystemene og -tjenestene, i forordningens artikkel 32 nr. 1-b.
[10] Eksempler på informasjon kan være samtaler, dokumenter, brev, notater, digitale filer med mer.
[11] Et eksempel på et virksomhetskritisk system kan være kommunens elektroniske pasient- og journalsystem.

2.2 Nærmere om personvernforordningen GDPR

Hovedformålet med GDPR er å styrke enkeltpersoners personvern og å skape enhetlig og tydelig regulering i hele EØS-området. Dette gjør at alle virksomheter som behandler personopplysninger om borgere i EØS fikk nye og endrede plikter.[12] Registrerte enkeltpersoner ble gitt større kontroll over sine egne personopplysninger, og virksomheter har gjennom GDPR fått et større ansvar for å ivareta den enkeltes personvern.

Mye av GDPR er en videreføring av den gamle personopplysningsloven og forskriften fra 2000, selv om GDPR har ført til strengere krav om informasjon til innbyggere og ansatte. Dette gjelder både ved innhenting av opplysninger, og bruken av opplysningene.

Når Bergen kommune skal behandle personopplysninger, skal dette alltid skje etter prinsippene i artikkel 5 i GDPR:

1) Personopplysninger skal

a- behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte.

b- samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene; viderebehandling for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål skal, i samsvar med artikkel 8 nr. 1, ikke anses som uforenlig med opprinnelige formålene («formålsbegrensning»),

c- være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»),

d- være korrekte og om nødvendig oppdaterte; det må treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller rettes («riktighet»),

e- lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for; personopplysninger kan lagres i lengre perioder dersom de utelukkende vil bli behandlet for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1, forutsatt at det gjennomføres egnede tekniske og organisatoriske tiltak som kreves i henhold til denne forordning for å sikre de registrertes rettigheter og friheter («lagringsbegrensning»),

f- behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet»).

og i tillegg skal det skje gjennom:

1) Et klart språk og forståelig informasjon om behandlingen skal være lett tilgjengelig.

[12] https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/om-personopplysningsloven-og-nar-den-gjelder/

2) All informasjon som gis til barn skal være tilpasset deres forståelsesnivå.

3) På en sikker måte, og på den plattformen den det gjelder mestrer.

Forordningen pålegger kommunen ansvar for å vurdere konsekvenser ved behandling av personopplysninger, og iverksette risikoreduserende tiltak ved behandling av disse. Med GDPR ble det stilt strengere krav enn tidligere til at personvernet bygges inn i de digitale tjenestene kommunen tilbyr. Innebygd personvern betyr at det tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning.[13]

Med GDPR følger det også kraftige sanksjonsmuligheter.[14] Virksomheter som ikke møter kravene i forordningen, kan ilegges overtredelsesgebyr på inntil fire prosent av den årlige omsetningen. Et annet moment hvor GDPR skiller seg fra tidligere lov- og regelverk, er at GDPR legger vesentlig mer vekt på hvordan virksomhetene som behandler personopplysninger kommuniserer med den registrerte. Kapittel 3 i forordningen trekker frem at all kommunikasjon knyttet til artikkel 15-22 og 34 skal foregå på en kortfattet, åpen, forståelig og lett tilgjengelig måte. Dette gjelder særlig i de tilfellene der det gjelder informasjon knyttet til barn.

I tillegg til å stille krav til selve behandlingen av personopplysninger, gir personopplysningsloven og GDPR den registrerte flere rettigheter, som i varierende tilfeller gjør seg gjeldende. Disse knytter seg blant annet til:

- Rett til innsyn
- Rett til retting
- Rett til sletting
- Rett til begrensning
- Rett til å protestere
- Rettigheter knyttet til dataportabilitet, automatiske avgjørelser og informasjon.

Som regel skal Bergen kommune som behandlingsansvarlig legge til rette for å vurdere, utføre og gi tilbakemelding uten ugrunnet opphold, og senest innen en måned.[15]

GDPR endrer seg over tid og rettspraksis er ikke fullt ut avklart. Et eksempel er Schrems II hvor EU-domstolen i 2020 nye og tydelige føringer for overføring av personopplysninger til tredjeland (land utenfor EU/EØS). For Bergen kommune innebærer Schrems II en ny praksis for behandling av personopplysninger. Kommunen må derfor ha oversikt og vurdere eksisterende overføringer av personopplysninger til tredjeland i lys av dommen. Uavhengig av Schrems II, må kommunen følge den videre juridiske utviklingen tett og være tilpasningsdyktig når ny praksis utvikles.

[13] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/

[14] Artikkel 5 – generelle vilkår for ilegging av overtredelsesgebyr og ved brudd på bestemmelsene i forordningen kan aktuell tilsynsmyndighet gi virksomheter overtredelsesgebyr på opptil 4% av global årsomsetning i forutgående regnskapsår.

[15] Unntaksvis kan fristen forlenges med 60 dager i de tilfellene der kommunen får inn mange og kompliserte forespørsler. Dersom dette er tilfelle, plikter kommunen å opplyse om dette og begrunne utsettelsen.

3 Situasjonen i dag

Bilde: Unsplash.com

3. Situasjonen i dag – organisering, status og utfordringer på områdene

3.1 Arbeidet med informasjonssikkerhet og personvern i dag

Byrådssak 1401/14 beskriver ansvaret, rammebetingelsene og oppdraget en byrådsavdeling med konsernansvar har for å veilede, kontrollere, støtte, tilrettelegge og gi råd i fagfunksjoner som er konserngjennomgående for hele kommunen. Sammen med andre styrende dokumenter, som reglement for digitalisering og IKT, akseptabel bruk av IKT, styringssystemet for informasjonssikkerhet og personvern og reglementet for personvern og informasjonssikkerhet beskriver og regulerer de kommunens arbeid innenfor digitalisering, personvern og informasjonssikkerhet. [16]

Som kommunens eget fagorgan med konserngjennomgående oppgaver innenfor digitalisering, IKT, informasjonssikkerhet og personvern, har Seksjon for digitalisering og innovasjon (heretter omtalt som SDI) på fullmakt fra kommunaldirektør, myndighet til og ansvar for å:

- Utvikle og holde ved like felles overordnede rutiner og systemer (regler, prosedyrer og støtteverktøy).
- Se til at felles overordnede rutiner og systemer blir fulgt i hele kommunens virksomhet.
- Etterkontrollere de aktuelle fagområdene i hele kommunens virksomhet, som stikkprøvekontroller basert på risikovurderinger.
- Veilede og tilrettelegge overfor byrådsavdelingene i spørsmål som gjelder hele konsernet.

Med bakgrunn i strategi for informasjonssikkerhet (2015), og i forkant av GDPR (2018), opprettet Bergen kommune et eget personvernombud i 2016. [17] Personvernombudets stilling, oppgaver og rolle i organisasjonen er beskrevet i et eget mandat, og er forankret i GDPR artiklene 37, 38 og 39. Bergen kommune har satset og tatt initiativ til en samordnet og regional digitalisering av kommunal sektor. Bergen kommune løser derfor personvernombudsfunksjonen for flere omegnskommuner som en del av samarbeidet i DigiVestland. [18]

Siden 2015 har Bergen kommune styrket arbeidet med informasjonssikkerhet og personvern i tråd med den økte digitaliseringen. Fra å ha én dedikert ressurs på konsernnivå, var det høsten 2018 fire personer som arbeidet med informasjonssikkerhet og personvern i SDI. Høsten 2020 er avdelingen bemannet med åtte årsverk. Sentrale oppgaver for avdelingen er å utarbeide og følge

[16] Vedlegg er foreløpig ikke lagt inn i utkastet.
[17] Personvernombudsfunksjonen ble med innføring av GDPR obligatorisk for alle offentlige virksomheter.
[18] For mer informasjon om DigiVestland og det regionale samarbeidet: www.digihordaland.no

opp overordnet strategiarbeid, i tillegg til å drive utstrakt rådgivnings- og veiledningsarbeid ut mot byrådsavdelingene. Personvernombudsfunksjonen utøves også i avdeling for personvern og informasjonssikkerhet. Rådgivning og veiledning gjøres i dag primært gjennom styrende dokumenter, veiledere, reglement, oppgaveløsere, prosedyrer og dialog med ansatte i Bergen kommune. [19]

Strategien for informasjonssikkerhet (2015) anbefalte som ett av flere tiltak å etablere et konserngjennomgående informasjonssikkerhetsforum. Dette ble gjort for å tilrettelegge for «ledelsens gjennomgang» og forsterke oppfølgingen av informasjonssikkerheten på tvers i kommunen.

Gjennom tidligere praksis, som en del av styringssystemet og annen styrende dokumentasjon har Bergen kommune etablert ulike roller som er sentrale i arbeidet med å ivareta personvernet og sikre god informasjonssikkerhet. Hver for seg har rollene ulike oppgaver og ansvar, men samlet og hver for seg, er de sentrale i arbeidet for å ivareta informasjonssikkerheten og personvernet. Disse er i dag:

- Behandlingsansvarlig (kommunaldirektør i den enkelte byrådsavdeling)
- Personvernombudet
- Direktør ved Seksjon for digitalisering og innovasjon (SDI)
- Leder av Enhet for digitale driftstjenester (EDD)
- Resultatenhetsleder
- Systemeier
- IKT-koordinator
- Systemkoordinator
- Ansatte

Forvaltningsrevisjonene, interne gjennomganger og hendelser i løpet av 2018 og 2019, har pekt på flere områder med svakheter og forbedringspotensial. Dette har særlig handlet om etterlevelse av styringssystemet for informasjonssikkerhet og personvern, kompetanse hos de ansatte på områdene og tilrettelegging for god og riktig praksis. Forvaltningsrevisjonene har blant annet dokumentert at kommunen tidvis har hatt manglende oversikt og ufullstendige risikovurderinger, men har ikke avdekket funn som tyder på at styringssystemet ikke er i tråd med gjeldende regelverk.

Forvaltningsrevisor har funnet at system og rutiner for tilgangsstyring i kommunen i varierende grad egner seg til å sikre at ansatte får de tilgangene de trenger, og sikre at ansatte som slutter i kommunen mister tilgangene. Revisor mener også at kommunen ikke i stor nok grad har tydeliggjort ansvar og oppgaver relatert til informasjonssikkerhet, og at systemeiere ikke i tilstrekkelig grad har mottatt opplæring og støtteverktøy som er nødvendig for å kunne gjennomføre sine oppgaver.

[19] Oppgaveløsere en konkret veiledning som knytter seg til en spesifikk arbeidsprosess, arbeidsoppgave eller en utfordring flere ansatte i Bergen kommune kan trenge veiledning på.

Undersøkelsene forvaltningsrevisor har gjort, har samtidig avdekket at de ansatte i varierende grad har tilstrekkelig kjennskap til retningslinjer og rutiner for informasjonssikkerhet, og at de ansatte derfor i varierende grad etterlever disse rutinene og retningslinjene. Forvaltningsrevisor konkluderer med at informasjonssikkerhetspraksisen hos enkelte ansatte bryter med flere grunnleggende informasjonssikkerhetsprinsipp, også i tråd med funn gjort i den helhetlige gjennomgangen.

Kommunen mangler i dag en felles plan for opplæring og kompetanse innenfor personvern og informasjonssikkerhet. Det henger også sammen med uklare definisjoner av roller og ansvar på fagområdene. Dette medfører blant annet at ivaretakelse av personvern og informasjonssikkerhet i digitaliseringsprosjektene, ikke har vært ivaretatt systematisk av kommunen.

Flere av funnene fra forvaltningsrevisor støttes av kommunens helhetlige gjennomgang av personvern og informasjonssikkerhet og tidligere interne gjennomganger. Foreløpige sentrale funn som er gjort i den helhetlige gjennomgangen underbygger at kommunen har utfordringer når det gjelder tilstrekkelig dokumentasjon av systemer, integrasjoner, dataflyt og systemtilganger, samt oversikt over det totale risikobildet. Kommunen har også manglet en systematisk tilnærming til kompetanseutvikling hos de ansatte på områdene.

Derfor pågår det et arbeid med å etablere en struktur som gir kommunen en nødvendig kontroll på fagområdene informasjonssikkerhet og personvern. Blant annet jobbes det i 2020 med å revidere styrende dokumentasjon, forbedre veiledning knyttet til sentrale arbeidsprosesser på fagområdene og kompetanse- og kulturbygging på kort og mellomlang sikt.[20] Bergen kommune skal lære av hendelsene, og kommunen skal gjennom dette forsterke egen evne til å forhindre brudd på informasjonssikkerheten og den enkeltes personvern.

Bilde: Pexels.com

[20] Revidert styrende dokumentasjon som har blitt utført i den helhetlige gjennomgangen bygger i stor grad på veiledningsmateriale utgitt av Digitaliseringsdirektoratet og Difi, som baserer seg på ISO/IEC 27001:2013.

3.2 Arbeidet fremover - strategiske satsingsområder for fagområdene informasjonssikkerhet og personvern

I innledningskapittelet i denne temaplanen lanserer byrådet en visjon og fem hovedmål for arbeidet med informasjonssikkerhet og personvern. Disse skal være retningsgivende for kommunens arbeid på fagområdene fremover.

Visjon: Bergen kommunes informasjonsforvaltning skal alltid være trygg og tillitsskapende.

Mål:

1. Bergen kommune skal gi helhetlige og samordnede føringer for arbeidet med informasjonssikkerhet og personvern, som etterleves i hele organisasjonen.
2. Ansatte og innleide skal ha kompetanse til å håndtere personopplysninger, slik at hensynet til informasjonssikkerhet og personvern ivaretas i tråd med gjeldende regler.
3. Bergen kommune skal i tett samarbeid med nasjonale og regionale partnere styrke informasjonssikkerheten og personvernet, slik at vi tar vare på den enkeltes rettigheter og sikrer samfunnets interesser.
4. All digitalisering og bruk av teknologi i Bergen kommune skal legge til grunn informasjonssikkerhet og personvern i tråd med kommunens arkitekturprinsipper i anskaffelse, innføring, bruk, endring og utfasing.
5. Fundamentet for digitalisering gjennom infrastruktur og systemer skal til enhver tid være oppdatert i henhold til beste praksis for å understøtte informasjonssikkerhet i alle løsninger og tjenester.

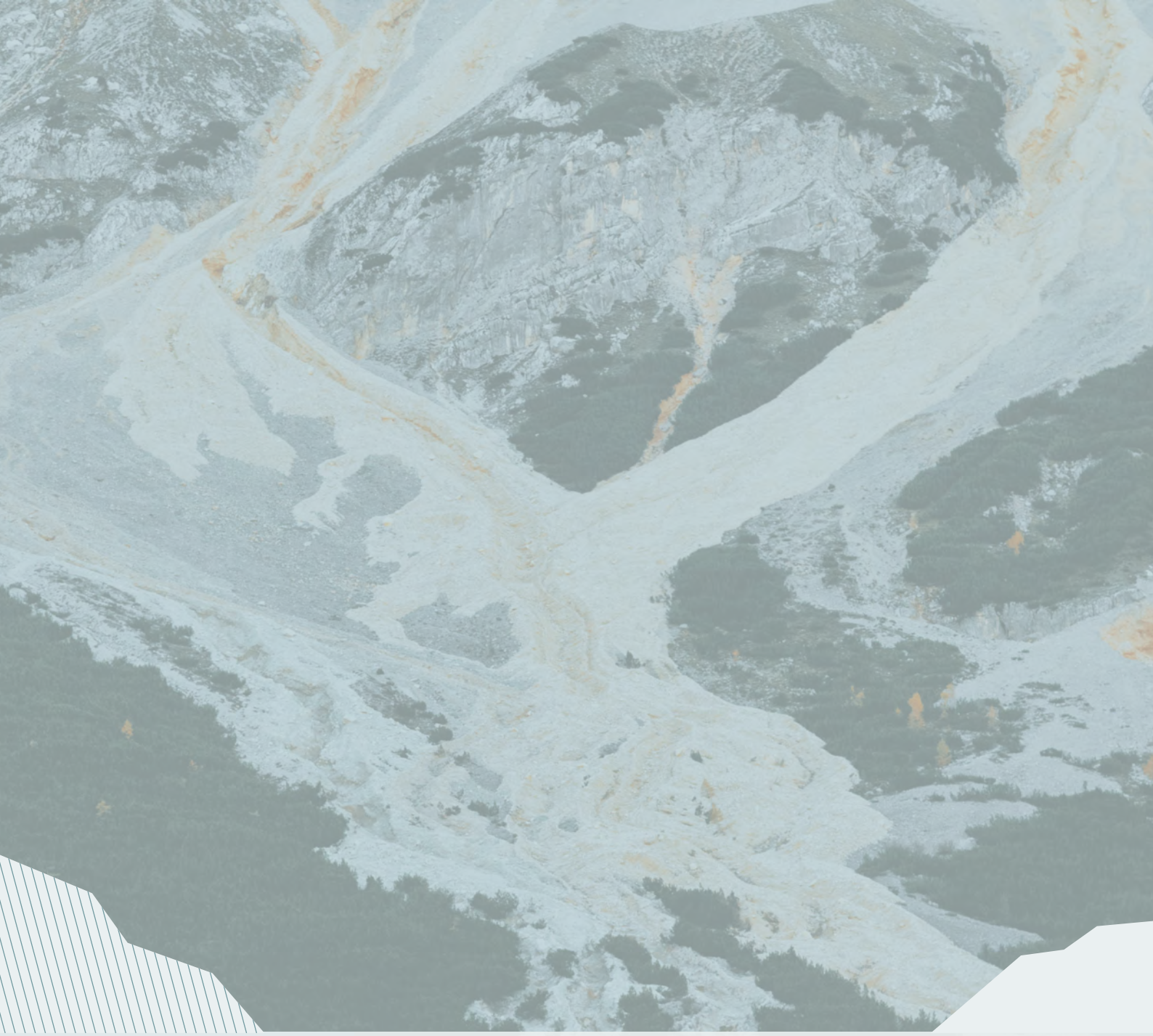
Mål for kommunens arbeid med fagområdene informasjonssikkerhet og personvern.

For å nå målene vil byrådet prioritere følgende strategiske satsingsområder:

1	Innebygd personvern, infrastruktur og systemer som tåler det uforutsette
2	Infrastruktur og forvaltning av fagsystem
3	Tilrettelegging og etterlevelse
4	Samarbeid mellom lokalt, regionalt og nasjonalt nivå
5	Kompetanse, sikkerhets- og personvernkultur

Tabell 1: Oversikt over strategiske satsingsområder for kommunens arbeid med fagområdene informasjonssikkerhet og personvern.

Visjon, mål og strategiske satsingsområder skal sees i sammenheng med hverandre. Satsingsområdene presenteres nærmere i kapitlene 4-8.



4

Strategisk satsingsområde:

Innebygd personvern, forvaltning, infrastruktur og systemer som tåler det uforutsette

Bilde: Pexels.com

4. Strategisk satsingsområde: Innebygd personvern, forvaltning, infrastruktur og systemer som tåler det uforutsette

Etablering av infrastruktur som tåler det uforutsette og innebygd personvern er viktige satsinger for byrådet. Innebygd personvern er også et sentralt moment i personopplysningsloven. Datatilsynet definerer innebygd personvern som at det tas hensyn til personvern i alle faser av et system eller løsning.[21]

I tråd med hovedmål 4 i temaplanen, skal all digitalisering og bruk av teknologi i Bergen kommune sette innebygd personvern som premiss i alle faser av løsninger eller systemer. Dette innebærer at hele systemet aktivt tilrettelegger for å ivareta den registrertes rettigheter. Dette skal skje gjennom løsningens livsløp fra ide via anskaffelse og bruk til utfasing. Systemer, som ikke legger til grunn innebygd personvern, øker sannsynligheten for dårlig informasjonssikkerhet og brudd på grunnleggende personvernrettigheter. Dette vil kunne medføre svekket tillit mellom innbyggere og myndigheter. Byrådet, innbyggerne og de registrerte i Bergen kommune sine systemer forventer at løsningene kommunen anskaffer er trygge og møter standardene Datatilsynet og GDPR setter for innebygd personvern.

Kommunen skal gjennomføre organisatoriske og tekniske tiltak som bidrar til å senke risikoen for at brudd på den registrertes rettigheter oppstår. Bergen kommune må ta flere grep for å få til dette. Ett av grepene er å rekruttere og samle nødvendig spisskompetanse på digital sikkerhet i et nytt samarbeid med det nye Samfunnssikkerhetens hus i form av et operasjonssenter for sikkerhet (SOC).[22] Gjennom samarbeidet med kommunens og regionens øvrige beredskapsmiljøer vil operasjonssenteret bidra til å avdekke sårbarheter i kommunens digitale infrastruktur og løsninger.[23] Operasjonssenteret kan også forhindre personvernbrudd når nye løsninger eller systemer skal fases inn. Operasjonssenteret vil i tillegg kunne nyte godt av et tett samarbeid med Samfunnssikkerhetens hus. Dette vil trolig også kunne bidra til kompetanseoverføring på tvers av enhetene dersom samvirke etableres. Etableringen av et slikt operasjonssenter vil gjøre det enklere å samhandle om å håndtere hendelser med nasjonale sikkerhetsmiljøer som PST (Politiets sikkerhetstjeneste), Kommune C-SIRT (Nasjonalt senter for informasjonssikkerhet i kommunesektoren), Helse CERT (helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet) og NSM (Nasjonal sikkerhetsmyndighet).

For kommunen er det viktig at kompetanse og ressurser fra ulike miljøer blir brukt effektivt til å løse de oppgavene som må løses. I forlengelsen av å etablere SOC-basert operasjonssenter, skal kommunen også utrede behovet for et sentralt testmiljø. Utredningen skal gjennomføres med sikte på å etablere et slikt miljø i løpet av strategiperioden. Det planlagte testmiljøet skal på sikt

[21] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/

[22] Security operation centre.

[23] Samfunnssikkerhetens hus (se byrådssak 1143/19)

teste systemer og IKT-løsninger underveis i utvikling, men også når løsningene skal tas/er tatt i bruk. Testmiljøet må samarbeide tett med SOC og det foreslåtte sentrale ressursmiljøet for utvalgte oppgaver (tjenester) som risikovurderinger, personvernkonsekvensvurderinger, databehandleravtaler, protokollføring og mer.

Det sentrale ressursmiljøet må vurdere risikoen av en løsning i lys av systemets kontekst og innhold. Deretter vil miljøet vurdere behovet for ytterligere sikring gjennom ulike sikringstiltak som f.eks. kryptering eller to-faktorautentisering. Hvilken effekt sikkerhetstiltaket har, vil bli testet av kommunens sentrale testmiljø med utgangspunkt i risikovurderingen. Sammen vil de ulike miljøene kunne avdekke sårbarheter (jf. GDPR Artikkel 32, bokstav D). De samlede miljøene skal samarbeide om å regelmessig teste, analysere og vurdere hvor effektive de tekniske og organisatoriske sikkerhetstiltakene er. I sum vil de samlede miljøene trolig øke kommunens kapasitet på til å forhindre brudd på personvern og informasjonssikkerheten vesentlig.

Prioriteringen for rekkefølgen av hvilke systemer, løsninger og behandlinger av personopplysninger som testes, analyseres og vurderes av de to miljøene skal gjøres på bakgrunn av gjennomførte risikovurderinger og eventuelle personvernkonsekvensvurderinger. I tillegg til dette, bør prioriteringen på rekkefølgen også avgjøres utfra hvilken type personopplysninger som behandles og hvilke(n) gruppe registrerte det gjelder. Systemer eller løsninger som behandler personopplysninger om barn og unge eller sårbare grupper, bør prioriteres sterkt i arbeidet med å sikre informasjonens konfidensialitet, integritet og tilgjengelighet.

Bergen kommune har gjennom GDPR en rekke plikter overfor den registrerte som omhandler informasjon, innsyn, retting og mer.[24] Økt oppmerksomhet omkring personvern, og rettigheter som tas mer i bruk, øker behovet for å ha en enhetlig standard for å oppfylle virksomhetens plikter overfor den registrerte.[25] På sikt vil nye løsninger, applikasjoner og systemer som utvikles av eller for Bergen kommune, ha «innebygget personvern» og personvern ved «design» [26] og «default» [27] som grunnleggende prinsipper. Disse prinsippene vil i fremtiden forenkle arbeidet med å oppfylle den registrertes rettigheter, men dette er gradvise endringer som tar tid. I dag løses disse oppgavene hovedsakelig ute i byrådsavdelingene, men med støtte og rådgivning fra konserngjennomgående funksjon.

Det er derfor behov for en bredere innsats for å forbedre disse arbeidsprosessene. I tråd med temaplanens hovedmål 1 og 2 skal Bergen kommune gi enhetlige og samordnede føringer for arbeidet med fagområdene. Ansatte eller innleide skal ha kompetanse til å håndtere personopplysninger, slik at fagområdene ivaretas i tråd med gjeldende regler. Personvern skal ha stor oppmerksomhet og være standard når nye løsninger blir utviklet. Det gjelder spesielt i de tilfellene hvor kommunen skal behandle personopplysningene til sårbare grupper (e.g. barn og unge). Høy grad av innebygd sikkerhet gjennom design og utvikling skal derfor være et

[24] Omtalt nærmere på s. 10 i temaplanen 1a-f.
[25] Se kapittel 3 i GDPR for en nærmere beskrivelse av den registrertes rettigheter.
[26] Personvern by «design» må forstås som at det tidligst mulig i prosessen hvor det utvikles løsninger for behandling av personopplysninger, iverksettes tilstrekkelige tekniske og organisatoriske tiltak for å beskytte personvernet.
[27] Personvern by «default» må forstås som at applikasjoner eller løsninger som standard har personvernvennlige innstillinger slik som at systemet kun viser personopplysninger på bakgrunn av rolle (tilgangsstyring) og informasjon det er behov for (tjenstlig behov).

grunnprinsipp for alle digitale systemer i Bergen kommune. Dette betyr at kommunens systemer skal være tilpasset rimelige forventninger til kompetansenivå hos ansatte og innleide.

Systemdesign, tilpassede brukergrensesnitt og tilgangsstyring skal bidra til å ivareta informasjonssikkerhet og personvern. Gjennom dette skal Bergen kommune ha en praksis som understøtter prinsippet om «innebygd sikkerhet» i tråd med Digitaliseringsdirektoratets veiledning på området.[28] Kommunen skal oppnå dette gjennom at informasjonssikkerhet er:

- Innarbeidet i virksomhetsstyringen og understøtter virksomhetens mål.
- Innarbeidet i virksomhetens prosesser og prosjekter fra starten av.
- Tatt hensyn til i hele livssyklusen til IKT-løsninger.
- Et tema alle ansatte i kommunen kjenner til og vet hva innebærer for sine arbeidsoppgaver.

Med bakgrunn i dette er det nødvendig at Bergen kommune i et tett samarbeid mellom byrådsavdelingene og konsernfunksjon utreder hvordan vi fremover kan løse utfordringene med å etablere en enhetlig praksis mellom byrådsavdelingene.

For å sikre måloppnåelse i tråd med temaplanens mål og helt sentrale lovkrav i kapittel 3 i GDPR, skal Bergen kommune derfor sette ned et nytt prosjekt som inkluderer alle byrådsavdelingene og konsernfunksjon. Prosjektet skal som en del av dette oppdraget utrede alternative løsninger. Det skal vurderes om «Min Side» kan brukes til å gjøre det enklere å få innsyn i egne personopplysninger. Arbeidsfordelingen mellom konsern og de andre byrådsavdelingene må utredes som en del av det innledende arbeidet. Prosjektet skal komme med en anbefaling for fremtidig oppgaveløsing og organisering, slik at kommunen effektivt oppfyller de registrertes rettigheter.

Bergen kommune skal satse på utvikling av syntetiske testdata.[29] Dette innebærer at kommunen skal vurdere syntetiske data fremfor reelle data/personopplysninger i forkant av fullskala implementering av systemer eller løsninger som behandler personopplysninger. Testing av løsninger, der personopplysninger av særlige kategorier eller særlig sårbare grupper behandles, skal gjøres i et adskilt miljø. Miljøet må være oppdatert for å sikre at aktive sårbarhetsanalyser og inntrengningstester kan gjennomføres uten å påvirke den registrertes personvern.

Samtidig med å følge prinsippene for innebygd personvern, skal kommunen ha en infrastruktur som gjør at vi kan levere tjenestene på en trygg måte. I tillegg til å levere tjenester trygt må infrastrukturen også legge til rette for den digitale transformasjonen. Kommunen skal vektlegge følgende prinsipper i fremtidig drift av IKT-systemer som behandler personopplysninger i anskaffelse, innfasing, etablering, forvaltning, endring og utfasing:

[28] https://www.difi.no/nyhet/2016/09/innebygd-informasjonssikkerhet

[29] Å bruke syntetiske testdata innebærer at virksomheten istedenfor å bruke reelle personopplysninger benytter kunstige personopplysninger. Dette gjøres for å teste sikkerheten ved behandling av personopplysninger i et mest mulig «naturlig» miljø, og for å forhindre at noe går galt ved behandlingen av ekte personopplysninger.

Personvern skal være innebygd i, og være grunnleggende innstilling (by design) for alle løsninger og systemer, som behandler personopplysninger i kommunen. Dette innebærer at alle systemer og løsninger blant annet skal ha funksjonalitet for:

- Rollebasert tilgang
- Autentisering
- Logging av bruk/endring
- Visning av personopplysninger begrenses alltid utfra tjenstlig behov

Bergen kommune skal følge prinsippet om at alle løsninger og systemer som behandler personopplysninger i kommunen blir utviklet på en slik måte at personvernet ivaretas.

I tråd med kommunens reviderte styringssystem for informasjonssikkerhet og personvern skal kommunen følge Nasjonal sikkerhetsmyndighets grunnprinsipper for sikkerhet. Grunnprinsippene for sikkerhet skal, sammen med kommunens vedtatte rammeverk for risikostyring, være kjernen i det videre sikkerhetsarbeidet:

1. Identifisere og kartlegge	• Kartlegg styringsstrukturer, leveranser og understøttende systemer • Kartlegg enheter og programvare • Kartlegg brukere og behov for tilgang
2. Beskytte og opprettholde	• Ivareta sikkerhet i anskaffelses- og utviklingsprosesser • Etabler en sikker IKT-arkitektur • Ivareta en sikker konfigurasjon • Beskytt virksomhetens nettverk • Kontroller dataflyt • Ha kontroll på identiteter og tilganger • Beskytt data i ro og i transitt • Beskytt e-post og nettleser • Etabler evne til gjenoppretting av data • Integrer sikkerhet i prosess for endringshåndtering
3. Oppdage	• Oppdag og fjern kjente sårbarheter og trusler • Etabler sikkerhetsovervåkning • Gjennomfør inntrengingstester
4. Håndtere og gjenopprette	• Forbered virksomheten på håndtering av hendelser • Vurder og klassifiser hendelser • Kontroller og håndter hendelser • Evaluer og lær av hendelser

Tabell 2: Prinsipper for en personvern- og sikkerhetsvennlig vennlig praksis i utvikling og forvaltning av systemer og løsninger.

Kommunen må alltid vektlegge å etablere infrastruktur, systemer, løsninger og organisatoriske/tekniske tiltak som gjør at organisasjonen evner å håndtere både små og store hendelser gjennom tilstrekkelig situasjonsforståelse. En tilstrekkelig situasjonsforståelse innebærer at Bergen kommune alltid er i stand til, og kan gjennomføre:

- Hendelseshåndtering på en slik måte at konsekvensene begrenses mest mulig.
- Infrastrukturanalyse for å avdekke svakheter i infrastrukturen, fremtidige eller pågående uønskede aktiviteter.
- Skadevareanalyse gjøres i henhold til virksomhetens retningslinjer, slik at skadevare ikke kompromitterer kommunens systemer.
- Trussel- og sårbarhetsforståelse videreutvikles kontinuerlig hos virksomhetens ansatte internt, og i samarbeid med nasjonale kompetansemiljøer.

Gjennom god hendelseshåndtering, tilfredsstillende kryptering basert på risikovurderinger, infrastrukturanalyse, skadevareanalyse, samarbeid med nasjonale kompetansemiljøer og trusselforståelse skal Bergen kommune sørge for at virksomheten unngår at:

- Uvedkommende får tilgang til informasjon i Bergen kommunes systemer som de ikke skal ha (konfidensialitet).
- Urettmessig eller ukontrollert endring av informasjon i et av Bergen kommunes systemer (integritet).
- Bergen kommune ikke får tilgang til egen informasjon (tilgjengelighet).

Oversikt og kontroll med infrastruktur er en forutsetning for at kommunen når temaplanens fem hovedmål. Dette innebærer at kommunen fremover må bygge kapasitet og kompetanse til å iverksette egnede organisatoriske og tekniske tiltak rundt infrastrukturen. Gjennom tilstrekkelig kapasitet, verktøy og kompetanse må kommunen lykkes med å etablere og vedlikeholde en oversikt over nettverkstrafikken i virksomhetens infrastruktur som logges og følges opp tilstrekkelig.

Med hensyn til hovedmål 4 og 5, er infrastruktur som tåler det ukjente et sentralt premiss. Bergen kommune skal ha en infrastruktur som tåler skalering i volum, og som er forberedt på å levere også under uforutsette hendelser. Kommunen må derfor legge til rette for at virksomheten har en digital infrastruktur som *tåler* nye og uforutsette hendelser. Dette utfordrer Bergen kommune både på *kapasitet* og *bruksmetodikk*.

Bergen kommune vil

Etablere et operasjonssenter for sikkerhet, SOC, som skal samarbeide tett med Samfunnssikkerhetens hus.

Utrede behovet for å etablere et sentralt miljø for testing og utvikling av testmetodikk. Utredningen skal gjøre rede for organisering, kostnader og videre innretting med sikte på å etablere et slikt miljø i strategiperioden.

Utrede hvordan Bergen kommune enklere og mer effektivt kan oppfylle retten til innsyn på tvers av kommunens fagsystemer og løsninger. Utredningen skal avklare hvilke fagsystemer som bør integreres med «Min Side» (portal). Arbeidet skal også redegjøre for kostnader, ansvarsfordeling mellom byrådsavdelingene og videre innretting med sikte på å etablere den nye funksjonaliteten i Min Side i strategiperioden.

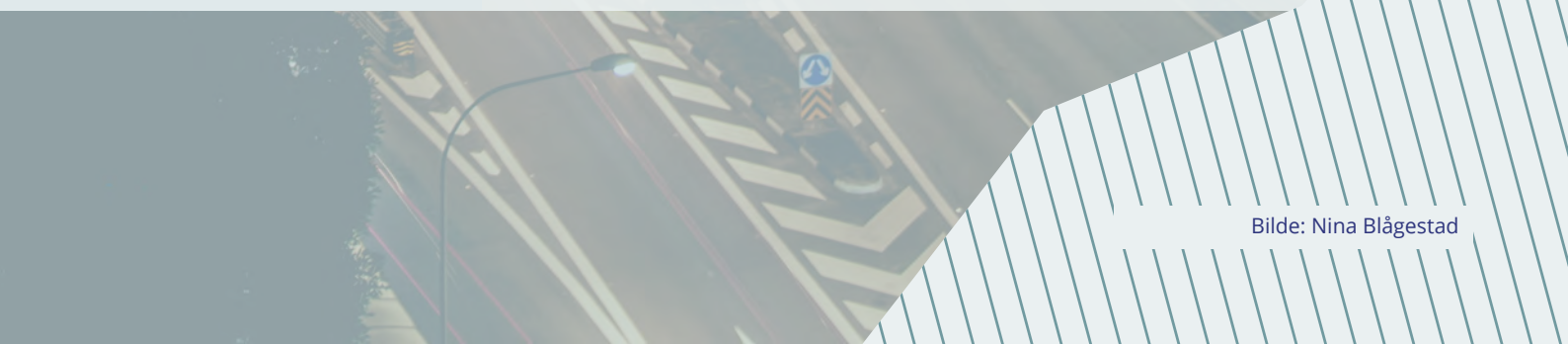
Det skal utarbeides en oversikt over tiltak for tilstrekkelig sikring av kommunalt endepunktsutstyr.

At to-faktorautentisering eller tilsvarende skal være standard verifiseringsmetode for alle løsninger Bergen kommune bruker, der det er teknisk og praktisk gjennomførbart, og nødvendig for å sikre behandling av personopplysninger og ivareta informasjonens sikkerhet. Med utgangspunkt i dette skal kommunen også etterstrebe en mest mulig brukervennlig løsning.

5

Strategisk satsingsområde:

Infrastruktur og forvaltning av fagsystem



Bilde: Nina Blågestad

5. Strategisk satsingsområde: Infrastruktur og forvaltning av fagsystem

For å sikre informasjon og personvern er det en forutsetning at kommunen lykkes med å drifte og forvalte infrastruktur og systemer i henhold til beste praksis. En slik praksis i organisasjonen, vil understøtte informasjonssikkerhet i alle løsninger og tjenester.

Innenfor IKT-sikkerhet er det en realitet at manglende vedlikehold av infrastruktur og systemer direkte påvirker sikkerheten. Infrastrukturen og systemene må derfor jevnlig vedlikeholdes for å ivareta informasjonssikkerheten. For systemer må kommunen følge leverandørers versjonsoppdateringer slik at man til enhver tid har de siste sikkerhetsoppdateringene. Samtidig er det en forutsetning at infrastruktur og komponenter gjennom vedlikehold og kontroll oppdateres og skiftes ut ved behov.

Noen konsernomfattende elementer i infrastrukturen blir i dag forvaltet og vedlikeholdt av Byrådsavdeling for finans, næring og eiendom gjennom Enhet for digitale driftstjenester (EDD). Fagspesifikk infrastruktur og systemer eies i dag av den enkeltstående byrådsavdeling. Ansvaret for å oppdatere og vedlikeholde infrastrukturen og systemene, tilhører dermed den aktuelle byrådsavdelingen med eierskap til infrastrukturen og de fagspesifikke systemene. Konsernfunksjon fungerer i dag som rådgiver og veileder overfor byrådsavdelingene i disse spørsmålene. I et IKT-sikkerhetsperspektiv må infrastrukturen og kommunens samlede systemer ses i sammenheng med hverandre. Konsekvensen av at ett system eller enkeltdeler av infrastrukturen ikke systematisk blir vedlikeholdt og oppgradert kan være alvorlig. Et sentralt miljø må følge opp, veilede og pålegge vedlikehold, oppgradering eller endring av fagspesifikke systemer og infrastruktur hos den enkelte byrådsavdeling, hvis disse ikke møter kravene til personvern og informasjonssikkerhet.

I bystyresak 215/18 ble det besluttet å etablere redundant datasenter for parallell drift av virksomhetskritiske systemer i Bergen kommune.[30] Redundans betyr at systemer og informasjon, som regnes som virksomhetskritiske, vil være tilgjengelige fra to lokasjoner. I praksis betyr dette at dersom noe skulle føre til at systemer eller informasjon blir utilgjengelig fra det ene datasenteret, kan Bergen kommune innen rimelig tid, tilgjengeliggjøre system og informasjon gjennom det andre datasenteret. Dette er i tråd med temaplanens satsingsområde *innebygd personvern, infrastruktur og systemer som tåler det uforutsette* og prinsippet om at informasjon skal være *tilgjengelig* for de som har et tjenstlig behov.

[30] Gjennomføringsvedtak for etablering av redundant datasenter.

Med drift av virksomhetskritisk infrastruktur på to lokasjoner, tar det kortere tid å få opp tjenestene ved en uforutsett hendelse. For å møte behovet for å videreutvikle kommunens kapasitet til å sikre informasjonens tilgjengelighet, er det nødvendig å etablere et sentralt styrt prosjekt med tre faser. Prosjektet må, for å sikre informasjonens tilgjengelighet, gjennomføre en kartlegging sammen med byrådsavdelingene for å avklare hvilke systemer og løsninger som skal etableres i det nye redundante datasenteret. Prosjektet må i fase 1 belyse flere viktige dimensjoner:

1. Hvilke systemer og løsninger skal etableres i det nye datasenteret i tillegg til det primære datasenteret.
2. Avklare ambisjonsnivå for redundansen vedrørende det enkelte system og løsning.

Fase 1 i prosjektet.

Basert på de funnene og konklusjonene som gjøres i prosjektets første fase, må arbeidet med fase 2 starte som en del av prosjektet beskrevet over. I samarbeid med leverandører innebærer denne fasen planleggingen av oppstart, og forberedelser til redundant drift av systemene som prioriteres gjennom fase 1 i prosjektet. På sikt innebærer dette arbeidet også en tredje fase. I fase 3 vil kommunen gjennomføre selve etableringen av redundant drift for systemene i det nye datasenteret. Denne fasen må imidlertid planlegges og vurderes nærmere igjennom senere prosesser, fordi ambisjonsnivå og kostnadsbilde ikke fullt ut er avklart før fase 1 og 2 er gjennomført.

Bergen kommune vil

Sette ned et sentralt styrt prosjekt som i fase 1 skal utrede hvilke kommunale systemer og løsninger som skal etableres i det redundante datasenteret. Prosjektet skal også avklare ambisjonsnivå for hvor raskt det enkelte system og løsning kan tilgjengeliggjøres, dersom det primære datasenteret utsettes for en uforutsett hendelse. Basert på konklusjonene fra fase 1, skal prosjektet i fase 2 sammen med leverandører starte arbeidet med å planlegge og forberede oppstart av redundant drift av systemene.

6

Strategisk satsingsområde:

Organisering, tilrette-legging og etterlevelse

Bilde: Unsplash.com

6. Strategisk satsingsområde: Organisering, tilrettelegging og etterlevelse

Informasjonssikkerhet handler om at virksomheten har et bevisst forhold til *hva* slags informasjon som forvaltes, og hvordan virksomheten sikrer informasjonen mot unødig innsyn, endring eller tap. Personvern som fagområde legger føringer på hvilke personopplysninger som behandles og hvordan kommunen avveier innbyggernes rettigheter mot kommunens eget behov. Personvern og informasjonssikkerhet er regulert av personopplysningsloven som gjennomfører personvernforordningen (GDPR) i Norge, e-forvaltningsforskriften, sikkerhetsloven, pasientjournalloven og i annen sektorspesifikk lovgivning.[31]

Personvernregelverket krever at personopplysninger skal beskyttes på en tilfredsstillende måte mot unødig innsyn og endringer. Samtidig skal personopplysningene være tilgjengelig for dem som i tjenesten har behov for å behandle opplysningene.[32] Personvernet avhenger av tilstrekkelig informasjonssikkerhet som på tilfredsstillende vis håndterer risikoen for at informasjon tilgjengeliggjøres for uvedkommende, endres eller blir utilgjengelig for de som har tjenstlig behov for den. Informasjonssikkerhet handler om å håndtere risikoen for at personopplysninger og andre informasjonsverdier blir utsatt for brudd på informasjonens konfidensialitet, integritet eller tilgjengelighet.

Personvernforordningen, e-forvaltningsforskriften og kommuneloven stiller krav om at virksomheter skal ha en systematisk tilnærming til etterlevelsen av lov- og regelverk. Kommunen må sikre tilstrekkelig intern styring og kontroll, som gjør at vi kan sette i verk tekniske og organisatoriske tiltak som reduserer risiko ved behandling av personopplysninger og brudd på informasjonens konfidensialitet, integritet og tilgjengelighet. Et viktig virkemiddel er kommunens styringssystem på området og kvalitetssystemet (BkKvalitet).[33] I tråd med kommunens rammeverk for internkontroll må kommunen derfor hele tiden[34]:

[31] E-forvaltningsloven §15 slår fast at internkontrollen på informasjonssikkerhetsområdet skal være basert på anerkjente standarder, omfang og innretningen på internkontrollen skal være tilpasset risiko.
[32] Tjenstlig behov oppstår når tilgang til opplysninger er nødvendig for at en ansatt skal utføre jobben sin. Ansatte uten saklig grunn til å se opplysningene skal ikke ha tilgang.
[33] Løsningen er utviklet og driftet av Extend: EQS Kvalitetssystem.
[34] Byrådssak 1401/14 «Internkontroll i Bergen kommune. Overordnet rammeverk».

Figur 1: visualisering av sentrale oppgaver for konsernansvarlig byrådsavdeling og de andre byrådsavdelingene i arbeidet med å sikre god risikostyring.

Hvis vurderingene viser manglende eller utilstrekkelige tiltak, må behandlingsansvarlig vurdere å iverksette nye tiltak for å etablere tilfredsstillende sikkerhet. Deretter må de nye tiltakene følges opp gjennom kontrollrutiner for å sikre at de nye tiltakene virker etter hensikten.

E-forvaltningsforskriften krever at virksomheten bruker anerkjente standarder for internkontroll på informasjonssikkerhetsområdet. ISO/IEC 270001 er et eksempel på en slik standard, og er anbefalt av nasjonale myndigheter på området. Kommunens reviderte styringssystem for informasjonssikkerhet og personvern er derfor blitt revidert og bygger på ISO-27000 serien.

Figur 2: Visualisering av risikostyring i Bergen kommune som er basert på ISO-standard for risikostyring, ISO 31000.

Systematiske aktiviteter skal være kjernen i Bergen kommunes internkontroll på informasjonssikkerhetsområdet. Det er også nødvendig for å sette i verk risikobaserte sikkerhetstiltak. Disse må være basert på grundige risikovurderinger. Virksomheten må hele tiden følge kommunens vedtatte rammeverk for risikostyring slik figuren over viser. Samtidig må alle sikre at internkontrollen på informasjonssikkerhetsområdet er i tråd med kravene i lov- og regelverk.

Bergen kommune skal ha god styring og kontroll med informasjonssikkerhet og på personvernområdet. Den helhetlige gjennomgangen og forvaltningsrevisjonen (2019) har

dokumentert mangelfulle risikovurderinger. Slike risikovurderinger må gjøres for å gjennomføre gode sikkerhetstiltak, kunne styre og ha god kontroll på området.

I tråd med hovedmål 1 skal Bergen kommune gi helhetlige og samordnede føringer for arbeidet med informasjonssikkerhet og personvern. Disse skal hele organisasjonen etterleve. Byrådssak 1401/14 definerer det konkrete oppdraget byrådsavdeling for finans, næring og eiendom som konsernavdeling har for å tilrettelegge, veilede og sikre etterlevelse av personvernregelverket og informasjonssikkerhet. God tilrettelegging fra konsernfunksjon er en forutsetning for etterlevelse i resten av organisasjonen.

Bergen kommune er organisert etter en parlamentarisk styringsmodell med byrådsavdelinger på myndighetsnivå 1, og etater/resultatenheter på myndighetsnivå 2 og 3. Med en sektorbasert tilnærming for å løse oppgaver, er en av hovedutfordringene som har vært trukket frem av forvaltningsrevisor, manglende etterlevelse av styringssystemet for informasjonssikkerhet. For å sikre etterlevelse av styringssystemets regler og prosedyrer har styringssystemet blitt revidert som en del av den helhetlige gjennomgangen.[35]

Skal hele organisasjonen kunne etterleve kravene må styrende dokumentasjon og veiledning alltid være:

Forståelig: Veiledningen, rådgivningen og styrende dokumentasjon skal være enkel å forstå.
Målrettet: Veiledningen, rådgivningen og styrende dokumentasjon skal tilpasset rollen som systemeier, systemkoordinator, behandlingsansvarlig eller andre roller i virksomheten med et særlig ansvar for informasjonssikkerhet og personvern.
Faglig korrekt: Veiledningen, rådgivningen og styrende dokumentasjon skal være faglig korrekt, oppdatert og skal fortløpende revideres ved behov.
Tilgjengelig: Ansatte skal enkelt finne frem til rådgivningen, veiledningen og styrende dokumentasjon de trenger for å fylle egen rolle på en god måte.

Tabell 3: Prinsipper for veiledning, rådgivning og styrende dokumentasjon fra konsern til byrådsavdelingene.

Det er kritisk at både ledelsen og de ansatte vet hvilke oppgaver de har, og hvordan de skal løse disse oppgavene. For å lykkes med dette er det nødvendig med enhetlig veiledning fra konsernfunksjon. Baset på vurderinger i helhetlig gjennomgang vil det på sikt bli obligatorisk å følge prosjekthåndboken for alle digitaliseringsprosjekter i kommunen. At det blir obligatorisk å følge prosjekthåndboken vil forenkle konsernfunksjonens arbeid med å utføre etterkontroller.[36] Det blir også lettere å følge opp og støtte byrådsavdelingene.

[35] Styringssystemet for informasjonssikkerhet i Bergen kommune bygger på ISO-standard 27001.
[36] Det kan dreie seg om kontroller av protokoll eller andre krav til tiltak forordningen viser til.

For å vite hvordan man skal løse oppgavene krever det en bred innsats fra både konsern og byrådsavdelingene for å:

1. Sikre økt kompetanse hos de ansatte ute i byrådsavdelingene på fagområdene.
2. Øke kapasitet til å støtte byrådsavdelingene hos konsernfunksjon.
3. Legge til grunn medvirkning i utøvelsen av konsernoppdraget på fagområdene.

Et revidert styringssystem, en tydeligere konsernfunksjon, oppdaterte veiledere, klare beskrivelser av roller og oppgaver, er nødvendig for å sikre at lovkrav blir etterlevd i hele virksomheten. Gode hjelpemidler for å få til dette, er at konsernansvarlig funksjon etterstreber medvirkning der det produseres veiledning, rådgivning, styrende dokumentasjon, støtteverktøy m.m. med representanter for de rollene det gjelder.

Samarbeid og klok organisering av oppgaver gir kvalitets- og stordriftsfordeler. Dette gjelder både byrådsavdelingene og konsernfunksjon. Forvaltningsrevisjonen i 2019 og helhetlig gjennomgang viser at kommunen mangler en felles tilnærming til forholdsvis like prosesser.

I dag gjennomføres risikovurderinger og personvernkonsekvensvurderinger i den enkelte byrådsavdeling. Byrådsavdelingene får råd og veiledning fra avdeling for personvern og informasjonssikkerhet sentralt i kommunen. Fra før vet vi at når oppgaver utføres sjelden, kan det gå ut over kvaliteten på arbeidet. Flere oppgaver kan potensielt løses mer hensiktsmessig, dersom oppfølgingen av disse plasseres i et større fagmiljø. Et større fagmiljø som utfører og støtter kommunen og behandlingsansvarlig på ressurskrevende oppgaver som personvernkonsekvensvurderinger, testing, risikovurderinger med mer, kan være et hensiktsmessig grep ref. for eksempel planens foreslåtte tiltak nr. 8.

En slik organisering kan føre til at byrådsavdelingene opplever at de får mindre innflytelse over utviklingen av løsninger som skal dekke deres faglige behov. En flytting av ansvar og prosesser må sørge for at byrådsavdelingene fortsatt har reell innflytelse på faglig utvikling av systemer som skal løse deres behov. Behandlingsansvaret vil fortsatt ligge til den enkelte kommunaldirektør. Da er det kritisk at byrådsavdelingene har nok ressurser og kapasitet til å forvalte behandlingsansvaret. Kapasiteten til byrådsavdelingene må være slik at de har nødvendig og nok kompetanse til å håndtere kompleksiteten i arbeidsprosessene fremover. Dette må gjøres i tråd med de funn som er gjort i den helhetlige gjennomgangen, og konkrete risikobaserte vurderinger som gjennomføres i den enkelte byrådsavdeling.

Kommunen vil se nærmere på fremtidens behov for ressurser med kompetanse rundt risikovurderinger, personvernkonsekvensvurderinger og protokollføring i relasjon til behovet for et sentralt ressursmiljø for utvalgte oppgaver (tjenester). Da kan kommunen bygge en mer solid oppgaveløsing som kan betjene byrådsavdelingene og kommunen i stort. Bergen kommune skal ha kapasitet til å gjennomføre arbeidet med tilfredsstillende kvalitet. Samtidig må vi sørge for at byrådsavdelingene har nok kapasitet til å ivareta personvern og informasjonssikkerhet i utførelsen og utviklingen av tjenester. I sum handler dette om å etablere et egnet sikkerhetsnivå for behandling av personopplysninger i hele Bergen kommune.

Alle offentlige virksomheter er pålagt å ha et personvernombud.[17] I tråd med forordningen skal Bergen kommune ha et personvernombud som er uavhengig og dermed fri fra instruksjon og interessekonflikter. Kommunen trenger også et faglig sterkt personvernombud med gjennomslagskraft i organisasjonen. I forbindelse med implementeringen av GDPR presiserte Datatilsynet hvilke krav til uavhengighet som må stilles til personvernombudet, og hvilke mulige

interessekonflikter som bør vurderes i den enkelte organisasjon. Datatilsynet gjorde rede for hvilke roller som i kombinasjon med personvernombudsrollen vil og kan føre til interessekonflikter. Primært kan derfor personvernombudsrollen ikke kombineres med ansvar, delegert eller direkte, for å bestemme formålet og måten personopplysninger behandles på.[37]

Som en del av arbeidet med å avdekke og utbedre påviste sårbarheter i kommunens systemer, prosesser og organisering i 2020, er det avdekket behov for et tydeligere skille mellom de oppgavene som er konserngjennomgående på informasjonssikkerhetsområdet og personvernombudets rolle og oppgaver i virksomheten. Det er en prioritert oppgave å sikre at personvernombudet er fri fra interessekonflikter, samtidig som ombudet gjennom oppdatert dybdekunnskap nær sentrale fagmiljø skal være i stand til å veilede virksomhetens ledelse og ansatte.

En endring av dagens sentrale fagmiljø for personvern og informasjonssikkerhet med vekt på de konserngjennomgående oppgavene knyttet til informasjonssikkerhet og personvern er foreslått innført medio 2021. I sum skal disse endringene bidra til at ombudets uavhengighet tydeliggjøres. Det skal også tilrettelegge for en fleksibel og robust oppgaveløsing også på de konserngjennomgående oppgavene i fremtiden.

Med bakgrunn i funn fra den helhetlige gjennomgangen, er det behov for et revidert informasjonssikkerhetsforum som spisses inn mot dagens behov. Behovet for et revidert informasjonssikkerhetsforum forsterkes ytterligere av omorganiseringen av arbeidet på feltet. Et slikt forum vil bli viktigere fremover fordi kommunens risiko- og sårbarhetsbilde stadig endrer seg. Den enkelte behandlingsansvarlige (kommunaldirektør) må derfor peke ut en fast representant som kan formidle byrådsavdelingenes perspektiver. Formatet på et revidert informasjonssikkerhetsforum må utredes med utgangspunkt i dagens og morgendagens behov. Den faste representanten bør ha en faglig kompetanse på områdene, og kunne[38]:

- Kommunisere risiko-, trussel- og sårbarhetsbilde for gjeldende byrådsavdeling til konsern- og egen byrådsavdeling.
- Spre informasjonssikkerhets- og personvernfaglig kompetanse i egen byrådsavdeling.
- Bestille rådgivning, veiledning og støtte fra konsernfunksjon til prosjekter eller løsninger ute i byrådsavdelingene.
- Varsle om svak informasjonssikkerhets- og personvernpraksis hos egen byrådsavdeling og sentralt hos konsern.

Bergen kommune er unik fordi vi har mye kunnskap om innbyggerne, samtidig som vi har mulighet til å kontakte alle for å hente inn mer informasjon. Dette og bredden i oppgaver kommunen skal løse, gjør oss til en ettertraktet samarbeidspartner for kunnskapsinstitusjoner som Universitetet i Bergen (UiB) og Høgskolen på Vestlandet (HVL) m.fl. Kommunen tar stadig i bruk nye muligheter for å jobbe mer kunnskapsbasert.

Forskning og kunnskapsinnhenting skjer oftere og i et større omfang enn tidligere. Det er nødvendig at kommunen etablerer premisser for hvordan dette skal gjøres på en måte som

[37] Datatilsynet om personvernombudets uavhengighet

[38] Det må også legges opp til en vara-ordning, slik at forumet til enhver tid er i stand til å gjennomføre oppdraget sitt.

tilfredsstiller kravene til informasjonssikkerhet og personvern. Forskning og kunnskapsinnhenting legger grunnlaget for at kommunen kan jobbe kunnskapsbasert og iverksette effektive tiltak som treffer målgruppene bedre. Behandling av personopplysninger er ofte en forutsetning for denne typen initiativer, og det blir desto viktigere at kommunen gjør dette på en god og forsvarlig måte.

Kommunen må både forvalte mulighetene som ligger i forskning og kunnskapsinnhenting og ansvaret overfor innbyggerne på en god måte. Kommunen må tenke nytt om hvordan vi i fremtiden skal være en aktiv og attraktiv samarbeidspartner for forskningsinstitusjoner, og samtidig sikre at prosjektene og informasjonsinnhenting er til det beste for innbyggerne. Derfor vil Bergen kommune utrede å etablere en funksjon etter inspirasjon fra Regionale komiteer for medisinsk og helsefaglig forskningsetikk (REK).

En slik funksjon kan vurdere og kvalitetssikre hjemmelfor behandlingen av personopplysninger og aspektene rundt informasjonssikkerhet og personvern ved behandlingen som ønskes gjennomført. Dette er noe som må utredes presist i form av et prosjekt som ser på behov, mulig organisering, formål, mandat, omfang og sammensetning. Videre skal prosjektet vurdere behovet for en regional eller nasjonal tilnærming.

Bergen kommune vil

Utrede behovet for å bygge opp et sentralt ressursmiljø for utføring og fasilitering av oppgaver (tjenester) som risikovurderinger, personvernskonsekvensvurderinger, databehandleravtaler og protokollføring. Utredningen skal gjøre rede for organisering, kostnader og videre innretting med sikte på å etablere et slikt kompetansemiljø i løpet av strategiperioden.

Konsernansvarlig funksjon for informasjonssikkerhet skal i løpet av strategiperioden utrede om ISO-standard 27000-serien har vesentlige fordeler i arbeidet med internkontroll på informasjonssikkerhetsområdet versus vedtatt rammeverk på konsernnivå som baserer seg på ISO-standard 31000. Utredningen skal anbefale hvorvidt 27000-serien skal ligge til grunn for kommunens internkontroll på området for informasjonssikkerhet i fremtiden.

Informasjonssikkerhetsforums mandat og sammensetning skal revideres i tråd med gjeldende fullmakter og funn fra den helhetlige gjennomgangen, slik at forumet er tilpasset dagens risiko- og situasjonsbilde.

Utrede behovet for en lignende funksjon, med vekt på personvern og informasjonssikkerhet, etter inspirasjon fra Regionale Komiteer for medisinsk og helsefaglig forskningsetikk. Dette skal gjøres gjennom en prosjektgruppe bestående av representanter for byrådsavdelingene med kompetanse på forskning, personvern, informasjonssikkerhet, jus og statistikk. Omfang, oppdrag og sammensetning skal belyses og prosjektet skal komme med anbefaling til løsning. Videre skal prosjektet vurdere behovet for en regional eller nasjonal tilnærming i disse spørsmålene.

7

Strategisk satsingsområde:

Samarbeid mellom det lokale, regionale og nasjonale

Bilde: Pexels.com

7. Strategisk satsingsområde: Samarbeid mellom det lokale, regionale og nasjonale

Hovedmål 3 fastslår at Bergen kommune skal samarbeide tett med lokale, regionale og nasjonale partnere for å styrke informasjonssikkerheten og ivareta personvernet. Demografiske endringer og et lavere inntektsgrunnlag gjør felles digitalisering til et nødvendig verktøy for å sikre økonomisk bærekraftige tjenester i fremtiden. Digitalisering er i tillegg et premiss for å både ivareta, og videreutvikle sikkerheten ved behandling av personopplysninger. Digitalisering sikrer tryggere og mer effektiv kommunikasjon gjennom blant annet krypterte løsninger mellom innbygger og kommunen. Som verktøy er digitalisering også nødvendig for å sette innbyggerne i stand til å hevde egne rettigheter gitt gjennom personopplysningsloven og GDPR.

Byrådets vurdering er at internt og eksternt samarbeid er en forutsetning for at Bergen kommune fortsatt skal levere gode og sammenhengende tjenester i fremtiden. Digi Vestland er et godt eksempel på at enkeltstående initiativer best kan koordineres og videreutvikles i fellesskap fremfor alene. Frem til nå har det regionale samarbeidet i hovedsak jobbet med å etablere og utvikle felles faglige arenaer for kommunene i samarbeidet, og gi tilgang til kompetanse og kapasitet gjennom fellesressurser. Gjennom Bergen kommunes engasjement i Digi Vestland og inn mot KS nasjonalt, skal kommunen utvikle egen fagkompetanse på fagområdene informasjonssikkerhet og personvern.

God informasjonssikkerhet, tilfredsstillende digital sikkerhet og ivaretakelsen av den enkeltes personvern er ikke noe kommunen kan lykkes med alene. Næringslivet, akademia og klynger spiller her en viktig rolle. Gjennom å engasjere seg, dele og erfare hva andre gjør, får Bergen kommune mulighet til å utvikle og forbedre egen metodikk for å ivareta informasjonssikkerhet og personvern i alle steg. Seksjon for digitalisering og innovasjon skal i tett samarbeid med Innkjøp konsern og byrådsavdelingene jobbe med å videreutvikle konkrete rutiner og sjekklister for blant annet følgende:

- Leverandørmarkedet skal ha lett tilgjengelig informasjon om kommunens krav til personvern i systemer som behandler personopplysninger.
- Det skal i tidlig fase av alle anskaffelser gjøres en risikovurdering og i de tilfellene der personopplysninger behandles, skal det også gjennomføres personvernkonsekvensvurdering.
- I leverandørdialog før anskaffelsesprosessen starter, skal det inngå informasjon om Bergen kommunes krav til behandling av personopplysninger, i henhold til databehandleravtale og kommunens arkitekturprinsipper.
- I kontraktbestemmelsene skal roller og rutiner i Bergen kommunes prosess for godkjenning og testing av leveranser beskrives.
- Det skal være faste rutiner for overlevering av kontrakter fra kontraktinngåelse til implementering og forvaltning med generell veiledning på kontraktoppfølging av særlig kritiske punkter i kontrakten.

Kommunen vil slik legge til rette for en tettere og bedre oppfølging av leverandører og forbedre egen innkjøpskompetanse. Sammen med absolutte minimumskrav skal dette sikre at informasjonssikkerhet og personvern ivaretas på en god måte i anskaffelser. Dette er særlig viktig hvis anskaffelsene angår sårbare grupper som f.eks. barn og unge. Byrådet legger til grunn at personvern og informasjonssikkerhet er absolutte minimumskrav som ikke vektes opp mot pris – dette er områder markedet og kommunen i fellesskap ved enhver anledning skal levere tilfredsstillende på. Erfaringene fra arbeidet over ønsker Bergen kommune etter hvert å dele med andre.

Bergen kommune skal fortsatt satse på et bærekraftig og gjensidig samarbeid med omegnskommunene. Byrådet er opptatt av at samtidig som at kommunens fagmiljø er med på å heve omgivelsenes kompetanse om informasjonssikkerhet og personvern. Sammen skal vi på sikt også etablere strukturer og rammer som kommer de registrerte til gode. Samarbeidet mellom Bergen og omegnskommunene skal bidra til å bygge kapasitet og kunnskap ute hos de andre i regionen, men også hos Bergen kommune.

Vi må også jobbe nasjonalt for å lykkes med å ha trygge lokale løsninger. Sentrale løsninger for register- og fellesdata, som ivaretar den enkeltes personvern og sikrer informasjon tilstrekkelig, må være et krav når kommunal sektor tar i bruk sentrale løsninger. Kommunal sektor må også få med seg de sentrale nasjonale aktørene for å skape gode retningslinjer ved bruk av nasjonale registerdata og fellestjenester lokalt. Den digitale transformasjonen forutsetter et nært samarbeid mellom forvaltningsnivåene.

For å få effektiv og trygg deling av data på tvers av forvaltningsnivåene, har Digitaliseringsdirektoratet utarbeidet «Norsk arkitekturrammeverk for samhandling».[39] Denne bygger på European Interoperability Framework (EIF). Det er kritisk at kommunal sektor klarer å beskytte informasjon og ivareta personvernet når sammenhengende tjenester blir utviklet på tvers av forvaltningsnivå og kommunegrenser. Bergen kommune skal oppfordre andre aktører til, men også aktivt ta forpliktende initiativ overfor andre, der etablering av felles retningslinjer, standarder og utveksling av ressurser og kompetanse står sentralt.

Felles datakatalog er et eksempel på et nasjonalt verktøy for å dele data mellom offentlige virksomheter. Katalogen har en begrepskatalog.[40] Denne katalogen er nøkkelen til å bygge felles begrepsforståelse ved bruk av register- og fellesdata på tvers. Uten bred enighet omkring praktisk bruk av felleskomponenter og fellesdata, blir det vanskeligere å utvikle nødvendige tjenester i fremtiden. Bergen kommune må fortsette å løfte disse og nye problemstillinger nasjonalt. Kommunen skal være en aktiv samarbeidspartner og drøfte dem med de relevante aktørene med sikte på å finne gode løsninger. Slik kan kommunen skape grunnlaget for trygge, gode og fremtidsrettede løsninger fra stat til kommune.

Hovedmål 3 legger også til grunn at virksomheten skal ta vare på den enkeltes rettigheter. For å ta vare på den registrertes informasjonssikkerhet og personvernrettigheter, må den registrerte være kjent med og forstå hvilke rettigheter de faktisk har. Bergen kommune må derfor satse på veiledning og innbyggerrettet informasjon som gjør at rettighetene er enkelt tilgjengelig og forståelig på eksisternde arenaer som nettsidene og innbyggerservice. Store grupper med tjenestemottakere mangler tilstrekkelig digital kompetanse eller kunnskap om egne rettigheter til

[39] https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/nasjonal-arkitektur/arkitekturrammeverk-samhandling
[40] https://fellesdatakatalog.digdir.no/

å ivareta egne interesser. Veilednings- og kunnskapsrettede tiltak er derfor ikke noe kommunen kun kan jobbe med internt, det må også prioriteres å jobbes med disse utadrettet. Dette kan handle om alt fra fysiske møter mellom kommunens ansatte og innbyggerne, til at innbyggerne mottar nye og digitale tjenester fra kommunen.

1. Innbyggere som ikke mestrer ny teknologi må få råd, støtte og veiledning til å håndtere den, når den er en forutsetning for å motta nye tjenester.
2. Innbyggerne må motta informasjon, råd og veilendning slik at de selv er kjent med egne rettigheter, forbundet med informasjonssikkerhet og personvern knyttet til kommunens tjenester.
3. Kommunen må jobbe for å spre kunnskap og holdninger knyttet til informasjonssikkerhet og personvern hos både unge og eldre.
4. Kommunen må ta i bruk virkemidler som sørger for at informasjonens konfidensialitet ivaretas uavhengig av den registrertes bakgrunn eller funksjonsnivå.

Dialogen kommunen har hatt med de kommunale rådene gjør at byrådet ser det er vesentlig å jobbe med å hjelpe innbyggerne til å være bevisst om sine rettigheter og sitt personvern. Ansatte i kommunen må ha kompetanse til å veilede og informere også til dem som ikke har anledning til å ta i bruk digitale tjenester. Med bakgrunn i punktene over, trenger kommunen en individuell, kollektiv og systematisk tilnærming for å øke kunnskapen på fagområdene blant de enkelte ansatte. Dette skal blant annet gjøres gjennom en variert sammensetning av kurs- og læringspakker.

Markedet leverer tjenester og løsninger hvor det ikke er hensiktsmessig at Bergen kommune selv utvikler eller drifter dem. Eksempler på dette kan være skytjenester som Microsoft 365 eller Google Workspace. I mange tilfeller behandler også de eksterne aktørene personopplysninger på vegne av Bergen kommune. I slike tilfeller, regulereres dette gjennom en databehandleravtale mellom behandlingsansvarlig og databehandler. I de tilfellene eksterne behandler personopplysinger om sårbare grupper er det en prioritert oppgave for kommunen å følge opp at databehandlers organisatoriske og tekniske tiltak for å ivareta personvernvernet er tilstrekkelig.[41] Innbyggerne i Bergen kommune må være trygge på at når personopplysninger behandles eksternt, så ivaretar både kommunen og databehandler de kravene som stilles i personopplysningsloven. Bergen kommune forventer at med økt testing av løsninger og systemer i adskilte miljøer i forkant av lansering, og også under forvaltning vil senke risikoen for brudd på personvern og informasjonssikkerhet vesentlig.[42]

[41] Dette kan være barn, unge, pasienter, asylsøkere og andre.
[42] Testing av systemer, løsninger m.m. som behandler personopplysninger skal alltid være i tråd med kommunens arkitekturprinsipper.

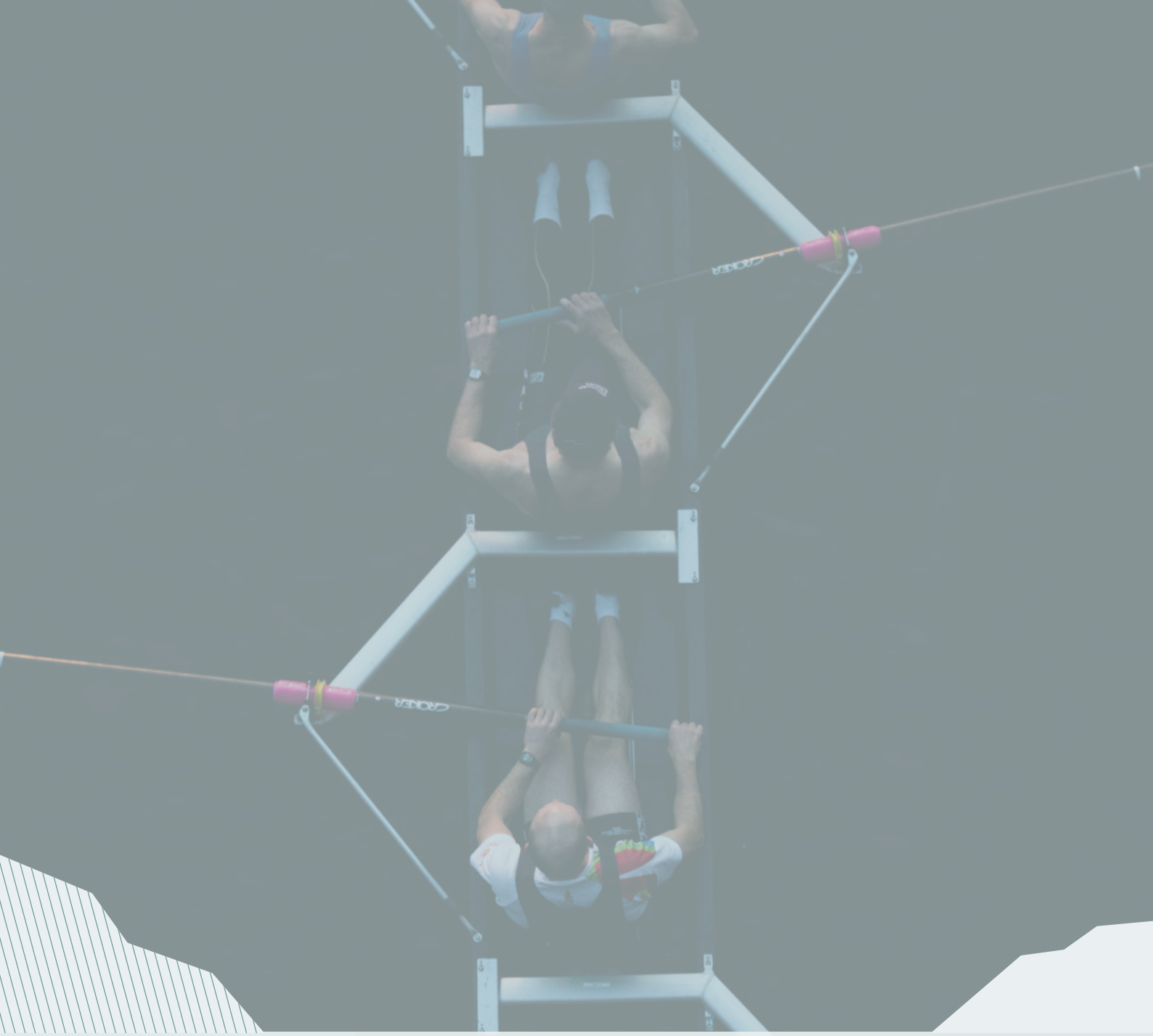
Bergen kommune arbeider for at det skal bli enklere å ta i bruk innovative anskaffelser, men fremover blir det enda viktigere å videreutvikle dette i fellesskap med regionale og nasjonale aktører.[43] Over tid har vi sett en endring i leverandørmarkedet når tilbyderne skal fortolke ansvar og plikter i rollen som leverandør eller som databehandler etter personopplysningsloven. For kommunen betyr dette at innsatsen inn mot kontraktsoppfølging, leverandørstyring og revisjon av avtaler må forsterkes, og vi må lete etter beste praksis med hensyn til fagområdene personvern og informasjonssikkerhet. Dette må gjøres slik at også andre kommuner og virksomheter kan nyttiggjøre seg ny kunnskap. Bergen kommune må sette anskaffelser i et informasjonssikkerhets- og personvernperspektiv på agendaen både i egen organisasjon, men også i regionale og nasjonale forum.

Bergen kommune vil

Bergen kommune skal videreutvikle metodikk sammen med andre kommuner og nasjonale aktører, for å forbedre egne anskaffelsesprosesser og forsterke kontraktsoppfølging, leverandørstyring og revisjon av avtaler i et informasjonssikkerhets- og personvernperspektiv.

Kommunen skal på eksisterende arenaer, ta intitiativ til at storbyene etablerer en mer aktiv fagdialog på områdene informasjonssikkerhet og personvern.

[43] Se for eksempel innovasjonspartnerskapet 1.000 bygg – 10.000 muligheter.



8

Strategisk satsingsområde:

Kompetanse, sikkerhets- og personvernkultur

Bilde: Unsplash.com

8. Strategisk satsingsområde: Kompetanse, sikkerhets- og personvernkultur

Med bakgrunn i hovedmål 2, skal Bergen kommune intensivere innsatsen for å sikre at alle ansatte og alle innleide ressurser har kompetansen de trenger for å ivareta sitt informasjonssikkerhets- og personvernansvar. Vår viktigste ressurs er medarbeiderne. De ansatte er også kommunens viktigste representanter for å sikre personvernet og informasjonssikkerheten. Byrådet vil at kommunen skaper gode læringssituasjoner og læringsarenaer for de ansatte. Kun en organisasjon med ansatte som er satt i stand til å avdekke og melde inn brudd på informasjonssikkerhet og personvern, kan utvikle den personvern-sikkerhetskulturen som kreves i den digitale transformasjonen.[44]

Fagområdene informasjonssikkerhet og personvern er i kontinuerlig endring ettersom stadig ny teknologi, nye sårbarheter og nye trusler gjør seg gjeldende. Bruken av informasjon endrer seg, og det oppdages stadig nye teknologiske metoder for å levere tjenester til innbyggerne. Helhetlig gjennomgang har dokumentert at situasjonen krever en annen tilnærming til de ansattes kompetanseutvikling i kommunen enn tidligere. Dette fører til endringer i – og gir nye muligheter for - hvordan organisasjonen driver rekruttering, opplæring og kompetanseplanlegging.

I tråd med ISO/IEC 270001:2013 kap. 7.2 skal Bergen kommune tilse[45]:

Fastslå hvilken kompetanse som er nødvendig for personen(e) som utfører arbeid under kommunens styring, og som påvirker dens informasjonssikkerhet
Sikre at disse personene har kompetanse tilegnet gjennom passende utdanning, opplæring eller erfaring.
Der det er relevant, iverksette tiltak for å erverve nødvendig kompetanse og evaluere virkningen av tiltakene som er truffet.
Oppbevare relevant dokumentert informasjon som bevis på kompetanse.

Tabell 4: Oversikt over utvalgte forutsetninger for å etterleve ISO/IEC 270001:2013.

Byrådet er opptatt av at arbeidet med kompetanse, opplæring og personvern- og sikkerhetskultur på fagområdene informasjonssikkerhet og personvern, er i tråd med HR-meldingens satsingsområder og etter inspirasjon fra standarden ISO/IEC 270001:2013. [46] Bergen

[44] Nasjonal sikkerhetsmyndighet definerer sikkerhetskultur slik: «Sikkerhetskultur handler om atferd knyttet til sikkerhet, for eksempel i forhold til informasjon eller objekter. Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd.

[45] ISO/IEC 270001:2013 spesifiserer kravene for å etablere, implementere, vedlikeholde og utvikle et styringssystem for informasjonssikkerhet i virksomheten.

[46] Et arbeidsliv i endring. HR-melding for Bergen kommune som arbeidsgiver.

skal være en fremtidsrettet og endringsdyktig kommune som følger lovkrav om informasjonssikkerhet og personvern. I tråd med HR-meldingen som bystyret behandlet i oktober 2019, er det nødvendig at kommunen er fremtidsrettet, endringsdyktig, inkluderende og attraktiv som arbeidsgiver.

Den helhetlige gjennomgangen har dokumentert behovet for en systematisk individuell og kollektiv kompetanseheving. Digitale virkemidler, som muliggjør bruken av individuelle og standardiserte opplæringsplaner for å videreutvikle den enkelte ansattes kompetanse på fagområdene, skal på sikt tas i bruk i virksomheten. Etter hvert vil resultater, mål og læringspunkter ut fra de krav som ligger til rollen bli en integrert del av medarbeidersamtalen for den enkelte ansatte. Kurs- og opplæringspakker vil tilpasses den enkelte funksjon, stilling og rolles behov for kompetanse og kunnskap på fagområdene. Som et mellom- og langsiktig grep er dette med på å berede grunnen for en kompetent organisasjon i arbeidet med å beskytte informasjon og ivareta den enkeltes personvern. Slik kan virksomheten rekruttere riktig og godt, og videre gi kyndige råd og støtte til både innbyggere og medarbeidere.

For å nå bredt ut i organisasjonen er det viktig at Bergen kommune jobber langs flere akser når det gjelder kompetanse og personvern- og sikkerhetskultur. [47] Fremover vil kommunen satse bredt med flere ulike virkemidler og verktøy for å sikre en kompetanseutvikling bygget på anerkjent metodikk. Kommunen vil ta i bruk både teknologistøttet læring og mer tradisjonelle kursopplegg. Kompetansepakken består av selvstudium, «på jobben-trening», gruppediskusjoner/fellesrefleksjon, veiledning og kollegastøtte. For at kompetanseutvikling skal gå i dybden og føre til varig endring både hos den enkelte ansatte og i organisasjonen (organisasjonslæring) bør det i fremtiden satses på flere virkemidler samtidig. Virksomheten skal ta i bruk «blandet læring». Hensikten er å kombinere e-læring og andre mer «analoge» metoder over tid. Dette vil i mange tilfeller kunne være gunstig for å skape varig endring.

Teknologistøttet læring kombinert med mer tradisjonell kompetanseutvikling, åpner opp for nye muligheter knyttet til aktiv oppfølging av medarbeidere. På den ene siden muliggjør teknologistøttet læring og undervisningsopplegg som i større grad er tilpasset den enkeltes rolle, og de kan også raskt justeres i tråd med det til enhver tid gjeldende risiko- og sårbarhetsbildet. På den andre siden gir også teknologistøttet læring muligheten til å tenke nytt omkring allerede eksisterende prosesser. Byrådet legger til grunn at mulighetsrommet teknologistøttet læring gir, aktivt brukes for å tilrettelegge undervisning tilpasset de ansattes reelle behov og rolle i organisasjonen. Systematisk planlegging basert på kunnskap om avvik blir et viktig virkemiddel for tilpasset opplæring i fremtiden.

Historisk sett har helse- og omsorgssektoren jobbet mye med å etablere en kultur for å melde avvik i sin sektor. At avvik meldes inn, og at disse kan følges opp, er en viktig forutsetning for systematisk kollektiv og individuell læring i organisasjonen. Ledere spesielt, men også medarbeidere har et ansvar for å jobbe i fellesskap med å skape en meldekultur i virksomheten. Ledere i Bergen kommune skal aktivt jobbe med å trygge de ansatte, slik at avvik meldes inn i tråd med retningslinjene og de fristene virksomheten har, for å eventuelt melde videre til Datatilsynet. Systematisk planlegging av kompetanseheving ute i byrådsavdelingene og

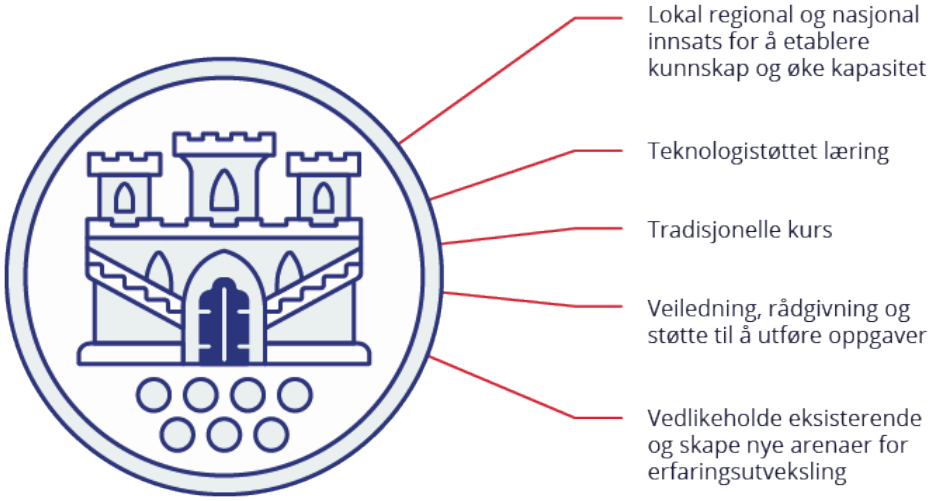
[47] Bergen kommune skal ha en kompetanse- og tiltakspakke på områdene informasjonssikkerhet og personvern i tråd med det som kalles for «blandet læring». Blandet læring innebærer at man tar i bruk en kombinasjon av ulike tilnærminger til læring, og til enhver tid tar i bruk de mest egnede metodene i et undervisningsperspektiv for å oppnå et mål.

konsernfunksjon, basert på erfaringer fra avvikshåndtering og oppfølging gjennom kvalitetssystemet, blir fremover et svært viktig virkemiddel for å sikre at virksomhetens ansatte gis tilpasset opplæring i fremtiden.

Kommunen skal ta i bruk ny metodikk for å endre kultur, holdninger og skape bevissthet. Bergen kommune skal derfor som en av flere metoder satse på modulbasert læring. KS-Læring legger til rette for det.[48] Å tilby enkelt tilgjengelige kurs- og kompetansepakker gjennom interaktiv modulbasert læring er viktige grep for å nå målsettingene nevnt over. Tradisjonell klasseromsundervisning, nanolæring, dilemmatrening, fagsamlinger, modulbasert læring gjennom KS-læring og andre former for «på jobben-læring», må kombineres med en systematisk planlegging og oppfølging av medarbeideres og lederes kompetanseutvikling på områdene.

Byrådet ønsker at medarbeidere og ledere i kommunen har kompetansen de trenger for å fylle egen rolle. Derfor innfører kommunen et digitalt system for kompetansestyring: Kompetanseportalen. For å sikre at alle ansatte har den samme grunnleggende kompetansen for bl.a. personvern og informasjonssikkerhet, vil det bli utarbeidet grunnleggende kompetanseplaner for de ansatte ut fra deres roller. Systemet vil også gi mulighet for å styre videre kompetanseutvikling innenfor feltet, både på individuelt og strategisk nivå.

Kunnskaps- og situasjonsbildet er i dag fragmentert og spredt på ulike steder i offentlig sektor. Ansatte i kommunen må oppsøke ulike kunnskapskilder for å holde seg oppdatert på fagområdene informasjonssikkerhet og personvern. Dette er en gjengs utfordring. I tråd med satsingen på Digi Vestland og opp mot det regionale og nasjonale nivået, skal Bergen kommune aktivt jobbe for å involvere flere av de nasjonale aktørene på eksisterende arenaer for fagområdene informasjonssikkerhet og personvern i arbeidet med kompetanse. Aktuelle aktører kan for eksempel være Datatilsynet, Politiets sikkerhetstjeneste, Digitaliseringsdirektoratet, forskjellige kunnskapsinstitusjoner, Nasjonal sikkerhetsmyndighet og Direktoratet for sikkerhet og beredskap m.m.



Figur 4: Visualisering av det langsiktige arbeidet med sikkerhetskompetanse og kultur samlet.

[48] Kommunesektorens organisasjon har gjennom KS-læring etablert en nasjonal modulbasert kurs- og læringsplattform som tilbyr kompetanseheving innen ulike fag og format for kommuner og fylkeskommuner.

Bergen kommune vil

Bergen kommune skal tilse at kompetansetiltak i Bergen kommune på områdene informasjonssikkerhet og personvern er i tråd med ISO/IEC-standard 27001:13.

Begrepet «blandet læring» skal operasjonaliseres og ligge som en forutsetning for det videre arbeidet med kompetanse- og kunnskapsutvikling på områdene informasjonssikkerhet og personvern.

Bergen kommune skal på sikt jobbe for å videreutvikle kvalitetssystemet slik at avvik kan aggregeres på et mer detaljert nivå, som et ledd i en bedre kompetanseutvikling og risikostyring.

Etablere nødvendig kapasitet mht. ressurser i organisasjonen for felles opplæring og kompetanseheving innen personvern og informasjonssikkerhet

9 Oppfølging av planen og økonomiske konsekvenser

Bilde: Pexels.com

9. Oppfølging av planen og økonomiske konsekvenser

Bergen kommune er en stor virksomhet, med mange ulike tjenesteområder, faglige tilnærminger og arbeidssteder. Å iverksette konserngjennomgående planer som både dekker konsernfunksjons behov sammen med byrådsavdelingen byr alltid på utfordringer i en så kompleks organisasjon. Dersom kommunen skal lykkes med å realisere målene, visjonene og ambisjonene byrådet har lansert i denne temaplanen, må kommunen ha kontinuerlig oppmerksomhet på informasjonssikkerhet og personvern og tiltakene foreslått i denne planen.

Organisasjonen må ha kapasitet i byrådsavdelingene og sentralt hos konsern til å se kommunens digitaliseringsstrategi, denne temaplanen og kommunens helhetlige gjennomgang av informasjonssikkerhet og personvern i sammenheng med hverandre. Verdi kan bare skapes når et prosjektets leveranser tas i bruk av organisasjonen.[49] Slik vil det også være med satsingsområdene og tiltakene i denne planen. Planen inneholder en del forslag som vil kreve økte budsjettrammer. Slike forslag forutsetter budsjettmessig prioritering og finansiering, og vil vurderes i forbindelse med årlige fremlegg av handlings- og økonomiplan/budsjett.

[49] Prosjekthåndboken s. 43.

10 Sammendrag

Bilde: Unsplash.com

10. Sammendrag

Denne planen er først og fremst en tematisk plan som skal sikre strategisk utvikling av fagområdene personvern og informasjonssikkerhet i organisasjonen. De tiltak og initiativer som fremmes i denne temaplanen gjøres hovedsakelig på bakgrunn av behovet for strategisk utvikling av fagene i kommunen. Flere av forslagene til tiltak i planen, bygger imidlertid på kartlegginger, funn og vurderinger gjort i kommunens helhetlige gjennomgang av informasjonssikkerhet og personvern. De gjøres også på bakgrunn av de risikoer og vurderinger som er blitt beskrevet gjennom forvaltningsrevisors vurderinger i 2019 på informasjonssikkerhet. Samtidig er det viktig å understreke at planen i seg selv ikke alene skal fremme sikkerhetstiltak – det skal kommunen gjøre gjennom sin ordinære drift og den risikovurdering som utarbeides for kommunen som konsern, byrådsavdeling og enkelte løsning.

For kommunens arbeid med plikter som å føre protokoll, risikovurderinger, databehandleravtaler og personvernkonsekvensvurderinger er det dokumentert mangler og sårbarheter i den helhetlige gjennomgangen. Disse knytter seg blant annet til at;

- Kommunen har ikke fullstendig oversikt over de behandlinger av personopplysninger i kommunen. Årsaken til dette er at kommunen har ulike behandlingsprotokoller og en ulik praksis gjennom bruk av forskjellige maler og verktøy. Manglende oversikt medfører at kommunen har svak kontroll med de personopplysninger som behandles, til hvilke formål og hvem som er involvert, herunder bruk av databehandlere. Det kan også føre til at kommunen potensielt behandler personopplysninger uten lovlig grunnlag.
- Kommunen har ikke en helhetlig og god oversikt over risiko forbundet med behandling av personopplysninger og bruk av teknologi. Årsaken til dette er ulik praksis og tilnærming til risikovurderinger og personvernkonsekvensvurderinger. Manglende helhetlig oversikt over risikobildet medfører at det er vanskelig å prioritere og iverksette effektive og egnede tiltak for å redusere risiko. Dette medfører svak risikostyring og økt sannsynlighet for uønskede hendelser og lovbrudd.

Dersom kommunen ikke utvikler en helhetlig og standardisert tilnærming til prosessene nevnt over, er ikke virksomheten kjent med hvilken risiko som foreligger for den enkelte behandling av personopplysninger. Mangelfulle risikovurderinger som forvaltningsrevisjonen i 2019 avdekket og helhetlig gjennomgang også har pekt på, medfører i tillegg at kommunen har en svekket kapasitet til å iverksette egnede sikkerhetstiltak. Forutsetningen for å iverksette egnede organisatoriske og/eller tekniske sikkerhetstiltak er systematisk risikostyring for hele virksomheten, men i særdeleshet grundige risikovurderinger som belyser nødvendige aspekter ved den enkelte løsning eller behandling.

Varierende etterlevelse av krav som stilles i styrende dokumentasjon og i lov- og regelverk medfører også en forhøyet risiko for den registrerte og kommunens informasjonshåndtering. Planen foreslår derfor flere utredninger med sikte på å etablere nødvendig kapasitet og kompetanse i organisasjonen. Planen foreslår blant annet at kommunen skal utrede behovet for et sentralt ressursmiljø for oppgaver (tjenester) som risikovurderinger, personvernkonsekvensvurderinger, databehandleravtaler, protokollføring og mer. Utredningen skal gi mer informasjon om konkret organisering, kostnader og behovet for kapasitet med sikte på å etablere et slikt miljø. Et samlet ressursmiljø for utvalgte oppgaver (tjenester) vil kunne

skape et større fagmiljø som er mer attraktivt og kan tiltrekke seg kompetanse det er mangel på i kommunen, men også i markedet. Med en standardisert tilnærming til sentrale personvernoppgaver på tvers av kommunens enheter, kan dette være med på å bidra til at kommunens evne til å etterleve lovkrav, retningslinjer og prosedyrer økes betraktelig.

Planen peker på behovet for at kommunen på sikt etablerer et sentralt miljø for testing og utvikling av testmetodikk. For å avklare organisatoriske behov er det nødvendig å gjennomføre en tilsvarende utredning for å redegjør for kostnader, omfang og organisering. For å senke risikoen for brudd på personvernet eller informasjonssikkerheten, er en metodisk tilnærming til testing av sikkerhetstiltakenes effekt i løsninger og utvikling av testmetodikk nødvendig. De to foreslåtte miljøene er tenkt å samarbeide nært med kommunens planlagte SOC (Security Operation Centre) som primært skal bistå i hendelseshåndtering.[50] Samtidig er det i sammenheng disse tre miljøene vil bidra til å svare ut et vesentlig behov – den systematiske tilnærmingen som er nødvendig for god risikostyring på fagområdene. I sum skal disse miljøene løfte kommunens kapasitet til å forebygge brudd på personvernet og informasjonssikkerheten vesentlig.

Planen peker også på nødvendigheten av at Bergen kommune jobber sammen med andre storbyer og kommuner. Det kommer frem av satsingsområdet at kommunen i strategiperioden skal videreutvikle dagens regionale samarbeid i DigiVestland og det som gjøres nasjonalt i KS. Kommunen skal bruke de eksisterende arenaene for samhandling på fagområdene som finnes, og gjennom det legge til rette for at egen og andres kunnskap kan videreutvikles. Særlig innen anskaffelser. Bergen kommune skal ta initiativ til fagdialog på områdene informasjonssikkerhet og personvern mellom storbyene på eksisterende arenaer.

Et stadig mer digitalisert samfunn medfører også et stadig økende behov for kompetanseheving innenfor informasjonssikkerhet og personvern. Forvaltningsrevisjonen dokumenterte i 2019 at en relativt stor andel av kommunens resultatsenhetsledere bare delvis oppgis å ha sørget for nødvendig opplæring for sine ansatte knyttet til informasjonssikkerhet. Forvaltningsrevisor fant også at ikke alle ansatte i kommunen har tilstrekkelig kjennskap til retningslinjer og rutiner for informasjonssikkerhet, samt at informasjonssikkerhetspraksisen hos enkelte ansatte brøt med flere sentrale prinsipper for informasjonssikkerhet. Planen vektlegger derfor at Bergen kommune skal jobbe langs flere akser i sitt arbeid med kompetanse, sikkerhets- og personvernkultur i organisasjonen, og ha en variert pakke med virkemidler og verktøy i dette arbeidet.

[50] En SOC (Security Operation Centre) er i hovedsak et reaktivt tiltak, men i samarbeid med det planlagte miljøet for testing og utvikling av testmetodikk og det sentrale ressursmiljøet for utvalgte oppgaver, skal operasjonssenteret også utføre inntrengningstester av prioriterte løsninger.

Kommunen skal derfor ta i bruk teknologistøttet læring og mer tradisjonelle kursopplegg som på sikt vil utgjøre kompetansepakker den ansatte kan bruke det til selvstudium eller «på jobben-trening». Gruppediskusjoner, veiledning og kollegastøtte er viktige virkemidler for å utnytte potensiale som ligger i denne typen metodikk. Samtidig som ny metodikk skal tas i bruk, skal kommunen på sikt bygge kapasitet til å utvikle og videreutvikle felles opplæring og kompetanseheving innen fagområdene for hele kommunen. Dette er sentrale momenter for å bygge kultur over tid. For å bygge kompetanse og en personvern- og sikkerhetskultur er det nødvendig at kommunen tar i bruk «blandet læring», der man kombinerer digitale støtteverktøy for læring med mer tradisjonelle metoder over tid. Temaplanen fremhever viktigheten av at kommunen har en systematisk innfallsvinkel til individuell og kollektiv kompetanseheving og kulturbygging i organisasjonen for de ansatte. For organisasjonen og de ansatte innebærer dette en praksisendring i hvordan kommunen systematisk følger opp ansatt-, leder- og avdelingsnivå på fagområdene informasjonssikkerhet og personvern. Informasjonssikkerhet og personvern vil, ut fra den enkelte ansattes rolle og behov for kompetanse, bli en sentral del av den årlige medarbeidersamtalen.

Bilde: Pexels.com

11 Tiltak

Bilde: Unsplash.com

11. Tiltak

Tiltak	Forslag til tiltak	Kostnad mill kr	Engangskostnad eller varig	Handlings- og økonomiplan
	Tiltak rettet mot å støtte opp under det strategiske satsingsområdet (1) innebygd personvern, infrastruktur og systemer som tåler det uforutsette og (2) infrastruktur og forvaltning av fagsystem.			
1	Opprette SOC (Security Operation Centre) med døgnbemanning. Basert på tidlige vurderinger ser vi for oss at det er behov for omkring 6 årsverk. 7,0 mnok er satt av til nye stillinger. 1,0 mnok er satt av til verktøy og lisenser. Ansvar for gjennomføring: *Seksjon for digitalisering og innovasjon (SDI) og Enhet for digitale driftstjenester (EDD).*	8,0	Lønnskostnader inkludert sosiale kostnader og driftsmidler knyttet til ansatte e.g. lisenser og annet.	Utenfor eksisterende ramme.
2	Utrede behovet for å etablere et sentralt miljø for testing og utvikling av testmetodikk. Utredningen skal gjøre rede for organisering, kostnader og videre innretting med sikte på å etablere et slikt miljø i strategiperioden. Basert på tidlige vurderinger ser vi for oss at det er behov for omkring 10 årsverk inkludert et egnet driftsmiljø med tilhørende kostnader knyttet til service og driftsavtaler. Utredningen vil beskrive kostnadsbildet nærmere. Ansvar for gjennomføring: *Seksjon for digitalisering og innovasjon (SDI).*	1,0 12,0	engangstiltak Lønnskostnader inkludert sosiale kostnader og driftsmidler knyttet til ansatte e.g. lisenser og annet.	Utenfor eksisterende ramme.
3a)	Utrede hvordan Bergen kommune enklere og mer effektivt kan oppfylle retten til innsyn på tvers av kommunens fagsystemer (i overkant av 350 systemer som behandler personopplysninger) og løsninger. Utredningen skal avklare hvilke fagsystemer som bør integreres med «Min Side» (portal). Arbeidet skal også redegjøre for kostnader, ansvarsfordeling mellom byrådsavdelingene og videre innretting med sikte på å etablere den nye funksjonaliteten i Min Side i strategiperioden.	1,0	Engangstiltak	Utenfor eksisterende ramme.

3b)	På bakgrunn av konseptutredningen vil prosjektet bli meldt inn til den årlige vurderingen av handlings- og økonomiplanen. **Ansvar for gjennomføring**: *Seksjon for digitalisering og innovasjon.*	20,0 0,5	Foreløpig estimat som knytter seg til innleie av ekstern kompetanse, utvikling, integrasjoner, testing og produksjon. Varige driftskostnader i service- og driftsavtaler	
4	Utarbeide en oversikt over tiltak for tilstrekkelig sikring av kommunalt endepunktsutstyr **Ansvar for gjennomføring**: *Enhet for digitale driftstjenester og Seksjon for digitalisering og innovasjon.*	-	-	Innenfor eksisterende ramme.
6	To-faktorautentisering skal være standard verifiseringsmetode for alle løsninger Bergen kommune bruker, der det er teknisk og praktisk gjennomførbart, og nødvendig for å sikre behandling av personopplysninger og ivareta informasjonens sikkerhet. Med utgangspunkt i dette skal kommunen også etterstrebe en mest mulig brukervennlig løsning. **Ansvar for gjennomføring**: *Ansvarlig byrådsavdeling i samarbeid med Seksjon for digitalisering og innovasjon og Enhet for digitale driftstjenester.*	-	-	Innenfor eksisterende ramme.
7	Sette ned et sentralt styrt prosjekt som i fase 1, skal utrede hvilke systemer som skal etableres i kommunens nye datasenter. Som en del av fase 1 skal prosjektet avklare ambisjonsnivå for hvor raskt det enkelte system kan gjenopprettes. I fase 2 skal prosjektet i samarbeid med leverandører starte arbeidet med å planlegge og forberede oppstart av redundant drift for de prioriterte systemene. **Ansvar for gjennomføring:** Enhet for digitale driftstjenester og Seksjon for digitalisering og innovasjon.	2,0	Engangstiltak	Utenfor eksisterende ramme.

	Tiltak rettet mot å støtte opp under det strategiske satsingsområdet (3) tilrettelegging og etterlevelse.			
8	Utrede behovet for å bygge opp et sentralt ressursmiljø for utføring og fasilitering av oppgaver (tjenester) som risikovurderinger, personvernskonsekvensvurderinger, inngåelse av databehandleravtaler og protokollføring. Utredningen skal gjøre rede for organisering, kostnader og videre innretting med sikte på å etablere et slikt kompetansemiljø i løpet av strategiperioden. Basert på tidlige vurderinger ser vi for oss at det er behov for omkring 10 årsverk. **Ansvar for gjennomføring**: *Seksjon for digitalisering og innovasjon.*	1,0 10,0	Engangstiltak Lønns- inkludert sosiale kostnader og driftsmidler knyttet til ansatte e.g. lisenser og annet.	Utenfor eksisterende ramme.
9	Utrede fordeler og ulemper ved bruk av ISO-standard 27001 sammenliknet med vedtatt rammeverk for risikostyring på konsernnivå knyttet til informasjonssikkerhet. **Ansvar for gjennomføring**: *Seksjon for digitalisering og innovasjon.*	-	-	Innenfor eksisterende ramme.
10	Revidere informasjonssikkerhetsforum sitt mandat og sammensetning på bakgrunn av funn i den helhetlige gjennomgangen. **Ansvar for gjennomføring**: *Seksjon for digitalisering og innovasjon.*	-	-	Innenfor eksisterende ramme.
11	Utrede behovet for en funksjon i kommunen etter inspirasjon fra «regionale komiteer for medisinsk og helsefaglig forskningsetikk». **Ansvar for gjennomføring**: *Seksjon for digitalisering og innovasjon.*	0,38		Innenfor eksisterende ramme.
	Tiltak rettet mot å støtte opp under det strategiske satsingsområdet lokalt, regionalt og nasjonalt samarbeid			
12	Videreutvikle metodikk sammen med kommuner og nasjonale aktører for å forbedre egne anskaffelsesprosesser, kontraktoppfølging, leverandørstyring og revisjon av avtaler i et informasjonssikkerhetsperspektiv.	-	-	Innenfor eksisterende ramme.

	Ansvar for gjennomføring: *Seksjon for digitalisering og innovasjon.*			
13	Kommunen skal på eksisterende arenaer, ta intitiativ til at storbyene etablerer en mer aktiv fagdialog på områdene informasjonssikkerhet og personvern. **Ansvar for gjennomføring**: *Seksjon for digitalisering og innovasjon.*	-	-	Innenfor eksisterende ramme.
	Tiltak rettet mot å støtte opp under det strategiske satsingsområdet kompetanse, sikkerhets- og personvernkultur.			
14	Tilse at kompetansetiltak på området for informasjonssikkerhet og personvern er i tråd med ISO/IEC-standard 27001 **Ansvar for gjennomføring**: *Seksjon for digitalisering og innovasjon.*	-	-	Innenfor eksisterende ramme.
15	Operasjonalisere begrepet blandet læring og bruke tilnærmingen i kompetanse- og kunnskapsarbeidet for områdene informasjonssikkerhet og personvern. **Ansvar for gjennomføring**: *Seksjon for digitalisering og innovasjon i samarbeid med HR-konsern.*	-	-	Innenfor eksisterende ramme.
16	Ta initiativ til å videreutvikle kommunes kvalitetssystem, hvis teknisk mulig, slik at avvik kan aggregeres på et mer detaljert nivå, som et ledd i en bedre kompetanseutvikling og risikostyring. **Ansvar for gjennomføring**: *Seksjon for digitalisering og innovasjon.*	-	-	Innenfor eksisterende ramme.
17	Etablere nødvendig kapasitet mht. ressurser i organisasjonen for felles opplæring og kompetanseheving innen personvern og informasjonssikkerhet. Arbeidet skal legges tettest mulig opp mot eksisterende strukturer for kompetanse, kurs og opplæring. Basert på tidlige vurderinger ser vi for oss at det er behov for omkring 4 årsverk. **Ansvar for gjennomføring**: *Seksjon for digitalisering og innovasjon.*	4,0	Lønns- inkludert sosiale kostnader og driftsmidler knyttet til ansatte e.g. lisenser og annet.	Utenfor eksisterende ramme.