# Datatilsynets regulatoriske sandkasse
# Søknadskjema del 2

**Dette er del to av søknadsskjemaet der vi ber om mer informasjon om tematikken dere ønsker adressert i sandkassen, gjerne med utgangspunkt i dialogmøtet.**

**Hvis søknad del 1 adresserte generelle problemstillinger, forsøk å konkretisere disse (2.5).**
**Hvis søknad del 1 adresserte mange problemstillinger, forsøk å prioritere disse (2.7).**

**Hvis spørsmål ansees besvart i søknad del 1, vis til hvor. Vi ber om at dere fyller ut dette skjemaet og sender til sandkasse@datatilsynet.no innen utgangen av 4. desember 2023.**

## Om virksomheten

| | |
|---|---|
| **2.1 Forankring i ledelsen**<br>*Hvordan er søknad om deltakelse i sandkassen forankret i ledelsen, også relatert til ressursbruk? Vis gjerne til leder/lederfunksjon prosjektet er forankret hos.* | Prosjektet er forankret hos IT-direktøren 04.12.2023. Direktør for organisasjon og infrastruktur er orientert om prosjektet.<br><br>Personellressurser til gjennomføring av prosjektet vil gjøres tilgjengelig primært fra Seksjon for Digital sikkerhet og Seksjon for IT-strategi og -styring |
| **2.2 Relasjon til Datatilsynet**<br>*Har virksomheten tidligere vært i kontakt med Datatilsynet – enten gjennom tilsyn, sak eller veiledning? Hvis ja, vennligst gi en kort* | NTNU har ved flere anledninger vært i kontakt med Datatilsynet i forbindelse med saker og avvik.<br><br>IT-avdelingen har også ved en tidligere anledning deltatt i veiledningsmøte sammen med vår tjenesteleverandør Sikt (25.08.22 forhåndsdrøftelse med Datatilsynet vedrørende en innovativ anskaffelse: «Levere løsning for innsamling og behandling av fortrolig lyd og video» gjennom NTNUs |

| | |
|---|---|
| *beskrivelse. Det understrekes at dette ikke diskvalifiserende, formålet med spørsmålet er å få oversikt over eventuell kontekst rundt sandkasseprosjektets initiativtager.* | forskningsdataprosjekt. Datatilsynets arkivreferanse: 22/03970). Dette møtet ble fra NTNUs side oppfattet som et nyttig og positivt tilbud, og resultatet fra veiledningen ble lagt til grunn i anskaffelsen. |
| **2.3 Personvern i virksomheten**<br>*Vennligst gi en kort beskrivelse av nåværende personverntiltak i virksomheten (har virksomheten personvernombud, har virksomheten styringssystemer/prosedyrer på plass for å ivareta personvernet, er virksomheten liten/ny og har begrenset erfaring med personvern)?* | NTNU jobber systematisk for å ivareta personvernet til de registrerte ved virksomheten. Organisasjonen har etablerte retningslinjer for blant annet behandling av personopplysninger, lagring, personopplysninger i forskningsprosjekter, personvern i undervisning mv. NTNU har også etablert styringssystem for informasjonssikkerhet og et IKT-reglement som oppdateres jevnlig. Alle styrende dokumenter ligger tilgjengelig på https://i.ntnu.no/informasjonssikkerhet, og siste totale revisjon av styringssystemet ble gjennomført 12.06.2023.<br><br>Virksomheten har flere pågående personverntiltak, blant annet:<br>- Personvernklyngen i Fellesadministrasjonen<br>  o Tverrfaglig klynge/nettverk i Fellesadministrasjonen.<br>  o Etablert med hensikt å koordinere et stort ansvarsområde og å samkjøre aktiviteter innenfor området.<br>  o Behandler saker fra ansatte og jobber for å øke kompetansenivået i organisasjonen, blant annet gjennom å tilby e-opplæringskurs i behandling av personopplysninger til alle ansatte (kurset er også tilgjengelig for studentene).<br>- Research Data (Forskningsdatahjelpen)<br>  o En felles støttetjeneste innen forskningsdata ved NTNU for forskere og studenter.<br>  o Bidrar med rådgivning innenfor blant annet personvern i forskning.<br>- Nettverk for personvern i forskning<br>  o Nettverk for administrativt ansatte med ansvar og/eller interesse for behandling av personopplysninger i forskning.<br>  o Bidrar til erfaringsdeling og kompetanseheving.<br>- KI-klyngen<br>  o Tverrfaglig klynge/nettverk for ansatte i organisasjonen med fokus på kunstig intelligens. Behandler undertemaer innenfor personvern og informasjonssikkerhet og kunstig intelligens. |

| | |
|---|---|
| | ○ Har utarbeidet retningslinjer for ansvarlig bruk av (generativ) kunstig intelligens ved NTNU som i skrivende stund er på høring i organisasjonen.<br><br>NTNU har etablert rollen som personvernombud (Thomas Helgesen). Personvernombudet har en fri og uavhengig posisjon i virksomheten, og rapporterer årlig til NTNUs styre. |
| **2.4 Annen relevant informasjon og egenvurdering av modenhet**<br>*Er det annen informasjon om virksomheten som kan være relevant for Datatilsynet å vite om i forbindelse med deltakelse i sandkassen?*<br>*Dette kan eventuelt inkludere noe mer detaljerte beskrivelser enn søknad av relasjoner/avhengigheter/forpliktelser til partnere for det spesifikke prosjektet, også internasjonale.*<br>*Gi også en kort egenvurdering av antatt modenhet knyttet til problemstillinger som ønskes adressert.* | NTNU har flere ulike miljøer som jobber systematisk med personvern i virksomheten. Tidligere nevnte personverntiltak bidrar til økt fokus på personvern blant ansatte. Modenheten blant de prosjektdeltakerne vil være høy.<br><br>Det må likevel anses at virksomheten i sin helhet har lav modenhet knyttet til de spørsmålene som reises i dette prosjektet, og kanskje særlig knyttet til trygg bruk av særlig generativ kunstig intelligens. Dette har vært en viktig motivator for å sende denne søknaden for å øke oppmerksomheten på et viktig felt som endrer seg fra dag til dag. NTNU ønsker å gjennomføre prosjektet for å forberede virksomheten på utviklingen som skjer innenfor kunstig intelligens og personvern. I prosjektet spesifiserer vi tjenesten som vi ønsker å undersøke, Microsoft 365 Copilot, men arbeidet vil like gjerne kunne forberede organisasjonen på andre verktøy og tjenester som enda ikke er utviklet. Temaet («Verktøy med kunstig intelligens ved NTNU») har blant annet vært oppe til behandling i vårt sentrale samarbeidsutvalg med fagforeningene (SESAM, dato 06.11.2023), og Studenttingets formøte med alle fakultetstillitsvalgte 27.11.2023). Begge instanser understreket viktigheten av at utviklingen innenfor dette feltet må foregå innenfor trygge rammer. |

| Om prosjektet | |
|---|---|
| **2.5 Beskrivelse av prosjektet**<br>*Hvis det er hensiktsmessig å gi mer utfyllende informasjon om sandkasseprosjektet i tillegg til det som framkom i søknad 1, kan det fylles inn her.*<br><br>*Eventuelt mer utfyllende og konkret informasjon om type plattform/løsninger/ metoder tenkt brukt for å realisere løsningen kan eventuelt tas med.*<br><br>*Beskriv eventuelle potensielle samarbeidspartnere som kan være aktuelle å involvere i sandkasseprosjektet.*<br><br>*Beskriv om det er mulig å konkretisere sandkasseprosjektet gjennom bruk av konkrete use-cases.* | NTNU ønsker å gjennomføre et pilotprosjekt for å teste om Microsofts kunstige intelligente assistent «Microsoft 365 Copilot» (https://adoption.microsoft.com/en-us/copilot/ - heretter omtalt som "Copilot") kan bli tatt i bruk i en stor organisasjon i offentlig sektor.<br><br>NTNU ønsker at sandkasseprosjektet skal resultere i tre konkrete delmål:<br>1. Utarbeide en verktøykasse for at organisasjoner i offentlig sektor kan bli «Copilot-ready»<br>2. Utvikle informasjonsmateriell om hvordan organisasjoner i offentlig sektor kan påvirke leverandører til å tenke operasjonelt personvern tidlig i utvikling av nye tjenester hvor kunstig intelligens benyttes<br>3. Arrangere et åpent fagseminar om temaet for alle i offentlig sektor juni 2024.<br><br>**1. Utarbeide en verktøykasse for å bli «Copilot ready»**<br>Hovedformålet med prosjektet er å utarbeide en verktøykasse som kan gjøre det enklere å vurdere om verktøy som Copilot er verktøy som kan innføres ved NTNU. NTNU vil måtte foreta en rekke vurderinger knyttet til robusthet i egen virksomhet, Orden i eget hus (dataforvaltning) og bruksområder som kan være nyttig for andre organisasjoner i offentlig sektor å lære av.<br><br>NTNU ønsker å utarbeide en verktøykasse bestående av vurderinger, beskrivelser av rammeverk, retningslinjer og utkast til personvernkonsekvensvurderinger som andre kan ta i bruk. Verktøykassa skal bestå av materiell for å hjelpe til med vurderinger av hvorvidt en organisasjon kan anskaffe og ta i bruk et verktøy som Microsoft 365 Copilot (eller tilsvarende). Verktøykassen som utarbeides vil tilgjengeliggjøres og deles med andre offentlige og private virksomheter.<br><br>Vurderinger av lovlighet, etikk og sikker bruk av en «digital assistent / Copilot» basert på kunstig intelligens og virksomhetens egne tilgjengeliggjorte data er hovedspørsmålet som skal behandles i prosjektet.<br><br>Om verktøy som Copilot kan brukes i offentlig sektor vil dette ha et stort innovasjonspotensial. Effektiviseringspotensial i driftsoppgaver, bedre kvalitet i saksbehandling og nye måter å fremstille informasjon og kunnskapsgrunnlag bør vurderes. Dette vil igjen kunne gi besparelser i både tid og kostnader. |

| | |
|---|---|
| | **2. Utvikle informasjonsmateriell om hvordan organisasjoner i offentlig sektor kan påvirke leverandører til å tenke operasjonelt personvern tidlig i utvikling av nye tjenester hvor kunstig intelligens benyttes**<br>NTNU ønsker å øke oppmerksomheten på viktigheten av å tenke innebygd personvern i prosessen når IKT-verktøy skal anskaffes. I dag er det ofte leverandørene som styrer utviklingen, og NTNU og andre offentlige instanser må leve med de vilkår og premisser leverandørene setter i utviklingen av sine verktøy. Å følge opp for eksempel «dynamiske kontrakter» med store internasjonale skyleverandører, kan være utfordrende både for små og store organisasjoner. Praksisen med for eksempel «opt out»-løsninger (bruker må aktivt følge med på og selv skru av funksjonalitet som øker personvernulempe) bør utfordres tidlig i anskaffelsesprosessen.<br><br>NTNU (som mange andre organisasjoner) har en avtale med Microsoft, men opplever at den reelle påvirkningskraften ligger i anskaffelsesprosessen. Det er da man kan stille krav til at nye IT-systemer skal støtte operasjonelt personvern, og ikke at personvernvurderingene først gjøres mot slutten av anskaffelsen. For å hjelpe til med hvordan en organisasjon bør tenke ønsker NTNU å utarbeide generelle krav som kan stilles i en anskaffelsesprosess slik at operasjonelt personvern faktisk blir operasjonelt.<br><br>En viktig del av dette delprosjektet blir også å gjenbruke allerede etablerte samarbeidsarenaer. NTNU har i dag en tett og god samarbeidsrelasjon med Microsoft, og denne arenaen kan danne et utgangspunkt for en bredere samarbeidsarena. NTNU antar at leverandører generelt, ikke bare Microsoft, er interessert i å være med på å skape en felles forståelse for hva som er viktig for offentlige virksomheter å ha på plass i anskaffelser av verktøy basert på kunstig intelligens, da dette stimulerer til økt konkurranseevne i markedet.<br><br>**3. Arrangere et åpent fagseminar om temaet for alle i offentlig sektor i juni 2024.**<br>NTNU har «Kunnskap for en bedre verden» som sin overordnede visjon. Denne visjonen gjelder ikke bare for vår vitenskapelige aktivitet – formidling er viktig for alle våre virksomhetsområder. Erfaringer fra dette prosjektet vil kunne benyttes av andre, og NTNU ønsker derfor å arrangere et åpent fagseminar om temaet og vise fram prosjektresultater mot slutten av prosjektperioden.<br><br>NTNU ønsker å legge til rette for erfaringsutveksling og deling på tvers i offentlig sektor, og dette gjelder særlig innenfor områder som for eksempel personvern. Å avslutte prosjektperioden med et fagseminar som legger til |

| | |
|---|---|
| | rette for erfaringsutveksling, tverrfaglig samarbeid og et vitenskapelig tilsnitt tror vi vil gi en god «punch-out» i sandkasseprosjektet. |
| **2.6 Prosjektfaser**<br>*Gi en beskrivelse av hvilke aktiviteter hovedprosjektet eventuelt allerede har gjennomført og hvilke planer hovedprosjektet har fremover. Dette gjelder prosjektet generelt, og personvernaktiviteter spesielt.*<br><br>*Oppgi i så stor grad som mulig forventet tidsløp for fasene i sandkasseprosjektet. Har hovedprosjektet konkrete planer for eventuell produksjonssetting?* | NTNU er allerede i gang med å forberede prosjektet. Forarbeidet inngår i allerede pågående personvernaktiviteter koordinert av Personvernklyngen i Fellesadministrasjonen.<br><br>- Aktiviteter høst 2023:<br>  o Forberede Copilot. Bing Chat Enterprise (bytter nå navn til Microsoft Copilot) er skrudd på i trygge og kontrollerte former som en sandkasse (testarena) for våre ansatte. Opplæring gis og retningslinjer for ansvarlig bruk av (generativ) kunstig intelligens ved NTNU er på høring i organisasjonen (frist 22. januar 2024). NTNU følger med på utviklingen av kunstig intelligens og IT-avdelingen etablerer to ressursgrupper for å jobbe med utvikling av kunstig intelligens («KI-klynga» og «AI Tech Lab»)<br>- Første halvår 2024:<br>  o Pilotere og forberede organisasjonen på å kunne tilby Copilot som tjeneste for deler av virksomheten.<br>  o Gjøre alle nødvendige tekniske, juridiske og etiske vurderinger<br>  o Forberede finansieringsmodell og rammeverk for FDVu (forvaltning, drift, vedlikehold og utvikling)<br>  o Forberede datakilder: lokale og sentrale. Sikre riktig klassifisering av data for å sikre at Copilot ikke får tilgang til konfidensielle datakilder.<br>- Andre halvår 2024<br>  o Tilby Copilot som tjeneste ved NTNU<br><br>NTNU kan starte et sandkasseprosjekt først 22. januar 2024. Vi kan dessverre ikke starte tidligere i fordi store deler av prosjektgruppa har hjemmeeksamen i perioden 4-18. januar (NTNU har til sammen 6 deltakere på høstens deltidsstudium i personvern på Høgskolen i Innlandet https://www.inn.no/studier/vare-studier/personvern/) |
| **2.7 Personvernutfordringer / risikovurderinger**<br>*Beskriv hvilke vurderinger som evt. allerede er gjort av lovlighetsvurdering,* | Vurdering av lovlighet, rettslig grunnlag og formål for behandlingen av ovennevnte personopplysninger vil måtte gjøres for hver enkelt behandling. Prosjektet vil omfatte behandlinger som gjenspeiles i NTNUs behandlingsoversikt (NTNU endrer hovedsystem for behandlingsoversikt våren 2024: Visma Draftit skal være |

| | |
|---|---|
| *behandlingsgrunnlag og formål for bruken av personopplysninger i prosjektet.*<br><br>*Hvis virksomheten allerede har gjort en personvernkonsekvensvurdering (DPIA) kan denne vedlegges søknaden.* | ferdig implementert 15. mars 2024). Hver behandling har en vurdert lovlighet i form av personvernforordningens personvernprinsipper, et fastsatt formål og et behandlingsgrunnlag.<br><br>I søknaden del 1 viste vi fram en rekke generelle problemstillinger (punkt 9). NTNU har gjennomgått temaene på nytt, og følgende problemstillinger er de prioriterte problemstillingene som ønskes belyst:<br>- Kan verktøy som Copilot tas i bruk i offentlig sektor? Har vi god nok kontroll på egne data, ref. Orden i eget hus?<br>- Kan vi forklare hvordan Copilot skaper resultater? Klarer vi å sikre at vi kjenner til hele beslutningskjeden fra hvor den henter den data til fram til resultatet den gir? Kan vi unngå at NTNU tar feil avgjørelser (Bias, hallusinering, oppgir feil svar, overbevisende svar osv)?<br>- Hvordan må brukere strukturere og organisere filer og data på egne lagringsområder for å kunne bruke Copilot? Hvordan tenke informasjonssikkerhet og klassifisering? Hvilke opplæringstiltak og retningslinjer bør en organisasjon ha?<br>- Er det mulig å sikre krav og forventninger til dataminimering? Får Copilot tilgang til alle data en bruker har lagret?<br>- Kan vi utvikle og dele retningslinjer for riktig bruk av Copilot med andre offentlige virksomheter?<br><br>Vedlagt ligger personvernkonsekvensvurdering for Bing Chat Enterprise (pr 21.09.2023). Bing Chat Enterprise er kun en samtalerobot, men mange av beskrivelsene og utfordringene er gjeldende også for annen bruk av kunstig intelligens. Bing Chat Enterprise bytter nå navn til Microsoft Copilot, og NTNU vil starte arbeidet med å oppdatere dokumentet på nyåret. |
| **2.8 Annet regelverk?**<br>*Er det andre regelverk som kan være relevante for prosjektet? Ingen omfattende gjennomgang, men kort beskrivelse av antatte tilgrensende regelverk som er relevant for prosjektet.* | - Likestillings- og diskrimineringsloven<br>  - Verktøy basert på kunstig intelligens kan diskriminere basert på skjevhet i datasett, trent på ulike data. Eksempel: Kan Teams behandle menn og kvinner ulikt hvis en Copilot-assistent skal oppsummere hva og hvordan møtedeltakere responderte i et møte?<br>- Arbeidsmiljøloven<br>  - § 9-1 i arbeidsmiljøloven omhandler kontrolltiltak på arbeidsplassen. Det kan tenkes at en assistent som Copilot kan bidra til at kontrolltiltak som overvåkning lettere kan brukes mot ansatte.<br>- Forvaltningsloven og Offentleglova<br>  - NTNU som offentlig aktør skal opptre redelig og forutsigbart i alle saksbehandlingsprosesser. |

| | |
|---|---|
| | NTNU forbereder seg også på nye regelverk fra EU/EØS som Digitaliseringsdirektoratet ber offentlig sektor forberede seg på (https://www.digdir.no/datadeling/oversikt-over-eu-regelverk-om-deling-og-bruk-av-data/3251). Særlig relevante regelverk for dette prosjektet:<br>- *KI-forordningen*<br>- *Dataforvaltningsforordningen*<br>- *Åpne data-direktivet* |
| | |

| Plan for sandkassen | |
|---|---|
| **2.9 Utkast til overordnet prosjektplan i sandkassen** | NTNU har utarbeidet en overordnet grovskisse til prosjektplan:<br><br>1. Oppstart prosjekt (tidligst) 22. januar – 31. januar<br>a. Sette prosjektgruppe: påmønstring prosjektdeltakere, informere og forankre arbeidet i Fellesadministrasjonen. Orientering på ledermøte Direktør for Organisasjon og infrastruktur.<br>b. Utarbeide mandat og revidere prosjektplan. Opprette samhandlingsrom, og avklare arbeidsform.<br>2. Oppstartsmøte med Datatilsynet (primo februar)<br>a. Spikre prosjektplan og bygge innhold i arbeidspakker: Spikre delprosjektledere, prosjektdeltakere og scope.<br><br>**3. Arbeidspakke 1 – Verktøykasse «Copilot Ready»**<br>a. Oppstart arbeidspakke 1 (medio februar)<br>b. Workshop med NTNUs IKT-leverandører som har «tidlig-tilgang» til Copilot: «Hva anbefaler leverandørene at vi gjør?»<br>c. Arrangere workshops med NTNUs tekniske fagmiljø, digital sikkerhet og arkitektmiljø: «Hva anbefaler IT-miljøet selv at vi gjør?»<br>d. Test av lisenser og bruk med utvalgte brukergrupper (hvis lisenser blir gjort tilgjengelig)<br>e. Sammenstille funn frist 20. april: Har vi tenkt rett?<br>i. Workshop med Datatilsynet<br>ii. Overlevere foreløpige resultater til Datatilsynet |

| | |
|---|---|
| | iii. Motta tilbakemeldinger fra Datatilsynet ca 10 mai.<br>f. Ferdigstille verktøykasse og rapport til 1. juni<br><br>**4. Arbeidspakke 2 – Hvordan skal det offentlige påvirke KI-leverandører**<br>a. Oppstart arbeidspakke 2 (medio februar)<br>b. Arrangere workshops med NTNUs administrative fagmiljø, digital sikkerhet, økonomi, juridiske, tekniske og arkitektmiljø: «Hva bør vi tenke på»<br>c. Test av forslag mot utvalgte NTNU-leverandører<br>d. Sammenstille funn frist 20. april: Har vi tenkt rett?<br>i. Workshop med Datatilsynet<br>ii. Overlevere foreløpige resultater til Datatilsynet<br>iii. Motta tilbakemeldinger fra Datatilsynet ca 10 mai.<br>e. Ferdigstille verktøykasse og rapport til 1. juni<br><br>**5. Arbeidspakke 3 – Fagseminar**<br>a. Oppstart Arbeidspakke (primo mars)<br>i. Finne dato rundt «10. juni», må ikke kræsje med eksamen.<br>ii. Bestille konferansepakke fra NTNU Videre, avtale lokasjon og teknisk rigg. Fortrinnsvis NTNU-internt (For eksempel Realfagbygget R1).<br>b. Lage kommunikasjonsplan og -pakke. Sende ut invitasjoner og hekte informasjon om arrangementet på andre arenaer.<br>c. Gjennomføre fagseminar<br><br>6. Avslutte sandkasseprosjekt:<br>a. Skrive sluttrapport, evaluering og anbefaling til videre arbeid innen 30. juni. |
| **2.10 Rammen rundt prosjektets deltakelse i sandkassen**<br>*Skriv litt om hvilke rammer det er rundt sandkassedeltakelsen til prosjektet. Prosjektets finansiering og hvilke internt ansatte (funksjoner, ikke navn) som* | Økonomiske rammer:<br>- Personellressurser til gjennomføring av prosjektet vil gjøres tilgjengelig primært fra Seksjon for Digital sikkerhet og Seksjon for IT-strategi og -styring. I tillegg kommer<br>- Kostnader til leverandørworkshops dekkes av IT-avdelingen<br>- Hvis tilslag på prosjektet vil vi søke om tilskudd fra IT-avdelingen og NTNUs Digitaliseringsprogram til å arrangere det planlagte fagseminaret i mai/juni 2024. NTNU kan selv stille med egne lokaler |

| | |
|---|---|
| *antas å bidra. Hvis de økonomiske og ressursmessige rammene ikke er på plass, ber vi dere gi et estimat når dette er på plass.* | og utstyr til strømming og opptak for digitale deltakere, så kostnaden anses som beskjeden. Fysiske deltakere må selv dekke utgifter til reise og opphold.<br>- IT-avdelingen har ennå ikke avklart finansiering av eventuelle testlisenser til Microsoft 365 Copilot. Vi er usikre på hvordan lisensmodellen fra Microsoft blir seende ut for akademisk sektor, og når lisenser blir gjort tilgjengelig. Prosjektet er derfor planlagt uten å være avhengig av tilgang på lisenser i prosjektperioden (høy risiko for at lisenser ikke kommer på plass)<br><br>Deltakere i prosjektgruppen:<br>- Rådgivere ved IT-avdelingen ved seksjonene Digital Sikkerhet og IT-strategi og -styring<br>- Jurister ved Avdeling for virksomhetsstyring og Avdeling for utdanningskvalitet<br>- NTNU Fellesadministrasjonens Personvernklynge<br>- Personvernombudet |