Sikker brug af følsomme data

A. INDLEDENDE OPLYSNINGER	
Aktivitetsområde	Indsatsområdet Digital sikkerhed, tillid og dataetik
Institut	Alexandra Instituttet
Titel *Dækker indholdet af aktiviteterne*	Sikker brug af følsomme data
Nummerering *Af beskrivelsen*	1
Version	1
Periode *Forventet start og slut*	1/1 2022 - 31/12 2022
Kontaktperson	Kristian Krämer

B. ÆNDRINGER
Angiv her, hvis en planlagt aktivitet er ændret i forhold til den forudgående version af beskrivelsen.

C. BESKRIVELSE	
1. Mål *Hvorfor?* Hvad er målet for aktiviteterne? Hvordan bidrager de til det overordnede mål for aktivitetsområdet?	Målet med aktiviteterne er at kortlægge de udfordringer, danske virksomheder har på dataadgangs- og anonymiseringsfronten samt at afprøve teknologier og værktøjer på dem. Baseret på vidensgrundlaget fra første år, vil vi fokusere på at udvikle ydelser om anonymisering, privacy-bevarende dataanalyse, samtykker og dataetik. Udviklingen vil være casedrevet, og vil ske i samarbejde med vidensinstitutioner, myndigheder og virksomheder. Aktiviteterne føder ind i den overordnede indsatsbeskrivelses sigte på at indfri det store potentiale for Danmark og danske virksomheder i cybersikker, tillidsværdig digital teknologi. For at indfri det har vi brug for en tværfaglig indsats til at udvikle metoder til at håndtere tillid, ansvarlighed og sikkerhed i brugen af teknologier. Digital ansvarlighed har potentiale til at blive en vigtig konkurrenceparameter for danske virksomheder, så derfor skal denne indsats sikre, at danske virksomheder føler sig overbeviste om og kan dokumentere over for aftagere, brugere, kunder og medarbejdere, at den teknologi, de anvender og udvikler, faktisk er ansvarlig og sikker. Aktiviteterne i denne aktivitetsbeskrivelse understøtter netop datasikkerhedsaspektet i denne problemstilling. Konkret bidrages der til indsatsens overordnede mål-indikatorer med to eller flere caseforløb med virksomheder, videreudvikling af teknologisk services indenfor privacy-bevarende dataanalyse, en ny teknologisk service om samtykker, kompetenceopbygning, etablering af samarbejde med én ny vidanspartner, samt vidanspredning i form af eksempelvis webinarer, indlæg på konferencer, formidlingsrapporter, artikler, indlæg.
2. Indhold *Hvad* skal der ske? Hvilke(n) konkret(e) aktiviteter udføres?	Vi vil arbejde med tekniske løsninger inden for sikkerhed og privacy, som kan åbne for muligheder for sikker adgang, og rådgivningsydelser inden for dette. Essensen af aktiviteten er at afsøge og udvikle metoder til at sørge for sikkerheden når der anvendes og deles data, både så det sker på en sikker og ordentlig måde, men også så data kan udnyttes til videnudvinding og brug i f.eks. udvikling af machine learning-modeller. Dette gælder f.eks. ift. datadrevne modeller, så de ikke uhensigtsmæssig kan lække personlig eller forretningskritisk information. Dette kan enten gøres post-

	hoc ved at se på informationerne, modellen uhensigtsmæssigt bevarer, eller ved at sikre, at data i første omgang forholder sig sikkert til disse forhold. Vi vil i denne aktivitetsperiode også betragte løsninger, hvor *både* algoritmen og data, vil blive holdt hemmelige i forbindelse med analyse af data.
	
	Vi vil igennem denne aktivitetsperiode arbejde problem- og casedrevet med at udvikle løsninger og rådgivningsydelser til understøttelse af dataadgang og anonymisering. Dette vil vi gøre ved at udvælge og afprøve forskellige cybersikkerheds- og privacyteknologier på aktuelle og relevante problemer/cases. I denne aktivitetsperiode vil fokus være på følgende aktiviteter:
	• Anonymisering og syntetiske data. Her vil fokus være på at videreudvikle en eksisterende ydelse gennem cases, så vi kan afdække huller i markedet og et eventuelt behov for andre teknologiske services til privacybeskyttelse.
	• Software til privacy-bevarende dataanalyse, særligt med fokus på:
	  ○ Beskyttelse af algoritmer og IPR. Dette vil ske i tæt samarbejde med aktiviteterne i Standardisering og Kritisk Infrastruktur og CRUCIAL projektet,
	  ○ Real-time optimering ifb. med model predictive control,
	  ○ Statistik og ML.
	• Samtykker og dataetik med fokus på hvordan samtykket passer ind i den tillidsfulde og reelt informerede brugerrejse, samt fokus på hvordan jura og UX passer sammen og potentielt står i vejen for hinanden.
	• Datadonation, med fokus på opsamling af erfaringer fra eksisterende litteratur og tidligere projekter.
	• Samarbejde med Tillidsskabende AI ift. dataetik og privacy-bevarende dataanalyse og anonymisering af ustruktureret data.
	
	Konkret vil vi gennemføre mindst to men gerne flere cases med virksomheder samt undersøge de udfordringer, danske virksomheder oplever i forhold til dataadgang og anonymisering. Arbejdet vil bygge på tværfaglige processer, der undersøger teknologiske, brugermæssige, samfundsmæssige og forretningsmæssige aspekter. På baggrund af dette vil vi udvikle teknologiske services målrettet danske virksomheders behov for at sikre de data, der må bringes i anvendelse for at skabe forretningsmæssig indsigt og værdi.

3. Aktører *Hvem* udfører aktiviteterne? Hvilken afdeling af instituttet? Evt. hvilke eksterne parter er med (videninstitutioner, virksomheder, erhvervsorganisationer, myndigheder, klyngeorganisationer eller andre).	Direkte involverede labs hos Alexandra Instituttet: Security Lab, Human Insights Lab, Artificial Intelligence and Data Analysis Lab, samt det tværgående team Research & Innovation. Eksterne samarbejdspartnere: • Universiteterne: I dette aktivitetsområde vil vi samarbejde med flere af de danske universiteter. Vi har samarbejder i gang med både AU, ITU og AAU, og vil både forsøge at udbygge samarbejdet med disse og indlede nye. • Klynger: Hovedsageligt DigitalLead, men også andre klynger hvor denne aktivitet kan støtte op med teknologiske løsninger.
4. Sammenhæng med andre projekter (evt.) Indgår aktiviteten i andre eksternt finansierede projekter?	Aktiviteterne hænger sammen med, og leverer tekniske løsninger, til indsatsområderne: ”*Accelerering af digital sundhed og velfærd i Danmark*” og ” *Digitale teknologier til data- drevet, bæredygtig vækst*”. Aktiviteterne har generelt sammenhæng med projekterne: AutoAI4CS (Industriens Fond), Health Data Exchange – HedaX (Innovationsfonden) og CRUCIAL (Innovationsfonden). I disse projekter anvendes aktiviteten som egenfinansiering.
5. Følgegruppe Har følgegruppen forholdt sig til aktiviteten? I så fald hvordan? Hvis ikke, hvornår forventes følgegruppen at blive præsenteret for aktiviteten? (Det	I den forgående periode har vi været i løbende dialog med både virksomheder, rådgivere, offentlige organisationer og universiteter gennem indsatsens netværks- og følgegrupper. Her har vi bredt identificeret markedsmæssige udfordringer og problemområder, som i dag ikke bliver dækket af teknologiske services. I den kommende

sidste bør kun gælde under opstarten af indsatsområdet).	aktivitetsperiode vil vi etablere 3 mindre følgegrupper (én for hver aktivitetsbeskrivelse), der vil være mere agile i forhold til den løbende dialog omkring markedssituationen og indsatsområdets aktiviteter. I denne aktivitet etableres en specifik følgegruppe med fokus på sikker brug af følsomme data. Følgegruppen sammensættes af aktører på tværs af private virksomheder, offentlige organisationer og vidensinstitutioner, der kan bidrage positivt ind i samtlige aktiviteter. Konkurrencesituationen vil desuden vendes løbende på møder med følgegruppen, så det sikres at der ikke udvikles komponenter og services der er konkurrenceforvridende. Aktivitetsbeskrivelsen er sendt i ”e-mail/telefonisk høring” i følgegruppen, forinden den er uploadet på Bedreinnovation.dk. Hen over perioden præsenteres følgegruppen for fremdrift på aktiviteten på følgegruppemøderne og i den løbende ad hoc dialog.

6. Formidling af resultater (evt). Hvordan/hvor kan interesserede virksomheder og andre få viden om resultaterne af aktiviteterne? (Anføres/tilføjes hvis det ikke allerede fremgår af beskrivelsen ovenfor, f.eks. ved links til konferencer, hjemmeside, publikationer etc.).	Resultater og erfaringer vil blive formidlet i form af videnskabelige artikler, white papers, blog posts, oplæg på konferencer eller webinarer. Derudover indtænkes resultaterne i den generelle vidensformidling og i arbejdet omkring den videre etablering af TDU’en.
	
	Software udviklet i løbet af året vil blive gjort tilgængelig som open-source løsninger. Konkret vil vi løbende, baseret på behov og erfaringer fra cases, udgive nye versioner af FRESCO og FRESCO-stat til privacy-bevarende dataanalyse med secure multi-party computation. De er begge tilgængelige på GitHub.
	
	OPDATERING:
	Væsentlige aktiviteter og resultater opnået i 2022:
	• Videreudvikling af teknologisk services indenfor privacy-bevarende dataanalyse: Videreudvikling af FRESCO hen mod brug i CRUCIAL projektet og brug i HEDAX projektet.
	• Kompetenceopbygning:
	  ○ Konkret arbejde med teknologierne: ”syntetiske data” og ”differential privacy”
	  ○ Deltagelse i international konference i Zürich om privacy-bevarende teknologier
	• Konkret arbejde omkring samtykker er primært foregået igennem HEDAX projektet, hvor der også er arbejdet med emner som datadonation og sikker brug af sundhedsdata.
	• Nyt samarbejde med vidanspartnere:
	  ○ Udvidet samarbejdet med ITU med nye personer og et nyt område, dette er sket igennem et klyngeprojekt under Cph Fintech
	  ○ CRUCIAL projektet er startet i samarbejde med AAU.