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*	6
Version	1
Periode *Forventet start og slut*	1/1 2021-31/12 2021
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 indsatsområdet?	Målet med aktiviteterne er at kortlægge de udfordringer, danske virksomheder har på dataadgangs- og anonymiseringsfronten samt at afprøve teknologier og værktøjer på dem. Vi vil dette første år danne et videngrundlag for resten af periodens arbejde ved induktivt at kortlægge og analysere, hvordan udfordringerne opleves hos de danske virksomheder, ligesom det er vores mål gennem casearbejder at komme med konkrete bud på teknologiske løsninger til disse udfordringer. 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 handlingsplan understøtter netop datasikkerhedsaspektet i denne problemstilling. Konkret bidrages der til de overordnede mål med en eller flere caseforløb med virksomheder, en ny teknologisk/rådgivnings-service omkring anonymisering og syntetisk data, samt et nyt samarbejde med en vidanspartner.
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 igennem denne aktivitetsperiode arbejde problem- og case-drevet med at kortlægge behov for teknologisk understøttelse af dataadgang og anonymisering. Dette vil vi gøre ved at udvælge og afprøve forskellige cybersikkerheds- og privacyteknologier på aktuelle og relevante problemer/cases. Metoderne og teknologierne vi vil afprøve til en endelig værktøjskasse til løsningen af udfordringerne, er f.eks.: • Anonymisering, herunder differential privacy og anonymisering af ustrukturerede data • Generering og brug af syntetiske data • Edge computing • Multi Party Computation • Federated learning • Blockchain-løsninger • Samtykkeløsninger • Brugercentriske løsninger • Dataetik Konkret vil vi gennemføre mindst én, 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 en teknologisk 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 lab hos Alexandra Instituttet: Security Lab, People Technology and Business Lab og Artificial Intelligence and Data Analysis Lab. Eksterne parter: • Universiteterne: I dette aktivitetsområde vil vi samarbejde med flere af de danske universiteter. Vi har samarbejder i gang med både AU og KU, og vil forsøge at udbygge samarbejdet med de to universiteter, men også med flere universiteter. • De kommende klynger: Hovedsageligt DigitalLead, men også andre klynger hvor denne aktivitet kan støtte op med teknologiske løsninger.
4. Sammenhæng med andre projekter *Indgår aktiviteten i andre eksternt finansierede projekter?*	Aktiviteterne hænger sammen med, og levere tekniske løsninger, til indsatsområderne: ”*Accelerering af digital sundhed og velfærd i Danmark*” og ” *Digitale teknologier til datadrevet, bæredygtig vækst*” Aktiviteterne har generelt sammenhæng med projekterne: Blockchain Data and Privacy – BlockDAP (Industriens Fond), Blockchain Academy Network (Industriens Fond), AutoAI4CS (Industriens Fond), Health Data Exchange – HedaX (Innovationsfonden) og Health Data 360 (Innovationsfonden).
5. Følgegruppe *Har følgegruppen forholdt sig til aktiviteten? I så fald hvordan?*	Samarbejdet med følgegruppen vil ske gennem aktiviteten *Demonstration af anvendelighed og værdiskabelse ift. indsatsområdet Digital sikkerhed, tillid og dataetik.* Dette aktivitetsområde leverer dyb fagligt og relevant indhold og oplæg til teknologisk services, som følgegruppen efterfølgende forholder sig til. Da aktivitetsområdet er fagligt bred vil følgegruppen blive en løst tilknyttet bred gruppe, hvor nogle medlemmer kan involveres yderligere i visse aktiviteter.
6. Formidling af resultater *Hvordan/hvor kan interesserede virksomheder m.fl. 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.*	Formidling af aktiviteternes resultater vil ske gennem aktivitetsbeskrivelsen ” *Demonstration af anvendelighed og værdiskabelse ift. indsatsområdet Digital sikkerhed, tillid og dataetik*”, hvor dette aktivitetsområde bidrager med fagligt indhold, case beskrivelser, teknologioversigt og demonstration etc. De udviklede ydelser vil også stilles til rådighed for markedet gennem den digitale TDU. OPDATERING: Væsentlige aktiviteter og resultater opnået i 2021: • Udgivelse af NLP model til genkendelse af navngivne personer på dansk.

	• Nye forskningsprojekter: Bl.a. et om privacy-bevarende optimering og analyse på vand og el og et om sporing af svindel og hvidvask hos banker. • Udgivelse af open-source software til privacy-bevarende statistik på distribuerede data. • Videnskspredning i form af oplæg på konferencer, podcasts, webinarer og debat-indlæg. • Udgivelse af to videnskabelige publikationer. • Case om anonymiseret brug af data fra spørgeskemaundersøgelser.