SDU Digital

Referat

7. december 2022

Emne:	Møde i Udvalget for informationssikkerhed og databeskyttelse
Dato og tidspunkt:	7. december 2022 klokken 10-12
Sted:	O New Sapphire
Deltagere:	Bue Raun Andersen, Jacob-Steen Madsen, Jan I. Kristensen, Rune Nørgaard Jørgensen, Mads Lildholdt, Peder Thusgaard Ruhoff, Bjarne Nielsen, Simon Kamber (observatør) og Janni Lee B. Bang Brodersen (observatør)
Afbud fra:	Jesper Bo Nielsen
Referent:	Natalie Olsen

Dagsorden:

1. Godkendelse af dagsorden og referat

Bue Raun Andersen bød velkommen og meddelte, at rækkefølgen på de enkelte dagsordenspunkter tilpasses af hensyn til Jan I. Kristensen, som kun havde mulighed for at deltage på en del af mødet.

Ingen bemærkninger til dagsorden og referat.

2. Meddelelser

Udvalget behandlede på seneste møde ophørs- og sletteproces for ansatte- og studerendekonti. Jacob-Steen Madsen takkede for Udvalgets input og meddelte, at disse er blevet indarbejdet i den dokumentation, der er udarbejdet. Jacob-Steen nævnte, at processen nu også er beskrevet i SDU's informationssikkerhedshåndbog.

Janni Lee B. Bang Brodersen henledte opmærksomheden på, at Udvalget tidligere har godkendt retningslinjer for håndtering af brud på persondatasikkerheden på SDU. Udmøntningen af disse er påbegyndt ved oplæg om definitioner, processen og ansvar på område- og sekretariatschefsmøde, og workshop for de lokale GDPR- og informationssikkerhedskoordinatorer. Retningslinjerne skal bidrage til at sikre tydeligere roller og ansvar mellem SDU RIO, SDU IT og SDU Digital i håndteringen af persondatabrud samt sikre læring, så SDU kan forebygge brud på persondatasikkerheden.

Janni meddelte, at Udvalget på næste møde forelægges en årsrapport for 2022. Årsrapporten vil have samme format som sidste gang, og vil også indeholde status fra SDU IT og SDU RIO.

Syddansk Universitet
Campusvej 55
5230 Odense M
T +45 6550 1000
www.sdu.dk

På SDU er der et kontinuerligt fokus på at sikre en god sikkerhedskultur for ansatte. Janni meddelte, at GDPR- og informationssikkerhedskoordinatornetværket samt øvrige interesserede er inviteret til et oplæg om netop god sikkerhedskultur. Oplægget afholdes af Politiet Efterretningstjeneste i næste uge. Dette kompetenceudviklingsformat afprøves i første omgang på ovennævnte gruppe, hvorefter der tages stilling til, om der skal udbydes et lignende oplæg målrettet f.eks. ledere på SDU.

Janni meddelte, at SDU Digital – som et produkt af den strategi for awareness som Udvalget har godkendt – i samarbejde med SDU HR og SDU RIO udbyder to medarbejderkurser i foråret 2023. Kurserne henvender sig til ansatte, som behandler personoplysninger i forbindelse med ansættelsesforhold, studieadministration eller forskning. Kurserne vil være en del af SDU HR's kursuskatalog og vil være frivillige at deltage i.

Udvalget drøftede på seneste møde Udvalg om retningslinjer for internationalt forsknings- og innovationssamarbejde (URIS) anbefalinger. Drøftelserne tydeliggjorde, at der var behov for at afklare Udvalgets rolle i den sammenhæng. Bue Raun Andersen har drøftet det med Universitetsdirektør, Thomas Buchvald Vind, og Direktionen har initiativretten og -pligten, når det vedrører implementeringen af URIS' anbefalinger på SDU.

Simon Kamber orienterede om, at Datatilsynet har nedsat et ekspertudvalg om forskning. Udvalget består af forskellige repræsentanter herunder blandt andet Danske Universiteter (Aarhus Universitet og Danmarks Tekniske Universitet), professionshøjskolerne, Danske Regioner og Danmarks Statistik. Bue Raun Andersen spurgte, om udvalget løbende leverer produkter. Simon Kamber svarede, at udvalget i første omgang vil udkomme med en vejledning om dataansvar i forskningsprojekter. Datatilsynet estimerer, at vejledningen vil komme i første halvdel af 2023, men det er usikkert om den målsætning kan indfries.

3. Drøftelsespunkt: Politik for opfyldelse af oplysningspligten

Simon Kamber rammesatte punktet. SDU er efter databeskyttelsesforordningen forpligtede til oplyse de registrerede om, hvordan SDU behandler oplysninger om dem. SDU efterlever i højere grad forpligtelsen, når det vedrører forskningsprojekter, mens der er et forbedringspotentiale på andre centrale områder.

Problemstillingen er todelt; dels skal SDU opfylde oplysningspligten overfor ansatte og studerende men også ved f.eks. afholdelse

af konferencer. Førstnævnte forefindes men efterlever på nuværende tidspunkt kun delvist reglerne, mens sidstnævnte opfyldes meget ad hoc.

Udvalget bedes drøfte, hvordan SDU sikrer bedre dækning i oplysningspligten til ansatte og studerende og øvrige kategorier af registrerede. Udvalgets drøftelser vil, i tillæg til drøftelser i område- og sekretariatschefskredsen, danne baggrund for en politik, som på et senere tidspunkt forelægges Udvalget til godkendelse.

Udvalget drøftede indledningsvist, hvad opgaven består af, hvilken værdi oplysningspligten giver for de registrerede og hvilken risiko SDU påtager sig ved manglende eller ufuldstændig opfyldelse. Simon Kamber understregede, at SDU ved opfyldelse af oplysningspligten sikrer gennemsigtighed over for de registrerede, når SDU behandler oplysninger om dem. Opfyldelse forudsætter, at SDU har et samlet overblik over behandlingsaktiviteter. Manglende eller ufuldstændig opfyldelse af oplysningspligten, vil for de registrerede betyde, at de reelt ikke har mulighed for at klage over en behandling, da de ikke er klar over, den finder sted. Den primære risiko for SDU som forretning er kritik, påbud eller i sidste ende bøder, hvis Datatilsynet vælger at føre tilsyn med SDU's opfyldelse af oplysningspligten.

Udvalget vurderer, at det er ressourcekrævende både at etablere og vedligeholde det nødvendige overblik. Jacob-Steen Madsen foreslår, at der i højere grad fokuseres på at formulere overordnede principper og retningslinjer, som beskriver SDU's behandling af personoplysninger. Simon Kamber er positivt stemt overfor en sådan løsning, men påpeger sådanne principper også forudsætter et indgående kendskab til SDU's praksis. Et opmærksomhedspunkt Simon Kamber og Bjarne Nielsen i den forbindelse fremhævede var, at sådanne centralt formulerede principper kan pålægge decentrale enheder at følge centralt formulerede principper, og at der på SDU nærmere er tradition for høj grad af decentral medbestemmelse.

Mads Lildholdt påpegede, at det, set fra et brugerperspektiv, ikke er hensigtsmæssigt at lave en lang, samlet beskrivelse af, hvordan SDU behandler personoplysninger om dem. Der er risiko for, at modtagerne ikke læser det, og at SDU derfor ikke reelt opnår den gennemsigtighed, der stræbes efter. Mads foreslår, at informationen i stedet opdeles, og at der f.eks. to gange årligt sendes en mail til eksempelvis de studerende med kortere beskrivelser af, hvordan SDU behandler deres personoplysninger. Rune Nørgaard

Jørgensen foreslog en tilgang, der består af to indsatser. Én hvor studerende kan tilgå den samlede oplysningspligt et sted (f.eks. tænkt som en slags cookieløsning, hvor de præsenteres for det), og en hvor der kommunikeres direkte til de studerende om særlige områder i tråd med det, Mads Lildholdt foreslog.

Janni Lee B. Bang Brodersen tydeliggjorde, at det uanset opgavens omfang er en forpligtelse SDU skal efterleve. Simon Kamber bemærkede hertil, at selvom en målsætning om komplet efterlevelse ikke er muligt, så kan SDU sagtens komme tættere på efterlevelse end der hvor SDU er nu.

Udvalget drøftede, hvem der i praksis skal sikre opfyldelse af oplysningspligten. Mads Lildholdt foreslog inddragelse af de kollegiale organer, mens Bue Raun Andersen informerede om, at område- og sekretariatschefskredsen ligeledes vil drøfte det. Bjarne Nielsen understregede, at det nøje bør overvejes, hvordan arbejdet struktureres, hvis opgaven placeres i én afdeling. Nogle områder i Fællesadministrationen kan ikke forventes at besidde den tekniske indsigt, det kæver. Janni Lee B. Bang Brodersen nævnte, at opgaven kunne løses ved at én afdeling er ansvarlig for opfyldelse af oplysningspligten, men at det sker på baggrund af input fra hele organisationen, som det også er foreslået i notatet.

Bue Raun Andersen opsummerede, at det ikke er realistisk at opnå en fuldstændig opfyldelse af oplysningspligten, men at SDU skal tage nogle væsentlige skridt i retningen af i højere grad at efterleve den. Bue understregede ligeledes, at dette er en fælles opgave. Udvalgets input vil indgå i udkastet til politik for oplysningspligt.

4. Beslutningspunkt: Retningslinjer for tilsyn med databehandlere

Janni Lee B. Bang Brodersen rammesatte punktet. Det er et krav, at SDU skal føre krav med sine databehandlere, og dette har hidtil været udført meget ad hoc. Det indstilles, at Udvalget godkender retningslinjerne for tilsyn med databehandlere. De beskriver arbejdsdelingen mellem SDU RIO, SDU IT og systemejerne og hvordan SDU i praksis vil føre tilsyn med databehandlere. Tilsynene koordineres af SDU RIO, som vil inddrage systemejere og SDU IT i det omfang, der er behov for det, men det er systemejeren der i sidste ende er ansvarlig for, at der bliver ført tilstrækkeligt tilsyn.

Martin Svensson ønskede at opklare, hvad der forstås ved systemejer, og hvilke systemer, der er tale om. Janni Lee B. Bang Brodersen og Jacob-Steen Madsen svarede, at det vil være systemer, hvor der behandles personoplysninger, og at størstedelen er fælles

systemer, hvor SDU IT, SDU Studieservice, SDU HR og Økonomiservice er systemejere. Lokale forskerservere, hvor der ikke behandles personoplysninger, vil derfor ikke være omfattet.

Jan I. Kristensen supplerede, at SDU RIO i den kommende tid ligeledes ved opstarte tilsyn med databehandlere i forskningsprojekter. Martin Svensson spurgte hertil, om det i så fald er den enkelte forsker, der er systemejer, og dette bekræftede Jan.

Bue Raun Andersen konkluderede, at Udvalget ikke har bemærkninger til retningslinjerne, og de godkendes derfor. SDU Digital, Compliance vil i samarbejde med SDU IT og SDU RIO skrive procedurer, som udmønter retningslinjen.

5. Drøftelsespunkt: Databeskyttelsesvurderinger ved anskaffelser af nye itsystemer og SDU's risikoappetit

Janni Lee B. Bang Brodersen indledte punktet. Indstillingen behandler en række forskellige, relaterede problemstillinger, herunder hvordan det sikres, at der laves databeskyttelsesvurderinger ved ibrugtagen af nye systemer, i hvilket omfang Udvalget inddrages ved overordnede og konkrete risikovurderinger samt input til, hvordan der etableres en pragmatisk tilgang til brugen af lokaladministratorrettigheder. Sidstnævnte vedrører særligt, at det også ved anvendelse af lokaladministratorrettigheder skal sikres, at de rette vurderinger foretages, samtidig med at det ikke begrænser agilitet i forretningen.

Udvalget er bakker op om, at der naturligvis skal laves de påkrævede vurderinger ved ibrugtagen af nye systemer. Flere af Udvalgets medlemmer er tilhængere af en pragmatisk løsning, hvor behandling af personoplysninger er sekundær (f.eks. kun e-mail og IP-adresse) ikke udløser en større vurderingsopgave. Mads Lildholdt opfordrede i den forbindelse til, at det ikke bør være unødigt kompliceret for slutbrugeren at navigere i, hvilken brug af systemet der er tilladt, og hvilken der ikke er. Martin Svensson påpegede, at det i designet af processen ligeledes bør indtænkes, at opsættes der for mange barrierer for særligt forskerne, så risikerer SDU, at forskerne benytter alternative systemer.

Martin Svensson bemærkede, at det i indstillingen er foreslået at gøre et kursus, som beskriver ansvar i forbindelse med brugen af lokaladministratorrettigheder, obligatorisk. Martin vurderer, at det ikke bør være obligatorisk, men være op den lokale ledelsesstreng at sikre, at medarbejderne kender og overholder retningslinjerne. Simon Kamber gjorde opmærksom på, at denne vurdering ikke laves i dag, men at lokaladministratorrettigheder kan bruges på alle

udleverede enheder. Dette er efter Datatilsynets vurdering ikke i overensstemmelse med databeskyttelsesreglerne.

Jacob Steen-Madsen fremhævede, at Rigsrevisionen har anerkendt SDU's risikoappetit på dette område særligt når det vedrører forskeres behov for at benytte lokaladministratorrettigheder, og at dette bør medtages, når vi drøfter brug af lokaladministratorrettigheder på SDU.

Bue Raun Andersen konkluderede, at der er tilslutning til grundprincipperne i oplægget, og at disse kan danne grundlag for at det fremadrettet i højere grad sikres, at der udarbejdes databeskyttelsesvurderinger på de systemer, SDU anvender/indkøber. Udvalget forelægges et overordnet risikovurderingskoncept på et kommende møde. Udvalget vil på et senere tidspunkt drøfte brugen af lokaladministratorrettigheder på SDU.

6. Beslutningspunkt: MAM-WE på mobile enheder

Jacob-Steen Madsen rammesatte punktet. Udvalget har tidligere behandlet ibrugtagen af MAM-WE for ansatte, som benytter private enheder. SDU IT har allerede implementeret MDM på SDU-udleveret udstyr. MAM-WE er applikationsbeskyttelse, som sikrer tilstrækkelig beskyttelse af data. Det betyder i praksis, at SDU udelukkende har indsigt i de SDU-data, der behandles på enheden og ikke øvrige aktiviteter eller behandling af data, der sker på enheden. SDU IT har gennemført pilottest ved udvalgte områder i Fællesadministrationen og i den forbindelse indarbejdet Udvalgets ønsker om mere transparens overfor brugerne. SDU IT har i pilottesten ikke identificereret udfordringer i brugeranvendelse. Udvalget forelægges et implementeringsoplæg, hvorefter det indstilles til Hovedsamarbejdsudvalget, at MAM-WE implementeret for alle ansatte på SDU.

Martin Svensson spurgte, om dette vedrører anvendelsen af privat udstyr samt om det drejer sig om beskyttelsen af data. Jacob-Steen Madsen bekræfter, og siger at det omfatter dels muligheden for at hjemtage data ved bortkomne enheder men også krav om sikkerhed på selve enheden (f.eks. nyere opdateringer, kodeord mv.).

Martin Svensson mente, at dette kan skabe problemer for forskere, som anvender private enheder efter eget ønske. Hvis SDU pålægger denne gruppe at installere særlige programmer for at kunne anvende privat udstyr, er der risiko for, at de omgår SDU's retningslinjer og i stedet anvender en privat e-mailadresse til behandling af SDU-data.

Rune Nørgaard Jørgensen er meget enig i, at SDU skal være transparente, men mener samtidig at organisationen og brugerne på SDU bør indstille sig på, at have set toppen af brugervenlighed og mulighederne for lokale løsninger, når det vedrører informationssikkerhed. Det giver ikke mening at implementere en masse foranstaltninger på en række områder, og så samtidig ikke sikre forsvarlig beskyttelse af data, når det vedrører private enheder.

Flere af Udvalgets medlemmer er meget enige med Rune, men understregede vigtigheden af, at det er gennemsigtigt for brugerne, hvad der foregår. Det skal beskrives indgående og på en brugervenlig måde, hvilken betydning MAM-WE har for den enkelte (tekniske krav til enheden, hvad SDU kan se, hvad formålet er, hvad med to SIM-kort, begrænsninger mv.). Martin Svensson efterspurgte i den forbindelse, at kommunikationen differentieres, så de ansatte med høj grad af teknisk indsigt også kan tilgå informationer herom.

Rune Nørgaard Jørgensen foreslår, at de detaljerede tekniske beskrivelser indsættes som en fodnote i kommunikationsmaterialet, og tilbyder samtidig at give feedback på kommunikationsmaterialet, inden det udsendes.

Bue Raun Andersen opsummerede, at der er behov for at styrke sikkerheden på mobile enheder på SDU, og at det er vigtigt at dette gøres på en gennemsigtig måde overfor brugerne. Udvalget input medtages i det videre arbejde.

7. Beslutningspunkt: SSPR (Self-Service Password Reset) for ansatte på SDU

Jacob-Steen Madsen præsenterede punktet. SDU anvender et værktøj, som kan isolere en konto, der har mistænkelig eller ændret brugeradfærd, som en foranstaltning for at imødegå cybertruslen. Det betyder, at ansatte kan opleve, at deres konto isoleres på tidspunkter, hvor det ikke er muligt at få support i Servicedesk. Det indstilles derfor, at SSPR (Self-Service Password Reset) implementeres for ansatte på samme måde som det er det for studerende. De studerende har positive erfaringer med, og Servicedesk har oplevet mindre support.

Løsningen gør det muligt for den enkelte at nulstille sin adgangskode, således at ens identitet kan blive bekræftet, og man derved igen kan tilgå SDU's systemer i tilfælde af at ens konto isoleres. Løsningen forudsætter, at den ansatte angiver en privat e-mailadresse og et telefonnummer. Det er muligt at blive undtaget løsning, hvis man henvender sig i Servicedesk.

Martin Svensson spurgte, om det er tilstrækkeligt at oplyse sit SDU-telefonnummer, og om oplysningerne angives i en browser. Jacob-Steen Madsen bekræftede begge spørgsmål, og Linux-brugere vil derfor heller ikke have problemer med at anvende løsningen. Jacob-Steen Madsen understregede desuden, at ingen telefonnumre eller mailadresser trækkes fra eksisterende lister, men at den enkelte udelukkende selv angiver disse oplysninger i løsningen.

Nogle af Udvalgets medlemmer spurgte, om det er muligt at ændre den mail, der i første omgang er angivet, hvad man gør, hvis man mister det man nulstiller med, og hvem i SDU IT, der kan se disse data. Jacob-Steen Madsen oplyste, at det angive altid kan ændres, at man ved bortkommen e-mailadresse eller telefonnummer skal henvende sig til Servicedesk, og at SDU IT ikke kan se data.

Udvalget drøftede kommunikationsstrategi, og Udvalget anbefaler, at Udvalgets medlemmer og informationssikkerhedskoordinatorerne kommunikerer beslutningen. SDU IT udarbejder et oplæg til kommunikationsmateriale i samarbejde med SDU Digital, som Udvalgets medlemmer kan benytte i den lokale kommunikationsindsats. Samtidig lægges en nyhed på SDUnet.

Bue Raun Andersen konkluderede, at Udvalget godkender indstillingen og tager udgangspunkt i udvalgets anbefalinger til kommunikation.

8. Eventuelt