Informationssikkerhed

Rapportering til KU's bestyrelse 2022

15. juni 2022

KØBENHAVNS UNIVERSITET

Bestyrelses rapportering

Informationssikkerhed handler om at sikre, at vi kan stole på vores informationer.

Dette gør vi ved struktureret at se på forhold, som skal sikre at fortroligheden af vores informationer er ordentlig, at integriteten af vores informationer er intakt og at tilgængelighed af vores informationer er god.

Dette gøres ved samlet at se på, om de faktiske forhold der er omkring organisatoriske procedurer, menneskelig adfærd og tekniske sikringer, står mål med de trusler som kan udfordre fortroligheden, integriteten og tilgængeligheden af vores informationer

Rapportering til KU's bestyrelse 2022

Informationssikkerhed, ydre krav og forhold.

- Ny national strategi for cyber og informationssikkerhed.
- Opfølgning fra Rigsrevisionen (2021) på Rigsrevisionens beretning om "Universiteternes beskyttelse af forskningsdata" (2019).
- Ministeriel opfølgning.
- GDPR.
- ISO 27001 opdatering.
- Ny national strategi for datamanagement baseret på FAIR principperne.

KU's modstandskraft, organisatorisk og teknisk.

- Informationssikkerhedsenheden.
- Udvalg og projekter.
- Fakulteter og Fællesadministrationen.
- GDPR.
- KUIT.

KU risikovurdering.

- Samlet vurdering af trusler overfor organisatorisk og teknisk modenhed.
- Samlet vurdering af trusselsbilledet og KU's sikringsniveau
- KU's sikringsniveau ift. trusselbilledet
- Større sikkerhedshændelser: 'log4j', Workzone, NorS
- KU's sikringsniveau - teknisk
- GDPR

Informationssikkerhed, ydre krav og forhold.

Ny national strategi for Cyber og Informationssikkerhed.

- I december 2021 udgave regeringen en ny national strategi for cyber- og informationssikkerhed.
- Forskning nævnes eksplicit i strategien som et fokusområde.
- Der skal udvikles sektorspecifikke strategier inden for de fleste ministerieområder.
- KU's CISO deltager i en arbejdsgruppe med deltagelse fra SDU og DK-CERT ift. en sektorstrategi
- Der er afholdt indledende møder med ministeriet den 25. april 2022.

Opfølgning fra Rigsrevisionen i 2021 på Rigsrevisionens beretning om "Universiteternes beskyttelse af forskningsdata" fra 2019

- Rigsrevisionen meldte i marts 2021 at de ville følge op på beretningen fra 2019, dette arbejde afsluttede de i december 2021.
- Rigsrevisionen har på baggrund af revisionen i 2021 udgivet et notat (pt set som høringsudkast) til beretningen fra 2019
- Notat dækker både ministeriet, sektoren og specifikt KU.
- KU er blevet revideret på 3 institutter (Institut for Nordiske Studier og Sprogvidenskab (NorS), Biomedicinsk Institut (BMI) og Niels Bohr Institutet (NBI) samt KU-IT.
- Nors, BMI og KU-IT har bevæget sig frem siden 2019. NBI trækker dog det samlede indtryk ned.
- Generelt er Rigsrevisionen ikke tilfreds med tempoet for sektoren i forhold til at rette op på kritiske it-sikkerhedsbrister.
- Rigsrevisionen vil foretage en ny revision i 2023 på både KU og resten af sektoren.

Informationssikkerhed, ydre krav og forhold.

Ministeriel opfølgning.

- I Rigsrevisionen beretningen fra 2019 fik ministeriet kritik for ikke at følge ordentligt op på universitetssektoren omkring informationssikkerhed.
- Ministeriet har i 2019 og 2021 fulgt op på KU.
- I Rigsrevisionens notat (pt set som hørringsudkast) som opfølgning på beretningen fra 2019 fremgår det, at ministeriet først vil følge op på universiteterne igen i 2023, idet de vil afvente arbejdet med en sektorstrategien.

ISO27001 opdatering.

- KU arbejder med informationssikkerhed ud fra principperne i informationssikkerhedsstandarten ISO27001.
- ISO27001 er blevet opdateret med ISO27002, som gør standarden mere vejledende og nemmere at arbejde med når principperne skal implementeres, både når det gælder den organisatoriske og tekniske sikring.
- Ekstern opfølgning fra både myndigheder og samarbejdspartnere vil formentlig betyde større krav til en mere formel efterlevelse af ISO2700X, uden at dette dog nødvendigvis betyder at en ISO2700X certificering vil give mening på KU.

Informationssikkerhed, ydre krav og forhold.

GDPR

- Schrems II dommen, der bevirker at persondata ikke kan overføres til USA, er stadig en udfordring for EU og medlemslandene.
- Der arbejdes i EU på en ny standardaftale for overførsel til USA, den må dog forventes at blive udfordret på samme måde som de tidligere Schrems domme.
- Løbende nye vejledninger fra både det danske tilsyn, men også på EU-plan fra European Data Protection Board (EDPB), som har betydning for vores arbejde.
- Over 30 verserende sager ved EU-domstolen, som vil ventes at få betydning for, hvordan vi behandler personoplysninger.

Informationssikkerhed, ydre krav og forhold.

Ny national strategi for datamanagement baseret på FAIR* principperne.

- I oktober 2021 udgav ministeriet en ny national strategi for datamanagement baseret på FAIR principperne.
- KU's nye politik for forskningsdatamangement, som blev godkendt i begyndelsen af januar 2022 er i overensstemmelse med den nationale strategi for datamanagement.
- KU nye politik for forskningsdatamangement adressere samtidig et centralt kritikpunkt i Rigsrevisionens beretning fra 2019 omkring ansvar for forskningsdata.
- I forbindelse med implementering af den nationale strategi for datamanagement er KU's afdeling for informationssikkerhed repræsenteret.
- Der er nedsat en national følgegruppe under Uddannelses- og Forskningsministeriet der skal følge og koordinere strategi implementering på tværs af Danmark. John Renner Hansen er formand for gruppen og Susanne den Boer (F&I) er medlem
- Der er oprettet 5 arbejdsgrupper under følgegruppen, der vil arbejde med koordinering af data management support og FAIR implementering (fra KU: Lektor Klaus Steenberg Larsen, Science), infrastruktur, finansiering (Prodekan Lise Arleth, Science), uddannelse (Lektor Haakon Lund) og sikkerhed (CISO Thomas Schlichting – formand).
- Dual Use forsøges adresseret i sikkerhedssporet, i forhold til bedre at forstå hvordan data kan misbruges.

*FAIR principperne sætter rammen for, hvordan data kan gøres findable (søgbare), accessible (tilgængelige), interoperable (udveksles og behandles entydigt) og reusable (anvendelige) – så både mennesker og computere kan finde og behandle data.

Modstandskraft – organisatorisk tiltag

Informationssikkerhedsenhed er organisatorisk forankret under Forskning og Innovation i FA.
Informationssikkerhedsenheden består af 5 årsværk:

Informationssikkerhed: Informationssikkerhedschefen – CISO Informationssikkerhed konsulent (p.t. ubesat)	KU har pr. 1 januar fået ny CISO. Fra perioden 1/8 til 31/12 har funktion været varetaget af informationssikkerhedskonsulenten, som efterfølgende har overtaget stillingen som CISO. CISO funktionen referere nu til Prorektor for forskning David Dreyer Lassen. Der er etableret faste møder mellem CISO og prorektor for forskning. For at styrke det organisatorisk fokus på informationssikkerhed er der desuden etableret faste møder (hver anden måned) mellem Prorektor for forskning, Universitetsdirektøren, Vicedirektør for Forskning og Innovation samt Vicedirektør for KU-IT.
GDPR: Databeskyttelsesrådgiver – DPO	KU har pr. 1 april fået ny DPO. Fra perioden fra 12/12 hvor KU's tidligere DPO stoppede, har funktionen været varetaget af DeiCs DPO tjeneste. DPO funktionen referere forsat til Universitetsdirektør Jesper Olesen. Området forventes organisatorisk styrket som resultat af GDPR-arbejdsgruppens arbejde som er del af Jura kortlægningen. (vi ved ikke helt hvad vej det går endnu)
Forskningsdatamanagement: 2 specialkonsulenter	Forskningsdatamanagement er blevet styrket i Informationssikkerhedsenhed med et yderligere årsværk. Der er etableret en følgegruppe i forbindelse med implementeringen af forskningsdatamanagement politikken, med Kim Brinckmann som formand.

Modstandskraft – organisatorisk tiltag

Udvalg og projekter

Informationssikkerhedsudvalget (ISU): Formand: Prorektor for forskning Deltagelse af repræsentanter fra fakulteter og FA søjler samt CISO, DPO og Chef for fysisk sikkerhed.	KU modnes organisatorisk i disse år omkring informationssikkerhed. Hastigheden hvormed det sker er forskelligt i organisationen og den nødvendige modenhed vil variere i forskellige dele af organisationen. Der er i januar 2022 i ISU regi introduceret et årshjul for bl.a. at styrke muligheden for opfølgning på modningsniveauet ude i organisationen.
Rapportering af sikkerhedshændelser: ISU møderne bruges til at dele erfaringer omkring sikkerhedshændelser og rapportering af disse.	I KU-satsningen "Sammenhængende processer på KU" er flowet omkring sikkerhedshændelser udvalgt som en oplagt case for at arbejde med at optimere og digitalisere i 2022. Det forventes at dette arbejde vil styrke og ensrette indrapportering af sikkerhedshændelser, med det formål bedre at kunne mitigere mod potentielle sikkerhedshændelser.
Beredskabskoncept for Cyberhændelser: Der er i BCM gruppen iværksat et projekt for at udvikle et bredskabskoncept for Cyberhændelser.	Projektet vil adressere de specifikke udfordringer, som opstår i en beredskabssituation forårsaget af en cyberhændelse. Projektet forventes som en sideeffekt at skærpe opmærksomheden omkring informationssikkerhed i organisationen.

Modstandskraft – organisatorisk tiltag

Fakulteter og Fællesadministrationen

Lokale informationssikkerhedsudvalg (LISU): Fakulteterne og Fællesadministrationen har lokale informationssikkerhedsudvalg (LISU) og forskellige lokale tiltag på området.	Fakulteterne og Fællesadministrationen arbejder hver især med at modne organiseringen af informationssikkerhed. På Fakulteterne er arbejdet længst fremme på HUM, JUR og SUND. HUM, SUND og SCIENCE har ansat medarbejdere som i forskellig grad varetager arbejdet med informationssikkerhed. I Fællesadministrationen er især U&S, men også ØKO og KOM længst fremme med den organisatoriske forankring af informationssikkerhed.

Modstandskraft – organisatorisk tiltag

KU-IT

IT-sikkerhed i Basisservice, KU-IT Gruppe i KU-IT Basisservice med fokus på IT-sikkerhedområdet. Bemandet med 15 medarbejdere med variende opgaver inden for IT-sikkerhed	I forbindelse med dannelsen af KU-IT blev IT-sikkerhed forankret i en særskilt gruppe med 4 ÅV. Efter Rigrevisionens rapport om KU's beskyttelse af forskningsdata i 2019 godkendte rektoratet et IT-sikkerhedprogram bestående af en lang række forskellige initiativer med efterfølgende driftaktiviteter. I den forbindelse er IT-sikkerhed udvidet til 15 ÅV som arbejder med alle former for IT-sikkerhed dækkende awareness, risikovurderinger, loganalyse, kryptering etc. Der er som det seneste f.eks. Allokeret årsværk til at bemande et Security Operations Center (SOC)

Modstandskraft – tekniske tiltag

KUIT

KU Computer: KU-IT geninstallerer computere på hele KU. Geninstallationen øger bl.a. sikkerheden og sikre bedre opdatering af software som hjælper med at beskytte mod f.eks. malware og ransomware.	I forbindelse med etableringen af KU-IT har KU skulle geninstallere eller udskifte 13.500 computere. På nuværende tidspunkt udestår ca 3500 at blive omlagt til KU-computer. Det forventes færdig ved udgangen af Q2 2022. Herefter vil der stadig være forskningsudstyr, som af forskellige årsager ikke kan omlægges til KU-computere. Disse computere skal isoleres fra andet udstyr således at de ikke udgør en sikkerhedsmæssig udfordring.
Nyt Netværk: KU-IT implementerer nyt intelligent netværk på hele KU. Netværket vil, når det er færdigt, kunne isolere sårbart udstyr og bedre sikre følsomme og værdifulde informationer.	KU-IT har gennemført en test af teknologien på udvalgte områder af KU, og har nu påbegyndt implementering i produktion for campusservice IT-udstyr samt netværket på de respektive campus områder. Det forventes at være færdigimplementeret i løbet af 2023. Det nye netværk kommer til at sætteret højt niveau adgang til KU netværk, dette gælde også for forsknigsudstyr og Bring Your Own Device (BOYD)
Proaktiv overvågning: KU-IT arbejder med at kunne opdage angreb når de sker, i stedet for først at skulle reagere, når skaden er sket.	Det nødvendige værktøj er teknisk på plads til opsamling af diverse datalogs. Der arbejdes nu på at få identificeret hvilke logs på KU, som kan give den bedste mulighed for at opdage angreb og få disse logs leveret ind til logningssystemerne. De steder hvorfra der allerede leveres informationer til sikkerhedssystemerne, har vist sig funktionsdygtige og har fanget en række forsøg på angreb.

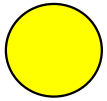
Trusselsbilledet og KU's sikringsniveau - læsevejledning

Rød betyder at **niveauet er faldet** eller at et **væsentlig kriterie har ændret sig**

Gul betyder at **der skal ekstra tiltag til** eller opmærksomhed for at forblive sikker

Grøn betyder at **sikkerheden/opgaven er på rette spor**

Samlet vurdering af trusler overfor organisatorisk og teknisk modenhed.



Med de nuværende organisatoriske og tekniske foranstaltninger som er implementeret, vægtet imod de trusler, som det er vurderet, at KU er mål for, vurderes det sandsynligt (4 på en skala fra 1-10), at KU i det kommende år vil kunne blive ramt af et angreb, som KU ikke har det fornødne sikkerhedsniveau til at kunne modstå. Det er desuden uvist, om KU har det fornødne beredskab (backup og restore evne) til at komme tilbage til et acceptabelt niveau.

Modenheden på Københavns Universitet vurderes til at være på niveau med det meste af sektoren, både nationalt og med dem som vi sammenligner os med internationalt.

Dette angår såvel sikkerhedsudfordringer forsaget af bl.a. teknisk gæld, som den meget åben kultur, der kendetegner sektoren.

Vurderingen kvalificeres på de efterfølgende slides.

Trusselsbilledet og KU's sikringsniveau - samlet vurdering

Emne	Trafiklys 19/4 2022	Kommentar
Trusselsbilledet og ændret risikooplevelse – siden seneste rapportering.	●	Truslen mod sektoren forsat meget høj. truslen fra cyberspionage og insidere blev i januar 2022 vurderet forhøjet af PET: • Cyberspionage, Cyberkriminalitet og Insidertruslen er meget høj • Cyberaktivisme er lav. Ved seneste vurdering, for et år siden, var der varsler om spionage rettet mod COVID 19-forskningen, og hvor vi i Danmark oplever Corona som overstået, er dette ikke tilfældet for store dele af resten af verden. Trusselbilledet fra sidste år er derfor stadig aktuel. **Situationen i Ukraine forhøjer især aktualiteten af insidertruslen. Universiteterne har en meget åben kultur og der er ikke tradition for baggrundstjek af hverken ansatte eller studerende. – dette er indskærpet i intern kommunikation.** **Hvor cyberangreb tidligere har haft form af ransomware til berigelse, kan angreb som udløber af krigen i Ukraine have en mere ødelæggende intention.**

Trusselsbilledet og KU's sikringsniveau - samlet vurdering

Emne	Trafiklys 19/4 2022	Kommentar
KU's sikringsniveau ift. trusselbilledet		KU-IT har siden sidste rapportering fået flere værtøjer sat i drift, som kan bruges til proaktivt at beskytte KU's IT-infrastruktur og udstyr. Etablering af en mere konstant proaktiv overvågning og deraf følgende beskyttelse vil kræve yderligere tiltag. Før udrulning af KU-computer og nyt netværk er tilendebragt vil KU-IT's tekniske sikringsløsninger ikke slå fuldt igennem i praksis. En endelig implementering af nyt nærværk er ligeledes en forudsætning for at håndtere "Bring You Own Device" som Rigsrevisionen påpeger. Som følge af den mere ødelæggende natur af cyberangreb, er test af evnen til at reetablere fra backup blevet yderligere aktuel. Der er behov for at indskærpe dette over for systemejere via KU's ssystemejerforum. Insidertruslen er som udgangspunkt svær at håndtere og især i en forskningskultur, og der er ikke tradition for at koble adgang til informationer af følsom karakter med baggrundstjek i forbindelse med ansættelse. Fortsat fokus på vedligeholdelse af informationssikkerhedvurderinger mhp. aktivt at kunne imødegå det høje trusselsniveau, der hvor det er identificeret i informationssikkerhedvurderingerne.

Større sikkerhedshændelser - log4j

Emne	Trafiklys 19/4 2022	Kommentar
Log4j er komponent i Java, som er meget udbredt på mange platforme.		Fredag d. 10. december 2021 blev en alvorlig sårbarhed (Log4Shell) som benyttes udbredt i Java logningsmodul, rapporteret som en 0-dagssårbarhed over hele verden. KU-IT beredskabsledelse eskalerede sagen til KU´s kriseberedskab tirsdag d. 14. december. • Der blev scannet ca. 1990 forsknings-, administrations- og systemservere (Linux og Windows). • Der blev identificeret 320 med log4j sårbarhed. • Af de 320 sårbare var der 22 identificeret som mistænkelige, som blev taget ud af drift til yderligere undersøgelse. • Af disse 22 er det efterfølgende konkretiseret at to af dem havde været udsat for mistænkelig trafik – men dog ingen tegn på databrud eller konkret efterfølgende udnyttelse af sårbarheden – hvorefter KU-IT fjernede sårbarheden. • De servere (320-22=298) som fik identificeret sårbarheden har ligeledes fået fjernet den. Organisatorisk blev det tydeligt at at især Campusdrift området havde en udfordring i forhold til at Campusdrifte områder er delt op mellem CAS og Sund og Science. Udfordringen blev løst ved en særlig indsats på dette område. Generelt manglede der beredskabsplaner og overblik lokalt i organisationen. Projektet om "Beredskabskoncept for Cyberhændelser" samt etablering af et årshjul for området forventes at hjælpe til delvist at rette op på dette.

Større sikkerhedshændelser - Workzone

Hændelse	Trafiklys 19/4 2022	Kommentar
Workzone er KUs journalsystem. En ændring i KUs centrale indentitetsstyring gjorde at rettighedsstyringen i workszone blev ændret så der kom for bred adgang på områder i systemet.	●	Da fejlen bliver opdaget vælger systemejer (HR) at lukke for systemet. Systemet er utilgængeligt i mere end et døgn og er påhvirket i 2 døgn. Kompleksiteten i fejlen kan kun udreddes fordi at Workzone driftes med udvidet log og med en funktionel backup. Udredning foregår i samarbejde med KMD. Systemejeren roser både KUIT's håndtering og KMD som leverandør. Hændelsen er et godt eksempel på nødvendigheden af logning på det rette niveau, backup og det rigtige leverandør forhold.

Større sikkerhedshændelser - NorS

Hændelse	Trafiklys 19/4 2022	Kommentar
KUIT observerer usædvanlig trafik fra en forskningsserver på instituttet NorS.		Serveren bliver taget ud af drift, og det viste sig at en service på serveren havde en sårbarhed som var blevet udnyttet. Efterfølgende evaluering tyder på utilstrækkelig patchning/opdatering af applikationer. Det er blevet tydeligt for instituttet at det er nødvendig at have en tættere dialog mellem dem som anvender serveren og dem som drifter serveren. Serveren blev taget ned i slutningen af marts og er endnu ikke oppe, da der er noget tesknisk gæld, som skal afklares. Servicegennemgange i 2019 konkluderede det samme mere generelt på KU

KU's sikringsniveau - teknisk

Emne	Trafiklys 19/4 2022	Kommentar
Klient siden - upatched		De standard klienter (KU computer model a og b) som vedligholdes af KU-IT bliver på nuværende tidspunkt patchet så både standard software og det meste specialsoftware opdateres inden for en passende tidshorisont efter frigivelse af sikkerhedspatches. Der er en resterende mængde klienter som brugerne selv står for at vedligholde, da det enten er forsknings- eller laboratorieklienter eller på anden måde er egenadministreret. Her er patchniveauet ikke på niveau med de øvrige klienter. KU computer patchet inden for 10 dage: Øvrigt udstyr patchet inden for 10 dage: (NB. Det er ukendt hvordan omfanget er for NBI og Kemi)

Emne	Trafiklys 19/4 2022	Kommentar
Server siden – upatched		Ud fra de scanninger og den viden som KU-IT har om serverenes patchniveau, så udestår der sikkerhedpatchning på mange servere. Det gælder både for de grundlæggende systemer og for det software som er installeret på serverne. Servere hvor leverandør af operativsystemer ikke levere sikkerhedspatches mere: Servere med software som er upatchet (kun sikkerhedsårbarheder som er vurderet kritisk og eller meget kritisk)

KU's sikringsniveau - teknisk

Emne	Trafiklys 19/4 2022	Kommentar
Overvågning		Logning på netværk og af systemer er væsentligt for at opdage sikkerhedshændelser. Udarbejdelse af informationssikkerhedsvurderinger til at identificere kritiske logningspunkter går for langsomt. KUIT's sikkerhedsafdeling har oparbejdet evnen til at modtage og forstå alarmeringer. Behandling af alarmer foregår pt kun inden for normal arbejdstid (i forbindelse med log4j var det 24/7). Oparbejdelse af evnen til at reagere 24/7 vil kræve en del yderligere personale og yderlige investering hos KUIT for at opnå en højre automatiseret respons på hændelser. En øget modenhed både teknisk og organisatorisk på KU vurders at være en forudsætning for at høste gevinsten for at overgå til 24/7 beredskab. Logning er et tema i forbindelse ved udviklingen af en sektor strategi.

Emne	Trafiklys 19/4 2022	Kommentar
Backup – disastor recovery		Der bliver taget backup af infrastruktur og services af KUIT. I servicegennemgangen i 2019 blev det tydeligt at de fleste systemejer manglede en dialog med KUIT om test af Backup. Det vurderes at enkelte FA-enheder har fået testet dette. Udarbejdelse og løbende forbedring af årshjulet for informationssikkerhed forventes at kunne skabe mere viden om niveauet af backup test.

GDPR

Emne	Trafiklys 15/6	Status	Kommentar
Opfølgning på Schrems-II-dommen angående overførsel af persondata til lande uden for EU/EØS		Der blev i 2021 nedsat en intern arbejdsgruppe, for at kortlægge aftaler og kontrakter, hvor persondata overføres til lande uden for EU/EØS. Arbejdsgruppen fik udarbejdet templates til registrering af databehandleraftaler mv. Det efterfølgende arbejde med en fortsættelse af analysen omkring Schrems-II blev dog sat i bero indtil ny DPO ansættelse. Arbejdet ventes genoptaget medio 2022.	EU-Domstolen har den 16. juli 2020 afsagt en dom, som betyder, at persondata ikke kan overføres til USA uden supplerende garantier. Dommen opstiller nye krav, hvis persondata skal overføres til andre lande uden for EU/EØS. KU-IT har som følge af Schrems-II arbejdet på at få en krypteringsløsning, som lever op til anbefalingerne fra Det Europæiske Databeskyttelsesråd når der anvendes en cloud-leverandører i lande, som ikke lever op til de europæiske garantier. KU-IT forventer at løsningen vil være tilgængelig på KU inden sommerferien.

GDPR

Emne	Trafiklys 15/6	Status	Kommentar
GDPR on-line kursus obligatorisk (ansatte)	🟡	Pr 21. april 2022 har 4847 medarbejdere taget kurset ud af 11435, som har adgang til kurset	Kurset blev i 2020 obligatorisk for alle medarbejdere, som behandler persondata Pr 29. april 2021 havde 4534 gennemført Der er nu indkøbt licenser, så studerende også kan tage et on-line GDPR-kursus.
GDPR on-line kursus (studerende)	🟢	Igangværende projekt	Det er et KU2023 projekt "Studerendes digitale dannelse", hvor tidligere DPO har deltaget. Ny DPO vil hurtigst muligt følge op med projektgruppen.
Privatlivspolitik, procedurer, vejledninger og skabeloner til persondata udarbejdet og i drift.	🟢	Løbende vedligehold	Evaluering af overholdelsen af GDPR er blevet udsat igen p.g.a. manglende DPO. Ny DPO vil snarest muligt kortlægge alle GDPR politikker, processer og procedurer, med henblik på en evaluering om evt. manglende politikker, processer og procedurer, samt at opbygge en kontrolfunktion af disse m.m.

GDPR

Emne	Trafiklys 15/6	Status	Kommentar
Sikkerhedshændelser indberettet til Datatilsynet	●	Få indberetninger i første 4 måneder af 2022	Hovedsagelige menneskelige fejl. Datatilsynet har stillet en række spørgsmål angående en sag hvor pseudonymiseret forskningsdata ved en fejl var lagt på KU's CMS til undervisningsbrug. Sagen venter endelig afgørelse fra Datatilsynet.
Whistleblower- ordning på KU	●	KU anvender en ekstern administration af ordningen	Tidligere DPO har deltaget i en arbejdsgruppe nedsat af rektorsekretariatet, om etablering af whistleblower – ordning jf. lov nr. 1436 af 29.juni 2021. Arbejdsgruppen har valgt, at KU anvender en ekstern administration af ordningen.
Projekt "Slettebanden"	●	Løbende vedligehold	Tidligere DPO har iværksat aktiviteten "Slettebanden", med henblik på at få administrative medarbejdere på KU til at slette persondata, som ikke længere skal bruges til formålet samt at dokumentere slettefrister. Ny DPO vil følge op på aktiviteten i løbet af 2022.