AALBORG UNIVERSITET

GDPR-tiltag

i

Projekt og systemforvaltning (POS)

Skrevet af: Lars Lohmann (LLO) og Merete L. Madsen (MLM)

Version: 8

Indhold

1 Formål og revision af dokumentet

1.1 Formål med dokumentet

Dette dokument har til formål at beskrive de tiltag, der skal prioriteres ift. implementeringen af databeskyttelsesforordningen (GDPR) pr. 25. maj 2018, samt identificere øvrige nødvendige tiltag til iværksættelse løbende efter den 25. maj.

1.2 Revisionshistorik

Dokumentet er underlagt følgende revisionshistorik:

Version:	Dato	Person	Kommentar
0.1	20-03-2018	LLO	Første udkast til dokument
0.2	04-04-2018	LLO	Kommentarer efter gennemgang med MLM
0.3	05-04-2018	MLM	Tilføjelse af følgende: • Afsnit 'Dokumentation' • Afsnit 'Kommunikationsplan'
04	11-04-2018	MLM	Revidering af følgende: • Afsnit ´Beskrivelse af afdelingens arbejdsområder' • Afsnit ´Implementering' • Afsnit 'Kommunikationsplan' • Afsnit 'Dokumentation' Tilføjelse af følgende: • Afsnit 'Opfølgning' • Afsnit 'Risikovurdering'
05	19-04-2018	MLM	Ændringer på tværs af hele dokumentet efter gennemgang med henholdsvis Gitte Melph og Lars Lohmann, samt dialog med Thomas Krumbak
06	03-05-2018	MLM	Ændringer på tværs af hele dokumentet
07	09-05-2018	LLO	Kommentarer til risikoanalyse og opfølgning
08	23-05-2018	MLM	Gennemlæsning, korrektur mv.

2 Beskrivelse af afdelingens arbejdsområder i relation til GDPR

2.1 Afdelingen

Afdelingen Projekt og Systemforvaltning (POS) er en del af ITS på AAU og udgør "Build"-funktionen i ITS' "Plan-Build-Run"-organisation. POS har til ansvar at overtage fra "Plan", eksekvere på "Build" og overlevere til "Run".

POS er opdelt i tre ansvarsområder:

1. UDVIKLING
   Ansvarlig for udvikling af nye services og ydelser baseret på forskellige teknologier. Indbefatter bl.a.:
   - Udvikling af nye løsninger/produkter
   - Udvikling af apps
   - Udvikling af integrationer mellem nye og eksisterende systemer
   - Egen-udvikling såvel som sourcing i samarbejde med leverandører
2. SYSTEMFORVALTNING
   Ansvarlig for faglig og teknisk forvaltning af en række eksisterende it-løsninger samt medvirke til at implementere nye services og løsninger. Indbefatter bl.a.:
   - Analyse og teknisk rådgivning mv. ved implementering af nye it-løsninger
   - Håndtering af ændringer i eksisterende it-løsninger
   - Samarbejde med leverandører
   - Afvikling af services og løsninger
3. PROJEKTLEDELSE
   Projektledelse af strategiske, taktiske og operationelle it-projekter. Strategiske projekter er ledet af projektledere i selvstændig organisatorisk enhed, hvorimod andre projekter bliver ledet decentralt. Denne enhed definerer ITS' projektledelsesmodel og den kvalitet, som skal være i modellen.

Organiseringen i POS er ikke afgrænset af opgavetyper, dvs. udvikling kan foregå i systemforvaltning og vice versa.

2.2 Arbejdsområder der kræver særlig bevågenhed ift. GDPR

I POS-sammenhæng vurderes det, at følgende arbejdsområder kræver særlig bevågenhed for at kunne efterleve GDPR-krav:

#	Navn	GDPR indsats	Prioritet
001	Udviklingsproces	Der skal være etableret en ensartet udviklingsproces, og vi skal være i stand til at dokumentere udviklingsforløbet med sporbarhed til beslutningsprocessen.	Høj
002	Testdata	Brug af testdata skal kvalitetssikres via etablering af en formel teststrategi, som udstikker fælles retningslinjer for planlægning og gennemførsel af test på alle udviklingsopgaver i POS. Testdata må ikke kunne kompromittere personhenførbare oplysninger.	Høj
003	Deployment	Ved deployment af ny software skal det sikres, at der laves en vurdering af det enkelte build i forhold til sikkerhed, GDPR-krav (informationssikkerhed) samt væsentlige risici.	Høj

004	Afvikling af services	Ved afvikling af services skal POS sikre, at oprydning af data, sletning, mv. opfylder lovgivning ift. bevaring vs. overholdelse af GDPR. Dette skal indgå som en del af den indledende planlægning.	Lav
005	Sourcing	Ved samarbejde med eksterne leverandører, der er sourcet til at udføre en opgave, skal persondata sikres gennem oprettelse af databehandleraftale. Derudover ved kritisk vurdering af behovet for adgangsrettigheder, ved anonymisering af data mv.	Mellem
006	Integration (eksternt)	Integrationer til eksterne systemer (f.eks. til cpr-registeret) skal risikovurderes, og det skal sikres, at der er taget de nødvendige forholdsregler ift. overholdelse af GDPR-krav.	Høj
007	Service til samarbejdspartnere på AAU	Ved opgaveløsninger skal POS bistå samarbejdspartnere med rådgivning ift. overholdelse af GDPR-krav.	Mellem
008	Databehandleraftale	Der skal indgås databehandleraftaler med alle leverandører.	Mellem
009	Privatlivsfremmende teknologier	Der skal laves en risikovurdering af eksisterende it-systemer mht. anvendelsesgraden af privatlivsfremmende teknologi. Herunder skal der tages stilling til, om der er behov for at prioritere en sikkerhedsmæssig opdatering.	Mellem
010	Privacy by design	Der skal laves en vurdering af, om man i igangværende og planlagte it-projekter følger retningslinjer for privacy by design.	Mellem
011	Konsekvensanalyse	Ved projektarbejde skal projektlederen sikre, at der udføres en konsekvensanalyse mhp. at vurdere, om der er behov for særlige tiltag for at sikre efterlevelse af GDPR-krav. Varetagelse af denne opgave skal indgå i og dokumenteres via ITS' projektmodel.	Mellem
012	Plan for opfølgning	Der skal etableres processer og kontroller til fremtidig styring af brug af persondata i forbindelse med udvikling og test. Ledelsen i POS skal fastlægge kontrolmål og forestå opfølgning af disse.	Mellem
013	Risikovurdering	Ledelsen i POS skal overveje tiltag for at kunne reducere/imødegå risici i relation til håndtering af persondata.	Mellem
014	Kommunikationsplan	Ledelsen i POS skal varetage kommunikation i et omfang der sikrer, at alle medarbejdere i afdelingen bliver klædt på til at overholde krav og retningslinjer i relation til GDPR.	Høj

Tabel 1 Indsatsområder for POS

2.2.1 Uddybning af emnerne 'Privacy by Design', 'Privacy by Default' og 'Konsekvensanalyse'

Design foregår på alle niveauer. Opmærksomhed omkring sikkerhed skal spille sammen fra de første designskitser og hele vejen ned, til det sidste punktum er sat i den enkelte løsning eller det enkelte projekt.

Arkitekterne, der indgår i Plan-funktionen, som varetages af afdelingen Strategi og Proces, har hovedansvaret for at arbejde med sikkerhed i forbindelse med design af løsninger. I arkitekternes designproces og metoder er sikkerhedsaspektet allerede indbygget. Arkitekturprocessen TOGAF ADM

sikrer, at de i design ifbm. projekter (fast track og safe track) håndterer krav til sikkerhed, herunder GDPR-krav.

Som referencearkitektur for eksterne integrationer baserer arkitekterne deres arbejde på ABB (Architecture Building Block). Arkitekterne er desuden i gang med at udarbejde arkitekturprincipper, hvor første udkast planlægges at ligge klar i løbet af Q2 2018. Medarbejderne i POS skal kende og efterleve arkitekturprincipperne.

Udviklerne og systemforvalterne, der indgår i Build-funktionen, arbejder med løsningsdesign på et mere detaljeret niveau, f.eks. design af brugergrænseflader. Her skal de være særligt opmærksomme på at efterleve retningslinjer for *Privacy by Design* og *Privacy by Default*:

- Privacy by Design betyder at indtænke databeskyttelse i it-systemer og kaldes databeskyttelse gennem design. Der skal tages hensyn til persondatabeskyttelse og informationssikkerhed, når vi udarbejder nye eller ændrer eksisterende it-systemer.

- Privacy by Default betyder, at virksomheder skal indføre procedurer, der som standard sikrer, at der kun behandles persondata, som er nødvendig for hvert enkelt formål med behandlingen, og især at data ikke indsamles og opbevares ud over det nødvenlige tidsrum til de specifikke formål, og at de kun opbevares i det tidsrum, der er nødvendigt for at levere produktet eller servicen.

Projektlederne i Build-funktionen skal fremover, som et element i ITS' projektmodel, vurdere, om der er behov for særlige tiltag i tilknytning til at sikre efterlevelse af GDPR-krav. Analysen foretages tidligt i projektet og skal revurderes, når der justeres på designet undervejs. Denne konsekvensanalyse kaldes *Data Protection Impact Assesment*, eller *DPIA*:

- En DPIA er en vurdering af risici set fra et individs synspunkt, ved at en aktør behandler individets personoplysninger. DPIA'en består af en analyse og af en proces. Analysen sikrer, at de rette spørgsmål bliver stillet og besvaret. Processen sikrer, at spørgsmål stilles og svar gives på det rette tidspunkt i en teknologis livscyklus.

3 Implementering

3.1 Prioriterede indsatser frem mod den 25. maj

Grundet den tidsmæssige dimension er der behov for en prioritering af indsatserne hos POS frem mod 25. maj. Derfor vil alle indsatsområder med prioritet "høj" blive prioriteret således, at der som minimum er foranstaltninger på plads pr. 25. maj. Disse vil efterfølgende løbende blive dybere implementeret. Denne tabel indeholder en udspecificering af de prioriterede indsatser:

#	Navn	Foranstaltning pr. 25. Maj	Ansv.
001	Udviklingsproces	Følgende er på plads pr. 25. maj: a. En fælles udviklingsproces for alle udviklingsaktiviteter er defineret b. Udviklingsprocessen er dokumenteret i AAU-Håndbogen c. Der er udvalgt et værktøj til eksekvering/eksponering af udviklingsprocessen d. Produktteams er migreret fra andre værktøjer og over i den fælles udviklingsproces e. Projektteams benytter den fælles udviklingsproces	BHP

		f. Kode som leveres fra leverandører følger også den fælles udviklingsproces. Når ovenstående aktiviteter er gennemført, vil al udvikling, der resulterer i deployment af kode, følge den fælles udviklingsproces og herigennem være dokumenteret på en standardiseret måde.	
002	Testdata	Følgende er på plads pr. 25. maj: a. Der er udarbejdet en formel teststrategi, som bl.a. indeholder en oversigt over personfølsomme testdata samt retningslinjer for håndtering af disse. Teststrategien gælder for såvel egenudviklet kode som kode leveret af eksterne leverandører b. Der er udpeget en person, som har ansvaret for at sikre, at teststrategien overholdes c. Teststrategiens hovedbudskaber er formidlet til medarbejderne. Når ovenstående aktiviteter er gennemført, vil al test af kode være underlagt de rammer, som er udstukket i teststrategien.	GE
003	Deployment	Følgende er på plads pr. 25. maj: a. Der er fastlagt en proces for hvordan vi håndterer deployments med henblik på at kunne efterleve GDPR-krav b. JIRA er tilrettet således at hver enkelt deployment vurderes ift. sikkerhed, GDPR og væsentlige risici c. Denne proces for deployment er dokumenteret i AAU Håndbogen d. Der er lagt en plan for jævnlig opfølgning på processen e. Processen for deployment er formidlet til medarbejderne.	BHP/LLO
006	Integration (eksternt)	Følgende er på plads pr. 25. maj: a. Integrationer skal vurderes ift. sikkerhed, GDPR og væsentlige risici b. Der skal udarbejdes en kravliste, som eksterne integrationer skal opfylde angående sikker kommunikation	BHP/LLO
014	Kommunikationsplan	Følgende er på plads pr. 25. maj: a. Der er gennemført et afdelingsmøde med formidling i relation til GDPR-tiltag i POS b. Der er udarbejdet info-mails som understøtter formidling af GDPR-tiltag i POS c. Der er udarbejdet et info-site, som understøtter formidling af GDPR-tiltag i POS	MLM

Tabel 2 Prioriterede indsatsområder frem mod den 25. maj

GDPR-grunduddannelse

En formaliseret GDPR-grunduddannelse, som vil være obligatorisk for alle medarbejdere ved AAU, vil blive effektueret i Q2 og vil foregå gennem en række e-lærings-moduler. Ansvarlig for denne indsats er Gitte Melph/informationssikkerhedschef og Teia Melvej Stennevad/DPO. E-lærings-modulerne vil blive revideret hen ad vejen, og man vil til hver en tid kunne genbesøge dem.

3.2 Indsatser efter den 25. maj

Efter den 25. maj vil vi implementere de indsatsområder, der har fået prioriteten ”mellem” eller ”lav”.

#	Navn	Indsatser efter 25. maj	Ansv.
004	Afvikling af services	Ved afvikling af services skal POS sikre, at oprydning af data, sletning mv. opfylder lovgivning ift. bevaring vs. overholdelse af GDPR. Dette skal indgå som en del af den indledende planlægning.	
005	Sourcing	Ved samarbejde med eksterne leverandører, der er sourcet til at udføre en opgave, skal persondata sikres gennem oprettelse af databehandleraftale. Derudover ved kritisk vurdering af behovet for adgangsrettigheder, ved anonymisering af data mv.	
007	Service til AAU	Ved opgaveløsninger skal POS bistå samarbejdspartnere med rådgivning ift. overholdelse af GDPR-krav.	
008	Databehandleraftale	Der skal indgås databehandleraftaler med alle leverandører.	
009	Privatlivsfremmende teknologier	Der skal laves en risikovurdering af eksisterende it-systemer mht. anvendelsesgraden af privatlivsfremmende teknologi. Herunder skal der tages stilling til, om der er behov for at prioritere en sikkerhedsmæssig opdatering.	
010	Privacy by Design	Der skal laves en vurdering af, om man i igangværende og planlagte it-projekter følger retningslinjer for Privacy by Design.	
011	Konsekvensanalyse	Ved projektarbejde skal projektlederen sikre, at der udføres en konsekvensanalyse mhp. at vurdere, om der er behov for særlige tiltag for at sikre efterlevelse af GDPR-krav. Varetagelse af denne opgave skal indgå i og dokumenteres via ITS’ projektmodel.	
012	Plan for opfølgning	Der skal etableres processer og kontroller til fremtidig styring af brug af persondata i forbindelse med udvikling og test. Ledelsen i POS skal fastlægge kontrolmål og forestå opfølgning af disse.	
013	Risikovurdering	Ledelsen i POS skal overveje tiltag for at kunne reducere/imødegå risici i relation til håndtering af persondata.	

Tabel 3 Indsatsområder efter den 25. maj

4 Risikovurdering

Gennem forløbet er der blevet afdækket følgende risici i forbindelse med GDPR-aktiviteter. Perspektivet er i denne risikoanalyse efter 25. maj, dvs. en driftssituation.

Risikoregister

ID	Risikokategori	Risikobeskrivelse	Sandsyn	Konsekver	I alt	Risikoreaktion	Risikostatus	Risikoejer
1.	Kvalitet	Der er en risiko for manglende fokus fra medarbejdere og ledelse på lang sigt, hvilket medfører, at tiltag ikke overholdes, og POS ikke følger etablerede processer	3	4	12	Mitigeringsplan: 25-05-2018: Der etableres en kommunikationsplan for perioden efter 25. maj 01-06-2018: Der etableres ledelsesinformation ift. GDPR 15-06-2018: Der etableres KPI for opfølgning af processer	Behandles	LLO
2.	Omfang	Der er en risiko for manglede kendskab til regler i relation til GDPR blandt medarbejdere og ledelse, hvilket medfører manglende overholdelse	2	4	8	Mitigeringsplan: 16-05-2018: FK afholder ITS møde om GDPR 18-05-2018: Der afholdes informationsmøde i POS om GDPR 27-05-2018: Informationssite lanceres 15-06-2018: Mail vedr. GDPR Q3: KPI vedr. GDPR offentliggøres	Behandles	LLO
3.	Omfang	Der er en risiko for at studentermedhjælpere og nye medarbejdere ikke får kendskab til reglerne, hvilket medfører manglende overholdelse af regler	2	5	10	Mitigeringsplan: 25-05-2018: POS ledelsen sikrer, at nye medarbejdere bliver orienteret om processer, som en del af introduktionen	Behandles	BHP, GE
4.	Omfang	Der er en risiko for at medarbejdere er usikre på krav og rammer for implementering af GDPR, hvilket medfører, at disse ikke følges	3	2	6	Mitigeringsplan: 16-05-2018: FK afholder ITS møde om GDPR 18-05-2018: Der afholdes informationsmøde i POS om GDPR 27-05-2018: Informationssite lanceres 15-06-2018: Mail vedr. GDPR Q3: KPI vedr. GDPR offentliggøres	Behandles	LLO

Tabel 4 Risici i forbindelse med GDPR-aktiviteter i POS

Den væsentligste risiko, der p.t. er identificeret, er, at den opmærksomhed og forståelse, der er for GDPR, lige så stille glider i baggrunden, og POS returnerer til at gøre tingene, "som vi plejer". Den kortsigtede mitigeringsplan er information og kommunikation, mens den langsigtede mitigeringsplan er ledelsesinformation, monitorering gennem KPI og procesefterlevelse. *Mitigering betyder at mildne. Det kan man gøre på 2 måder: Enten ved at gøre sandsynligheden for at risikoen udløses mindre, eller ved at sørge for, at skulle risikoen blive udløst, vil effekten være knapt så katastrofal.*

5 Opfølgning

Når vi har overblik over relevante GDPR-krav, vil vi have bedre mulighed for at designe løsninger, hvor enkelte processer eller kontroller bidrager til at opfylde flere kontrolmål. Klart definerede arbejdsprocesser, der følges op med faste intervaller, minimerer risikoen for fejl og dermed uønskede hændelser.

Som led i mitigeringen for flere risici i risikoanalysen vil POS derfor tage følgende træk:

- Udarbejde systematisk ledelsesinformation, der behandles 2 gange månedligt
- Udarbejde specifikke KPI'er, der monitorerer om, hvorvidt processer eksekveres og overholdes
- Specifikt tiltag vedr. CAB-møder og dokumentation af disse.

6 Kommunikationsplan

Det overordnede formål med denne kommunikationsplan er at sikre, at alle i POS modtager orientering og trækker i samme retning for at opnå de ønskede resultater. Målet er, at medarbejderne i afdelingen bliver i stand til at overholde krav og retningslinjer i GDPR.

Vi starter med disse tiltag for at komme i gang med GDPR.

#	Hvad skal kommunikeres	Hvordan – hvilke platforme og medier	Hvornår	Ansvarlig
a.	• Orientering om GDPR-tiltag i POS • Vi registrerer de spørgsmål, der bliver stillet på mødet for efterfølgende at lade dem indgå som en FAQ på info-sitet	Afdelingsmøde	18. maj	LLO
b.	• URL på info-site ligger klar med det første indhold på sitet	Info-site	18. maj	MLM

c.	• Tak for interesse og spørgsmål på mødet • Her er igen URL til info-site inklusive en gentagelse af budskabet om, at alle skal sætte sig ind i stoffet • Invitere til at feedback er velkommen. Vi har nok ikke ramt plet i første skud, og vi skal hjælpes ad med at få vores metoder kvalificeret yderligere efterhånden som GDPR-tiltag tages i anvendelse	Info-mail	22. maj	MLM og MFW
d.	• Reminder, nu gælder det	Info-mail	28. maj	MLM og MFW
e.	• Journalisering af dokumentation for kommunikation i workzone		Ultimo maj	MLM
f.	Kvartalsvis reminder – review af indhold på info-site	Intranet		LLO
g.	Tilretning af beskrivelse af udviklingsproces	AAU-Håndbogen	Ultimo maj	BHP, KA og MLM
h.	En indsats til POS-ledelsen om kommunikation verbalt		Ad hoc	
i.	En indsats til projektledelsen om, at de er en del af ledelseslaget i denne beslutning		Ad hoc	

Tabel 5 Kommunikations for POS

7 Dokumentation

Dokumentation for indsatsområder med prioriteten ”høj”.

#	Navn	Foranstaltning pr. 25. Maj	Ansv.
001	Udviklings-proces		BHP
	A	En fælles udviklingsproces for alle udviklingsaktiviteter er defineret *Dette krav er mødt. Der er udarbejdet en fælles proces, som er udførligt dokumenteret i værktøjet Confluence:* *https://confluence.its.aau.dk/pages/viewpage.action?spaceKey=AIU&title=Proces+for+softwareudvikling*	
	B	Udviklingsprocessen er dokumenteret jf. AAU-Håndbogen *Dette krav er mødt. Udviklingsprocessen er dokumenteret i AAU-Håndbogen under revisionskontrol: http://www.haandbog.aau.dk/dokument/?contentId=348312*	
	C	Der er udvalgt et værktøj til at eksekvere processen i *Dette krav er mødt. Alle udviklingsrelaterede opgaver registreres i JIRA. Det sikrer transparens af deres status, om de afventer behandling, om de er i gang med at blive behandlet, eller om de er færdigbehandlet. Rapportering støtter styring af et udviklingsforløb, så der konstant er overblik over, hvor en opgave befinder sig – det giver samtidig mulighed for at dykke ned i detaljerede informationer omkring den enkelte opgave. Udførlig beskrivelse af processen er dokumenteret i værktøjet Confluence:* *https://confluence.its.aau.dk/display/AIU/Proces+for+deployment*	
	D	Produktteams er migreret over i ny udviklingsproces fra andre værktøjer *Konverteringsoversigten kan ses her:* *https://confluence.its.aau.dk/display/AIU/Proces+for+softwareudvikling*	
	E	Projektteams benytter denne proces *Konverteringsoversigten kan ses her:* *https://confluence.its.aau.dk/display/AIU/Proces+for+softwareudvikling*	
	F	Kode fra leverandører gennem sourcing følger processen *Kode fra leverandører følger testproces jf. den fælles udviklingsproces:* *http://www.haandbog.aau.dk/dokument/?contentId=348312*	
002	Testdata		GE
	A	Der er udarbejdet en formel teststrategi, som bl.a. indeholder en oversigt over personfølsomme testdata samt retningslinjer for håndtering af disse. Teststrategien gælder for såvel egenudviklet kode som kode leveret af eksterne leverandører. *Teststrategi er udarbejdet.*	

	B	Der er udpeget en person, som har ansvaret for at sikre, at teststrategien overholdes *I POS er der etableret en rolle som Test Manager. Rollen varetages af Daniela Ivana.*	
	C	Teststrategiens hovedbudskaber er formidlet til medarbejderne. *Jf. kommunikationsplan i dette dokument.*	
003	Deployment		
	A	Der er fastlagt en proces for, hvordan vi håndterer deployments med henblik på at kunne efterleve GDPR-krav *https://confluence.its.aau.dk/display/AIU/Proces+for+deployment*	
	B	JIRA er tilrettet således, at hver enkelt deployment vurderes ift. sikkerhed, GDPR og væsentlige risici *https://confluence.its.aau.dk/display/AIU/Proces+for+deployment*	
	C	Denne proces for deployment er dokumenteret i AAU-Håndbogen *http://www.haandbog.aau.dk/dokument/?contentId=348312*	
	D	Der er lagt en plan for jævnlig opfølgning på processen ▪ *Udarbejde systematisk ledelsesinformation der behandles 2 gange månedligt* ▪ *Udarbejde specifikke KPI'er der monitorerer om, hvorvidt processer eksekveres og overholdes* ▪ *Specifikt tiltag vedr. CAB-møder og dokumentation af disse.*	
	E	Processen for deployment er formidlet til medarbejderne. *Jf. kommunikationsplan i dette dokument.*	
006	Integration		
	A	Integrationer skal risikovurderes ift. sikkerhed og persondata *POS har udvidet deployment-processen til at omfatte dette.*	
	B	Der skal udarbejdes en kravliste, som eksterne integrationer skal opfylde angående sikker kommunikation *Opgaven er en del af designprocessen, som varetages i Plan og er derfor opfyldt for POS.*	

Tabel 6 Dokumentation for indsatsområder for POS

Se generel information om håndteringen af persondata på AAU på www.persondata.aau.dk.