1. Netværksmøde Nøglemedarbejdere

Teia Melvej Stennevad

AALBORG UNIVERSITET

Dagsorden

- Rammerne for implementeringsprojektet
- Foreløbig projektplan
- Nøglemedarbejdere
- Lovgrundlaget: Databeskyttelsesforordningen og Databeskyttelsesloven
  - Vigtige begreber
  - Udvalgte artikler
- Afrunding

Dagsorden

- Rammerne for implementeringsprojektet
- Foreløbig projektplan
- Nøglemedarbejdere
- Lovgrundlaget: Databeskyttelsesforordningen og Databeskyttelsesloven
  - Vigtige begreber
  - Udvalgte artikler
- Afrunding

Rammerne for implementeringsprojektet

- Deadline 25. maj
- Tæller vi timerne sammen på de nuværende medarbejder, har vi ca. 5 på fuldtid

- Opgaverne bliver rammesat fra centralt hold, men de skal i høj grad løses ude i organisationen – der hvor databehandlingen sker…
  - Driftsansvaret kommer også i høj grad til at skulle løftes ude i organisationen

- Udgangspunktet er at kommet i mål med de kritiske opgaver per 25. maj
  - Derefter kommer implementeringen af lang række af andre opgaver, samt idriftsættelse af det persondataretslige regelsæt
  - Eksempler på driftsopgaver:
    - For systemejere: kontrol af databehandlere
    - For autorisationsansvarlige: kontrol af brugerautorisationer
    - For procesansvarlige: kontrol af behandlingsaktiviteter
    - M.fl.

Holdet – so far

- **Holdet består af:** ***(fra oven)***
  Sabine Jensen Jåtog (Projektleder)
  Gitte Melph (CISO)
  Anne Kielgast (Specialkonsulent)
  Rainer Bohm (IT-arkitekt)
  Kicki Damtoft (Studentermedhjælper - Jura)
  Karsten Kryger (Specialkonsulent)
  Teia Melvej Stennevad (DPO)
  Kathrine Tvorup Pajkes (Specialkonsulent)
  Maria Langendorff Hansen (Overassistent)
  Niels Dahl Thellufsen (Specialkonsulent)

- Jeg er den eneste på fuldtid til projektet. Der er et par stykker på 80%, mens resten er på mellem 10% og 50%

Foreløbig projektplan

De opgaver I (især) vil blive involveret i:

- Fortegnelser over behandlingsaktiviteter – *igangværende*
  Fra centralt hold er vi i færd med at lave kvalitetskontrol af fortegnelserne, inden vi sender jer videre med næste opgave

- GAP-analyser af jeres behandlingsaktiviteter
  Vi er ved at udfærdige materialet, der skal være grundlaget for GAP-analyserne, herunder: Afdækning af særlovgivning og regler, der påvirker hvordan personoplysninger skal behandles; planlægning af Åbent Kontor arrangementer; udfærdigelse af vejledning/skema

- Udfærdigelse af handlingsplaner for behandlingsaktiviteter, der ikke kan leve op til reglerne i GDPR

Tidsplanen er afhængig af, hvordan vores ressourcesituation ser ud/forbedrer sig. Vi er underbemandet ift. de medarbejdere, vi bør være for at komme godt i mål, så derfor kan jeg ikke sætte tidsramme på

Andre opgaver der skal løses

- Projektgruppen arbejder for indeværende med:
  - Udfærdigelse af samtykkeskabelon og vejledning til anvendelse af skabelonen
  - Skabeloner til Databehandleraftaler
  - Afdækning af eksterne parter vi skal have indgået/revurderet databehandleraftaler med
  - Skabelon og vejledning til efterlevelse af AAU's oplysningspligt
  - Vejledning i behandling af personoplysninger
  - Skabelon til udførelse af DPIA, herunder afklaring af klassificeringsmodel samt en AAU-specifik vejledning
  - Beredskabs-set-up herunder beredskabsplan, skabelon til hændelsesrapport og skabelon til anmeldelse til Datatilsynet og underretning til de registrerede
  - Opsætning af GDPR-modul i ISMS-løsning samt udarbejdelse af brugervejledning
  - Planlægning af uddannelsesmoduler: basismodul samt sær-moduler
  - Revidering af Informationssikkerhedspolitik samt udarbejdelse af Informationssikkerhedshåndbog
  - Indkøb og implementering af logningsløsning
  - Implementering af 2-faktor autentificering
  - Implementering/etablering af detektionsløsning
  - Etablering af storage-løsning til forskningsdata
  - Teknisk set-up for modtagelse af anmodning fra registrerede
  - Set-up for dokumentation af behandlingsaktiviteter indenfor forskning
  - M.fl.

Input til debat: Klassificeringsmodel

- Der er for indeværende udarbejdet den liste I arbejdede ud fra ift. fortegnelserne (Vejledning til Personoplysninger) http://www.informationssikkerhed.aau.dk/artikel-30/
- Her arbejdes med kategorierne:
  - Almindelige Personoplysninger
  - Fortrolige Personoplysninger
  - Straffedomme og Lovovertrædelser
  - Følsomme Personoplysninger
- Giver 'kategorierne' mening for jer (tænk her især den 'fortrolige' kategori)?
  - Info: indenfor andre danske love arbejder man med kategorierne 'fortrolige' og 'ikke-fortrolige'
  - Under den nuværende lovgivning kalder man kategorien for semi-følsomme

Nøglemedarbejdere

- Nøglemedarbejdere – samt de ledere der har udnævnt jer – er de AAU ansatte, der skal stå for den praktiske koordinering af GDPR-opgaver ude i organisationen
  - Det er ikke sikkert, det er jer, der skal stå for at løse opgaverne, men det er noget, I selv skal koordinere ude i jeres område/afdeling/mm.
- Det er nøglemedarbejderen, vi sender opgaverne/skemaer/vejledninger ud til
- Det kræver ingen særlige persondataretslige talenter at være nøglemedarbejder – faktisk er et godt kendskab til den del af organisationen, man arbejder i, den primære evne, man bør have
- Dertil skal man kunne koordinere opgaver

Nøglemedarbejder --- Superbruger

- Når vi kommer efter implementeringsfasen, vil der være brug for decentrale superbrugere, da der kun er én af mig og ca. 4.500 kolleger, jeg skal forsøge at hjælpe – det kan godt ende op med utålelig lang behandlingstid på selv små spørgsmål

- Superbrugere vil blive tilbudt kvalificerende opgradering, uddannelse, viden mm. så de er klædt på til at giverådgivning om den daglige/basis behandling af personoplysninger

- Tag en velovervejet snak med jeres leder om det skal være jer… Har I lyst? Er i den bedste til opgaven i jeres område/afdeling/mm.?

Lovgrundlaget

- Databeskyttelsesforordningen bliver suppleret af en dansk Databeskyttelseslov, der forventes at bliver vedtaget i slutningen af februar:
  Databeskyttelsesforordningen
  Databeskyttelsesloven - udkast
- Dertil kommer en lang række af særlove og regler, som i høj grad påvirker, hvordan AAU skal behandle personoplysninger – nogle af dem er også sendt til behandling på ændringsforslag:

  Arkivloven
  Sundhedsloven
  CPR-loven
  Regnskabsloven
  Krav til videnskabelig uredelighed
  Myndighedsudøvelse
  M.fl.

Databeskyttelsesforordningen - GDPR
Hvad er det?

Man ønskede med GDPR at få udskiftet forældet national lovgivning samt at:

- Beskytte EU borgeres grundlæggende rettigheder – herunder frihedsrettighederne
- Sikre den frie udveksling af personoplysninger
- Sikre ensartet anvendelse og håndhævelse af databeskyttelsesreglerne i EU

- Føre til administrative lettelser:
  - Harmonisering og simplificering af myndighedsstruktur
  - Effektivisering af myndigheders samarbejde

GDPR
Hvad er det nye?

- Vi vil i praksis opleve en del skærpelser. Ikke nødvendigvis fordi der kommer ny lovgivning, men fordi der kommer mere fokus på området og muligheder for sanktioner, så vi får et større incitament for at efterleve gældende lovgivning, herunder:
  - Retten til at blive glemt
  - Dokumentationskrav
  - Dataminimering
  - Samtykke
  - Privacy by Design
  - Privacy by Default

- Sanktioner: Der er kommet ca. 16 mio gode grunde på bordet, til at vi skal følge lovgivningen – *dette er dog ikke eneste sanktionsmulighed*

GDPR
Vigtige begreber

- Der er en række centrale begreber, der anvendes ofte i forbindelse med persondatabeskyttelse:
  - Personoplysninger
  - Behandling
  - Dataansvarlig
  - Databehandler
  - Den registrerede

Personoplysninger

- Enhver form for information om en identificeret eller identificerbar fysisk person også kaldet *den registrerede* Art. 4 (1)

- Ved identificerbar person forstås en person, der direkte eller indirekte kan identificeres med eller uden brug af hjælpemidler, navnlig ved en identifikator (navn, id-nummer, lokaliseringsdata, online-id) eller et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.
  - De hjælpemidler "der med rimelighed kan tænkes bragt i anvendelse" skal med i vurderingen af, om man behandler personoplysninger

- Irreversibelt anonymiseret data er ikke omfattet
  - Læs mere om specifikationerne for anonymisering på Datatilsynets hjemmeside, der refererer til Artikel 29-gruppens redegørelse
  - OBS: at anonymisere data er ikke så let som det lyder…
- IP-adresser (både statiske og dynamiske) er omfattet:
  - Se EU-dom: C-582/14
- Link til dokument om personoplysninger på AAU's hjemmeside

Behandling

- Ordet behandling dækker over: ”enhver aktivitet eller række af aktiviteter – med eller uden brug af automatiseret databehandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for…” Art. 4 (2)
  - Indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændringer, genfinding, søgning, brug, videregivelse ved fremsendelse, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse

- Så bare det, at man har eller giver nogle ‘se-adgang’ til personoplysninger, så bevirker det, at der behandles personoplysninger, og hvis den anden part er en ekstern tredjepart, der agerer på vegne af f.eks. AAU, så skal der indgås en databehandleraftale
  - Agerer tredjeparten på egen vegne og behandler personoplysninger til egne formål, så er de selv dataansvarlige, og der vil i disse tilfælde være tale om en videregivelse af personoplysninger fra én dataansvarlig til en anden dataansvarlig

Dataansvarlig, databehandler og den registrerede

Dataansvarlig:

- Art. 4 (7) en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger
- F.eks. udbyder af varer eller tjeneste ydelser, eller en arbejdsgiver
- Der kan være flere dataansvarlige

Databehandler:

- Art. 4 (8) en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler oplysninger på den dataansvarliges vegne
- F.eks. Service provider, hosting-firma, samarbejdspartner ved forskningsprojekter

Den registrerede

- Art. 4 (1)
- Personen/datasubjektet om hvem der behandles data
- Det er den registrerede, der ejer sine data, og dette ejerskab kan ikke overdrages til en dataansvarlig

Dataansvarlig, databehandler og den registrerede

- Medarbejdere ved AAU er aldrig selv dataansvarlige, når vi behandler AAU's data til AAU's formål. Vi er 'autoriserede medarbejdere' – *hvis vi vel at mærke behandler oplysningerne, som led i vores arbejdsopgaver!*
  - Man har fået opgaven uddelegeret af AAU - til at handle på vegne af AAU, som er den dataansvarlige
  - Det er AAU, der står med ansvaret og pligterne overfor de registrerede

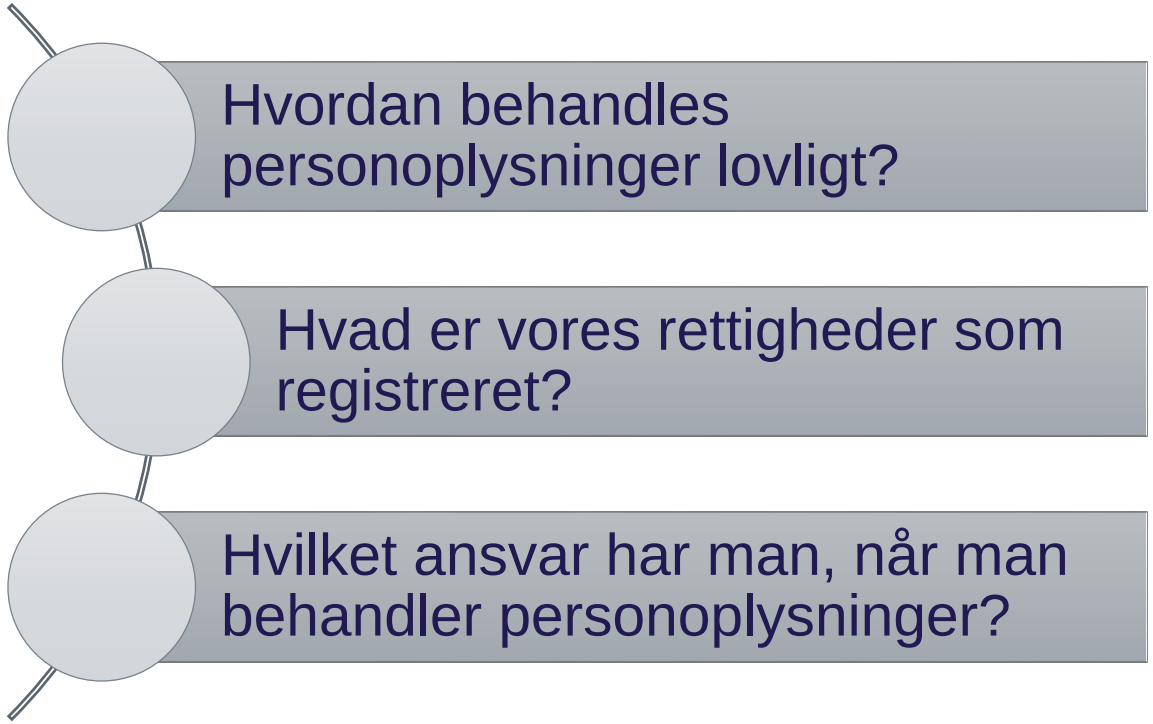
- Hvis medarbejderne selv er dataansvarlig, så er der tale om private projekter, som AAU ikke skal tage ansvar for, lægge udstyr til, stille garantier for mv.

- **OBS:** dataansvar har INTET med ophavsret at gøre – det er en helt anden boldgade
  Der tales ofte om dataejerskab: man kan ikke eje personoplysninger om andre, man kan kun have dataansvar. Termen dataejerskab kan kun referere til data, der ikke indeholder personoplysninger

GDPR
I praksis

Man kan groft sagt inddele forordningen i 3 hovedområder:

Hvert hovedområde definerer en række krav, vi skal kunne efterleve og dokumentere – især men ikke udelukkende afsnittet om *Dataansvarliges pligter*



Lovlig behandling

Hvordan behandles personoplysninger lovligt?

Artikel	Indhold
5	Principper for behandling af personoplysninger
6	Lovlig behandling af almindelige personoplysninger
7	Betingelser for samtykke
8	Lovlig behandling af oplysninger om børn
9	Lovlig behandling af følsomme oplysninger
10	Lovlig behandling vedr. straffedomme mv.
11	Behandling der ikke kræver identifikation

Behandlingsprincipperne

- Behandlingsprincipperne i Artikel 5 definerer, at personoplysninger skal:
  - Behandles lovligt, rimeligt og gennemsigtigt (**saglighed**)
  - Indsamles til udtrykkeligt angivne og legitime formål, og må ikke viderebehandles på en måde, der er uforeneligt med disse formål (**formålsbestemthed**)
  - Være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt ift. de formål, hvortil de behandles (**dataminimering**)
  - Være rigtige og om nødvendigt ajourførte (**rigtighed**)
  - Skal opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt (**lagringsbegrænsning**)
  - Behandles på en måde, der sikre tilstrækkelig sikkerhed (**integritet og fortrolighed**)

Artikel 5 vil påvirke opgaveløsningen på en del områder:
- Den tekniske understøttelse skal være med til at sikre integritet og fortrolighed
- Der skal laves delpolitikker og vejledninger for dataminimering og lagringsbegrænsninger
- Medarbejdere skal oplæres i at definere saglighed og formålsbestemthed
- mm

Lovlig behandling
Artikel 6 og 9

- Hjemmelsgrundlag – *ikke udtømmende:*

Hjemmel	Almindelige	Følsomme
Samtykke	Ja	Ja
For at indgå eller opfylde en aftale med den registrerede	Ja	Nej
Lovkrav	Ja	Ja
Nødvendig for at fastslå lovkrav	Ja	Ja
Offentliggjort af den registrerede	Ja	Ja
Interesseafvejningsreglen	Ja	Nej

- *OBS: Interesseafvejningsreglen gælder ikke for offentlige institutioner*

Samtykke
Artikel 7

- … *en frivillig, specifik, informeret og utvetydig viljestilkendegivelse*… hvormed den registrerede tilkendegiver, at man som Dataansvarlig må behandle deres personoplysninger

- Det påligger den Dataansvarlige at kunne påvise, der er indsamlet korrekt samtykke

- Dertil skal den registrerede informeres om:
  - Dataansvarliges identitet
  - Formålet med behandlingen

- Det kunne påvises, at den registrerede havde et reelt og frit valg

Registreredes rettigheder

Hvad er vores rettigheder som registreret?

Artikel	Indhold
12	Transparens og letforståelig kommunikation
13 – 14	Oplysningspligt ved indsamling af oplysninger
15	Ret til indsigt
16	Ret til berigtigelse
17	Retten til at blive glemt
18	Ret til begrænsning af behandling
19	Underretningspligt (ved berigtigelse, sletning eller begrænsning)
20	Ret til dataportabilitet
21	Ret til at gøre indsigelse
22	Automatisk beslutningstagning og profilering

Gennemsigtighed og nærmere regler
Artikel 12

- Transparens mm. I relation til udøvelsen af Art. 13 – 14

- Der findes krav til måden, hvorpå vi kommunikerer med de registrerede ift. oplysningspligten og den registreredes ret (Art. 15 – 22)
  - Kortfattet, gennemsigtig, letforståelig, lettilgængelig, klart og enkelt sprog
  - Oplysningerne skal gives skriftligt eller med andre midler, hvis det er det mest hensigtsmæssige

- Tidsfrister
  - Svartider uden ugrundet ophold og senest inden for en måned, dog med mulighed for forlængelse under særlige omstændigheder

- Økonomi:
  - Udgangspunkt: de registrerede skal ikke afholde udgifter i forbindelse med deres anmodninger
  - Grundløse eller overdrevne anmodninger
    - Disse kan enten afvises eller der kan opkræves et rimeligt gebyr under hensyntagen til administrative byrder
    - Bevisbyrden for at afvise en anmodning som grundløs eller overdrevne påligger den Dataansvarlige

Oplysningspligt
Artikel 13 og 14

- Differentieret efter om oplysningerne er direkte indsamlet ved den registrerede, eller om de er indsamlet ved tredjepart

- Udgangspunktet er, at den registrerede skal oplyses om følgende:
  - Kontaktoplysninger til og identitet på den dataansvarlige og eventuel repræsentant
  - Kontaktoplysninger på evt. DPO
  - Formål og hjemmel for behandlingen
  - Kategorier af oplysninger
  - Hvilke kategorier af oplysninger der behandles, og hvor de stammer fra
  - Vedr. profilering og automatiske beslutninger: betydning og de forventede konsekvenser af behandlingen
  - Eventuelle modtagere eller kategorier af modtagere
  - Hvor længe oplysningerne skal behandles (hvis dette ikke er muligt skal der oplyses hvilke kriterier det anvendes til at fastsætte behandlingstiden)
  - Den registrerede skal oplyses om sine rettigheder ift. f.eks. Indsigtsret, sletteret mv. (se artikel 15 – 22)
  - Den registrerede skal oplyses om retten til at tilbagekalde samtykke samt mulighed for at klage
  - Hvis data overføres til tredjelande skal den registrerede informeres om beskyttelsen ifb. med overførsel

Ret til indsigt og berigtigelse
Artikel 15 og 16

- Ret til indsigt
  - Den registrerede har ret til at få bekræftet, om personoplysninger behandles, og i givet fald få adgang til oplysningerne, samt de samme informationer som bliver givet når dataansvarlig udøver sin oplysningspligt

- Ret til berigtigelse
  - Den registrerede kan kræve, at den dataansvarlige uden unødig forsinkelse berigtiger urigtige oplysninger
  - Den registrerede har under hensyn til formålene med behandlingen ret til at få kompletteret ufuldstændige personoplysninger bl.a. ved at fremlægge en supplerende erklæring

Der findes undtagelser til alle disse regler, og der vil være tilfælde, hvor den registrerede ikke kan få lov til at udøve sine rettighede – der skal laves AAU retningslinjer til medarbejderne, så de kan modtage og behandle anmodning fra de registrerede korrekt ift. hovedreglerne og undtagelserne, så vi ikke imødekommer anmodninger vi ikke er pligtige til at behandle.

Ret til sletning
Artikel 17

- AAU skal som Dataansvarlig *uden ugrundet ophold* slette i flg. situationer:
  - Personoplysningerne er ikke længere nødvendige henset til formålet eller behandlingen er ulovlig
  - Den registrerede tilbagekalder sit samtykke, og der er ikke en anden hjemmel (enten i GDPR eller i anden særlovgivning)
  - Opbevaringsperioden er udløbet

AAU skal have skabt overblik over de personoplysninger vi behandler herunder:
- Hvor længe en behandling er nødvendig – en konkret vurdering:
  - Formål med behandlingen
  - Oplysningens karakter
  - Typen af registreret
  - Anden lovgivning
- Kan i nogle tilfælde defineres i et aftaleforhold:
  - F.eks. Aftalens løbetid og et tidsrum derefter
- En defineret slette-politik: sørg for at have en holdning og dokumenter retningslinjerne
  - Det er bedre at have en dokumenteret holdning, der bliver kendt ugyldig end slet ikke at have en holdning

Ret til sletning - fortsat

Hvor længe er det nødvendigt at opbevare data?

- Der skal foretages en konkret vurdering baseret på:
  - Formål med behandlingen
  - Oplysningens karakter (alm. eller følsom)
  - Typen af registrerede
  - Anden lovgivning

Der skal udarbejdes en slettepolitik med retningslinjer, der tilgodeser særregler mv. indenfor de forskellige forretningsområder

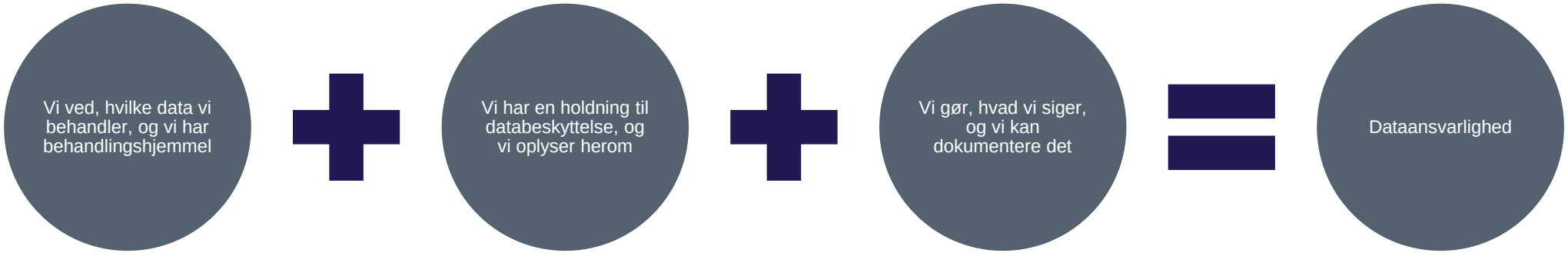
Dataansvarliges pligter

Hvilket ansvar har man, når man behandler personoplysninger?

Artikel	Indhold
24	Generalklausul om ansvarlighed
25	Databeskyttelse gennem design og standardindstillinger
26	Fælles dataansvarlige
28	Databehandlere
30	Dokumentation for behandling
31	Samarbejde med Datatilsynet
32	Behandlingssikkerhed
33 – 34	Anmeldelse af brud på datasikkerheden
35 – 36	Risikoanalyse
37 – 39	Databeskyttelsesrådgiver (DPO)

Den dataansvarliges ansvar
Artikel 24

- Generalklausul om dataansvarlighed/accountability
- Dataansvarlige skal indføre foranstaltninger for at **sikre** og være i stand til at **dokumentere** overholdelse af forordningen:



Databehandleraftaler
Artikel 28

- Skal indgås når den dataansvarlige vælger at overlade behandlingen til en anden, ekstern part
  - F.eks. outsourcing, hosting, drift, datasammenstilling (forskning), SLA (Serviceaftale) mm.
- Dataansvarlige bør kun vælge databehandlere, som kan levere den fornødne behandlingsgaranti ift. de tekniske og organisatoriske sikkerhedsforanstaltninger, overholdelse af lovgivning samt iagttagelse af den registrerede rettigheder
- Handler databehandleren uden instruks pådrager de sig selvstændigt dataansvar – *dog ulovligt*
- Ønsker en Databehandler ikke at underskrive en DBA, anbefales det at finde en anden Databehandler til at løse opgaven/en anden leverandør

Vi skal gennemgå alle gamle databehandleraftaler
Vi skal indgå databehandleraftaler, der hvor de mangler
OG: der skal følges op med årlige kontroller af databehandlere mht. deres sikkerhedsforanstaltninger

Databehandleraftale - fortsat

- En DBA skal som minimum indeholde følgende:
  - Instruksbeføjelse
  - Personer, der foretager behandling, skal være underlagt tavshedspligt
  - Iværksætte alle foranstaltninger i henhold til Art. 32
  - Brug af under-databehandlere kræver forudgående tilladelse fra Dataansvarlige (der gælder samme regler for under-databehandlere som databehandlere generelt)
  - Databehandleren skal bistå den Dataansvarlige med at overholde reglerne
  - Databehandleren skal overdrage alle resultater til Dataansvarlige efter endt behandling samt ophøre med behandling og slette alle kopier medmindre der følger andet af lovgivning (GDPR eller særlove)
  - Stille al nødvendig information til rådighed for Dataansvarlige, dennes repræsentant eller Datatilsynet

Der bliver udarbejdet AAU standarder – der er behov for flere, da de aftaleforhold vi indgår i er forskellige og skal detaljereguleres på forskellig måde

Fortegnelser
Artikel 30

Fortegnelser over behandlingsaktiviteter: (Dokumentation for behandling)

- Vi skal (både som Dataansvarlig og Databehandler) kunne dokumentere følgende til Datatilsynet:
  - Navn og kontaktoplysninger for den dataansvarlige (den fælles dataansvarlige, den dataansvarlige repræsentant og DPO'en)
  - Formålene med behandlingen
  - Kategorier af registrerede og kategorier af personoplysninger
  - Kategorier af modtagere
  - Eventuel overførsel til tredjeland
  - Hvor det er muligt: de forventede tidsfrister for sletning
  - Hvor det er muligt: en generel beskrivelse af sikkerhedsforanstaltningerne

Anmeldelse til Datatilsynet
Artikel 33

Anmeldelsespligt ved sikkerhedsbrud

- I tilfælde af sikkerhedsbrud, hvor personoplysninger er blevet kompromitteret, skal dataansvarlige uden unødig forsinkelse og ***indenfor 72 timer*** underrette Datatilsynet efter at være kommet til kendskab med sikkerhedsbruddet
  - En databehandler skal uden ophold notificere den dataansvarlige

- Anmeldelsen skal bl.a. omfatte:
  - Karakterne af sikkerhedsbrud samt dataomfang
  - Angive tiltag for at begrænse skaderne
  - Beskrive konsekvenserne ved sikkerhedsbruddet
  - Dokumentere omstændighederne ved sikkerhedsbruddet

- Undtagelse: Der skal ikke ske underretning, hvis der er usandsynligt, at sikkerhedsbruddet fører til en risiko for fysiske personers rettigheder eller frihedsrettigheder – læser man udtalelsen som KU fik i forbindelse med et sikkerhedsbrud, så er det meget få sikkerhedsbrud, der ikke skal anmeldes
  - Dette er f.eks. I de tilfælde man har sikret tilstrækkelig med kryptering, således der ikke er mulighed for at kompromittere oplysningernes fortrolighed

Underretning til den registrerede
Artikel 34

Underretningspligt ved sikkerhedsbrud

- Hvis et sikkerhedsbrud kan forventes at føre til en høj risiko for fysiske personers rettigheder og frihedsrettigheder, skal der ***uden unødig forsinkelse*** ske underretning om sikkerhedsbruddet til de registrerede

- Krav til underretningen:
  - I et klart og let forståeligt sprog
  - Karakteren af sikkerhedsbruddet samt dataomfang
  - Angive tiltag for at begrænse skaderne
  - Konsekvenserne af bruddet

- For at kunne leve op til forpligtelserne i Artikel 33 og 34 er det en forudsætning, vi har et effektivt beredskab døgnet rundt

Databeskyttelsesrådgiver - DPO
Artikel 37 til 39

- Alle offentlige myndigheder er forpligtiget til at få en DPO – det samme gælde for nogle private virksomheder og organisationer

- DPO har 3 roller i sit arbejde:
  - Skal *rådgive* organisationen om sikker og korrekt beskyttelse af personoplysninger
  - Skal *kontrollere* at organisationen arbejder sikkert og korrekt med personoplysninger
  - Skal *sikre* de registreredes rettigheder

- Dertil skal DPO'en fungere som bindeled til Datatilsynet og assistere når Datatilsynet udfører sine tilsyn
- DPO'en er underlagt tavshedspligt f.eks. i forbindelse med identitet på anmeldere

- Organisationen må ikke instruere DPO'en i, hvordan opgaverne skal udføres
- Opgaverne skal udføres med direkte reference til den øverste ledelse
- DPO'en må godt udføre andre opgaver for organisationen, men de må ikke have interessekonflikt ift. DPO-opgaverne

Afrunding

- Følg med på www.informationssikkerhed.aau.dk