Databeskyttelsesforordningen

Teia Melvej Stennevad

AALBORG UNIVERSITET

Hvordan kommer vi i gang?

Hvordan spiser vi elefanten?

Jeg vil forsøge at lave en let indflyvning til følgende spørgsmål:

- Hvad er Databeskyttelsesforordningen for en størrelse?
- Hvad er det nye?
- Hvad er godt at vide (grundbegreber)?
- Hvilke dele af forordningen er vigtig for os?
- Går jorden under d. 25. maj?

Databeskyttelsesforordningen
– hvad er det?

- Hovedmålet for arbejdet med forordningen er at få udskiftet forældet national lovgivning og skabe harmonisering på tværs af EU

Databeskyttelsesforordningen skal:

- 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

Begrebsforvirring

- Databeskyttelsesforordning eller Persondataforordning?
- Databeskyttelseslov eller Persondatalov?

Kært barn har mange navne…

- De korrekte termer er: Databeskyttelsesforordningen og den kommende danske lov: Databeskyttelsesloven (samlet kaldes de Databeskyttelsesreglerne). Persondataloven er den lov vi har haft hidtil, og der er aldrig noget, der har heddet Persondataforordningen
- Forordningen kaldes nogle steder for GDPR – en forkortelse for det engelske navn: General Data Protection Regulation

Total harmonisering?

- Nej!
  - De nationale datatilsyn vil forblive uafhængige, men ‘policy making’ vil overgå til EU Kommissionen
  - Der er 54 punkter i forordningen, hvor der skal ske national tilpasning

- Nationale regler kan bl.a. fravige forordningen på følgende områder:
  - Identitetsnummer (Cpr-nr.)
  - Ansættelsesforhold
  - Helbredsforhold
  - Videnskabelige forhold
  - Journalistiske forhold
  - Religiøse sammenslutninger

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 pålagt større ansvar for at efterleve lovgivningen

- Vi vil især opleve at følgende kommer i fokus:
  - Retten til at blive glemt
  - Dokumentationskrav
  - Dataminimering
  - Samtykke
  - Privacy by Design
  - Privacy by Default

- Og, så er der kommet ca. 16 mio. gode grunde på bordet, til at vi skal følge de kommende Databeskyttelsesregler

Sanktioner

Det alle taler om...

- Med Databeskyttelsesforordningen er der også kommet betydeligt større bøder i sigte
  - Databeskyttelsesloven er ikke endeligt vedtaget, men det lader til at de offentlige institutioner i Danmark kan forvente bødestørrelser op til 16 mio. dkkr.
  - Hidtil har den største bøde i Danmark være 25.000 dkkr.

- Andre sanktionsmuligheder:
  - Indstilling af behandling af data (permanent eller indenfor en tidsramme) hvilket kan resultere i at forskningsprojekter skal stoppes
  - Dertil findes der også ”folkets domstol”, hvor dårlig omtale kan føre til tab på konkurrenceevnen, tab af forskningsmidler, manglende evne til at tiltrække studerende, manglende evne til at tiltrække kompetent arbejdskraft

Grundbegreber

Som er gode at gøre sig bekendt med

I forordningen findes en række grundbegreber, som man bør være bekendt med, når man arbejder med personoplysninger:

- Personoplysning
- Behandling
- Dataansvarlig
- Databehandler
- Den registrerede

Hvad er en personoplysning?

- Personoplysninger er enhver form for information om en fysisk person – det vil sige et individ, der enten *er* identificeret eller som *kan* identificeres ud fra informationerne, hvilket ofte betegnes som en *identificerbar person*, der skal forstås som en person, der direkte eller indirekte kan identificeres, hvis man får informationer om dem, som kan sættes sammen og referere til en fysisk person
    - For at noget er en personoplysning skal en oplysning alene eller sammen med andre oplysninger referere til en fysisk person
    - Er der tale om en sammensætning af oplysninger eller hjælpemidler til at skabe identificering – især i de tænkte tilfælde – så skal det være ud fra, hvad der *med rimelighed kan tænkes bragt i anvendelse*
- Når vi taler om personoplysninger, så dækker termen over mere end blot de åbenlyse kategorier, så som navn, adresse, telefonnummer, nationalitet, køn, fingeraftryk, cpr-nummer m.fl. Personoplysninger er også: en persons stemme, eksamensnummer, e-mail-adresse, opkaldsliste, medarbejdernummer, IP-adresse, GPS-oplysninger
    - Se EU-dom vedr. IP-adresser: C-582/14

Hvad er *ikke* en personoplysning?

- Personoplysninger er meget mere, end vi umiddelbart tror. Der er dog også tilfælde, hvor vi behandler oplysninger, som ikke kan anvendes til at identificere fysiske personer
  - F.eks. at 57% af de ansatte i en virksomhed er kvinder. Eller det kan være oplysninger om en kommune, som f.eks. at Aalborg Kommunes Borgmesterforvaltning skifter adresse til Stigsborg Brygge 2

Anonymisering og pseudonymisering

- **Anonyme** oplysninger er ikke personoplysninger og er derfor ikke omfattet af forordningens regler. Imidlertid er en oplysning kun anonym, hvis både du og andre på ingen måde kan identificere personen bag oplysningen
  - Læs mere om specifikationerne for anonymisering på Datatilsynets hjemmeside, der refererer til Artikel 29-gruppens redegørelse
- **Pseudonymiserede** personoplysninger er *stadig* personoplysninger
  - Vælger man at pseudonymisere en personoplysning ved at erstatte et cpr-nr. med bogstaver, ved at benytte en studerendes eksamensnummer som identifikation eller ved at erstatte en interviewpersons navn med et nummer, er det ikke muligt for andre at identificere personen bag cpr-nummeret, da de ikke har nøglen til pseudonymet. Men da det er dig, der har oprettet pseudonymet, har du også nøglen, og du kan derfor tilbageføre pseudonymiseringen og identificere personen, og dermed er oplysningen ikke anonym

Begrebsforvirring

- Anonymisering eller irreversibel anonymisering?

- Der findes kun '*anonymisering*' i Databeskyttelsesforordningen, og denne status for data er i sig selv irreversibel, ellers vil det ikke leve op til forordningens formkrav til anonymiserede oplysninger

Kategorier af personoplysninger

- Databeskyttelsesforordningen deler personoplysninger op i to forskellige kategorier baseret på graden af deres følsomhed:
  - Almindelige personoplysninger
  - Følsomme personoplysninger
- Dertil forholder forordningen sig særskilt til oplysninger om straffedomme og lovovertrædelser, samt CPR-nummer

Begrebsforvirring

- Følsom personoplysning eller personfølsom oplysning?
- Det hedder '*følsom personoplysning'*. Begrebet *'personfølsom oplysning'* findes ikke i forordningen☺

Kategorier af personoplysninger

- Udover de almindelige og de følsomme personoplysninger, så arbejder AAU med yderligere en kategori: fortrolige personoplysninger
  - Begrebet og kategorier stammer fra kategoriseringen i f.eks. Straffeloven og de forvaltningsretlige regler
- Vi arbejder med denne kategori af personoplysninger, da vi skal være opmærksomme på de særlige regler, der kan omgærde disse oplysninger, og vi skal være opmærksomme på, at der kan gælde andre niveauer af sikkerhedsforanstaltninger

- Læs mere om kategorierne på AAU her

Kategorier af personoplysninger

Almindelige personoplysninger

Klassiske stamoplysninger, dvs. navn, køn, adresse og telefonnummer, fødselsdato, nær familie, oplysning om status vedr. hemmeligt nummer/ adresse og foto-ID.

Oplysninger om uddannelse, udtalelser, kursusbeviser, beskæftigelser, arbejdsopgaver.

Oplysninger om løn, skat, pension og lønkontonummer

Kørekort

Tilknytning til en eller flere institutioner

Nationalitet

Systembrugeroplysninger

Fortrolige personoplysninger

Personlighedstest, Logning af internetbrug
Skilsmisse, Registreret partnerskab, Adoptionsforhold

Alkohol- og narkotikatest

Registrering af snyd til eksamen, Karakterer

Væsentlige sociale problemer og familieforhold

Bortvisningsgrund og disciplinære sager

Referater af personlige samtaler, hvis disse indeholder oplysninger af særlig karakter

Hemmelig adresse

Følsomme personoplysninger

(listen er udtømmende)

Race og etnisk oprindelse

Politiske, religiøse og filosofiske overbevisninger

Fagforeningsmæssige tilhørsforhold

Genetiske data

Biometriske data (med det formål entydigt at identificere en person)

Helbredsoplysninger

Seksuelle forhold og seksuelle orientering

Straffedomme og loveovertrædelser

Oplysninger om at den registrerede er dømt i strafbare forhold

Oplysninger om at den registrerede har begået et eller flere strafbare forhold

CPR-numre

Hvad er en behandling?

- Begrebet ’behandling’ dækker over en lang række forskellige måder at håndtere personoplysninger på. I praksis er så godt som alt, hvad du foretager dig med personoplysninger, en *behandling* af personoplysninger
- Det dækker for eksempel over:
  - Indsamling, registrering, organisering, systematisering, opbevaring, tilpasning og ændring af personoplysninger. Det er også genfinding, søgning, brug af, videregivelse, formidling, sammenstilling, samkøring, begrænsning, sletning og tilintetgørelse
- Vær her opmærksom på, at hvis du har ret til at foretage én bestemt form for behandling af en eller flere personoplysninger, medfører det ikke automatisk, at du også har ret til at foretage andre former for behandling på personoplysningerne
- Bare det, at man har eller giver nogle ‘se-adgang’ til personoplysninger, bevirker, at der behandles personoplysninger, og hvis den anden part er en ekstern tredjepart, så skal der en databehandleraftale på bordet – *men det vender vi tilbage til*

Dataansvarlig, databehandler og den registrerede

Dataansvarlig:

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

Den registrerede

- 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 dataansvarlige, når vi behandler AAU's data, vi er 'autoriserede medarbejdere', og vi arbejder efter instruks – hvis vi vel at mærke behandler oplysningerne, som led i vores arbejdsopgaver!
  - De 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 (og selv bestemmer over oplysningerne), så er der tale om private projekter, som AAU ikke skal tage ansvar for, lægge udstyr til, stille garantier for mv.

Databeskyttelsesforordningen 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

Artikel 5-11

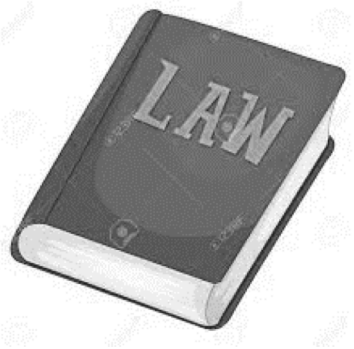
Artikel	Indhold
5	Principper for behandling af personoplysninger
6	Lovlig behandling af almindelige personoplysninger
7	Betingelser for samtykke
8	Lovlig behandling af oplysninger om børn
9	Lovlig behandling af følsomme oplysninger
10	Lovlig behandling vedr. straffedomme mv.
11	Behandling der ikke kræver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

Behandlingsprincipperne

- Behandlingsprincipperne 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**)

Hjemmel

Vær OBS på at nedenstående ikke er en udtømmende liste, men det er de mest relevante hjemmelsgrundlag for AAU



- Den registrerede har givet **samtykke** til, at vi må behandle den registreredes oplysninger til et eller flere specifikke formål
  - Her skal man være opmærksom, hvis der anvendes samtykke som hjemmel ved følsomme personoplysninger, da dette skal være *udtrykkeligt*
- Behandling er nødvendig af hensyn til **opfyldelse af en kontrakt**, som den registrerede er part i
- Vi er nødt til at behandle den registreredes oplysninger for at kunne overholde AAU's eller den registreredes **arbejds-, sundheds- og socialretlige forpligtelser**
  - For eksempel kan det i forbindelse med en medarbejders langtidssygemelding være nødvendigt at opbevare medarbejderens helbredsoplysninger for at kunne opfylde AAU's arbejdsretlige forpligtelse
- Vi behandler personoplysninger, som **tydeligvis er offentliggjort af den registrerede selv** (f.eks. via Facebook)

Hjemmel

Vær OBS på at nedenstående ikke er en udtømmende liste, men det er de mest relevante hjemmelsgrundlag for AAU

- Vi er nødt til at behandle den registreredes oplysninger for at kunne **fastlægge, forsvare eller gøre et retskrav gældende**
- Vi er nødt til at behandle den registreredes oplysninger af hensyn til **væsentlige samfundsinteresser**
  - Det kan for eksempel være i forbindelse med studieadministration, at vi er nødt til at indhente og registrere en studerendes helbredsoplysninger for at kunne behandle vedkommendes dispensationsansøgning
- Eller hvis vi er nødt til at behandle den registreredes oplysninger til brug for **arkivformål i samfundets interesse**, til **videnskabelige eller historiske forskningsformål** eller **til statistiske formål**
  - For eksempel kan det være, når følsomme personoplysninger indgår i forskningsprojekter som en del af datagrundlaget

Registreredes rettigheder

Artikel 12-22

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

Registreredes rettigheder

"Before I write my name on the board, I'll need to know how you're planning to use that data."

Transparens

- Der findes krav til måden, hvorpå vi kommunikerer med de registrerede på ift. oplysningspligten og den registreredes rettigheder generelt (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

- Oplysningspligt – differentieret efter om oplysningerne er direkte indsamlet ved den registrerede, eller om de er indsamlet ved tredjepart

- Standard 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 der behandles, og hvor de stammer fra
  - Vedr. profilering: 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 der 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

- Ret til indsigt
  - Den registrerede har ret til at få bekræftet, om deres personoplysninger behandles, og i givet fald adgang til oplysningerne
- 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

Retten til at blive slettet

- Retten til sletning – også kaldet retten til at blive glemt!
- 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

Retten til at blive slettet

- 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

- *Sletning er i vidt omfang bundet op på alle de andre love og regelsæt, vi skal efterleve*

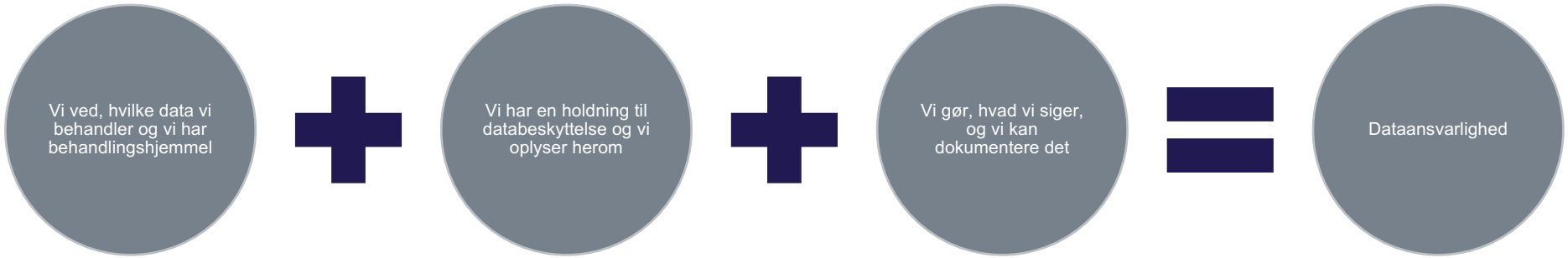
Dataansvarliges pligter

Artikel 24-39

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)

Dataansvarlighedsprincippet

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



Privacy by Design
Privacy by Default

Termerne dækker over at databeskyttelse skal tænkes ind i vores forretningsprocesser, services og produkter fra starten af.

- **Privacy by Design** er en tilgang, der sikrer, at virksomheden indarbejder databeskyttelse fra starten af
- **Privacy by Default** betyder, at produkterne allerede fra start er indstillet til det højeste niveau af persondatabeskyttelse

- Begge principper har til formål at reducere mængden af data, der automatisk deles, og sørge for at forbrugerne som udgangspunkt selv har ret til at bestemme, hvor meget af deres data, der skal deles og være synligt

- Fremtidige løsningers standardindstillinger skal derfor indstilles, så de begrænser unødvendig brug af data og fremmer formålsspecifik behandling.
- Det er dog ikke et krav, at eksisterende it-systemer bliver redesignet, så længe de overholder forordningen
    - Skal man fremadrettet lave tilpasninger på eksisterende it-løsninger, kan det dog være nødvendigt at tænke Privacy by Design/Default ind

Fælles dataansvar

- Dette er ikke et nyt fænomen, men der bliver åbnet mere op for det med forordningen

- Fælles dataansvar mellem to eller flere parter kan komme på tale, hvis parterne i fællesskab bestemmer, **hvorfor** der skal behandles personoplysninger, og **hvordan** de skal behandles
- Et fælles dataansvar kan dog kun komme på tale, hvis part 1 og part 2 sammen har ansvaret for en behandling, og hvis de begge har ret til at bruge oplysningerne til egne formål. Der er altså ikke tale om et fælles dataansvar, hvis en behandling kun foretages til den ene parts formål

- Er der tale om fælles dataansvar skal parterne indgå en skriftlig aftale, hvor de på en gennemsigtig måde fastlægger deres respektive ansvar for overholdelse af forordningen, og i særdeleshed ansvaret for overholdelsen af oplysningspligten overfor de(n) registrerede
- Det danske Datatilsyn har lavet en aftaleskabelon for fælles dataansvar se den her

Databehandleraftale

- Når en dataansvarlig overlader behandling af personoplysninger til en databehandler, så skal der indgås en skriftlig aftale mellem parterne: en databehandleraftale
  - F.eks. outsourcing, hosting, drift, datasammenstilling (forskning), SLA (Serviceaftale) mm.

- Der er en række indholds- og formkrav til sådan en aftale bl.a.:
  - Varigheden af behandlingen
  - Behandlingens karakter og formål
  - Typen af personoplysninger og kategorier af registrerede
  - Den dataansvarliges forpligtigelser og rettigheder

- Der til kommer der en række krav om sikkerhed og dokumentation.

Databehandleraftale

- Databehandleren må ikke bruge de overladte oplysninger til andet end udførelsen af opgaven for den dataansvarlige med mindre andet er defineret ved lov
  - Handler Databehandler uden instruks pådrager de sig selvstændigt dataansvar – *dog ulovligt*

- 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
  - Ønsker en Databehandler ikke at underskrive en Databehandleraftale, anbefales det at finde en anden Databehandler til at løse opgaven/en anden leverandør

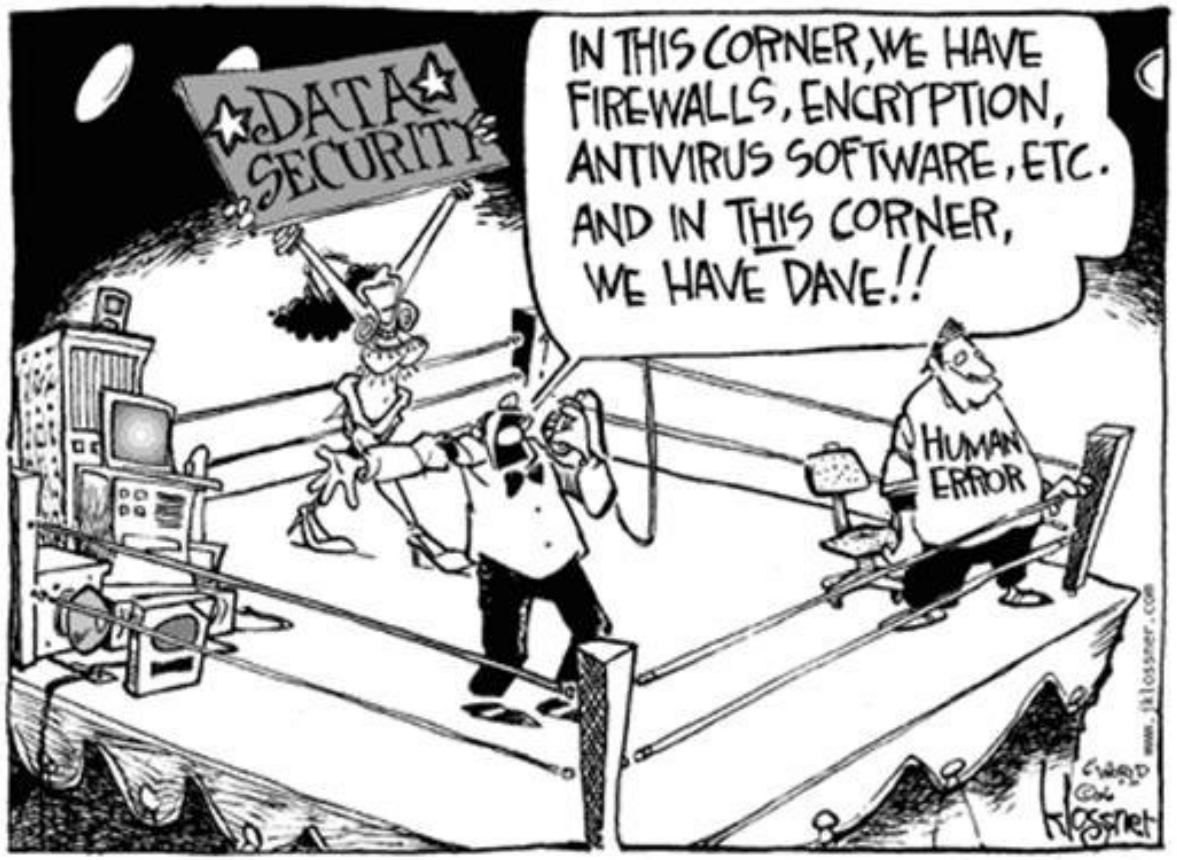
- Ved AAU er der lavet skabeloner, som skal anvendes til at regulere de databehandlerforhold som AAU er en del af. Hovedreglen er, at i de forhold, hvor AAU er dataansvarlige, er det AAU's aftaleskabelon, der skal anvendes, se dem her

Fortegnelser over behandlingsaktiviteter

- Fortegnelserne er en del af dokumentationspligten
- Der er en række form- og indholdskrav til fortegnelserne, herunder:
  - Fortegnelserne skal bl.a. indeholde oplysninger om den dataansvarlige, om formålene med behandlingen, kategorier af personoplysninger og registrerede
  - Fortegnelserne skal foreligge skriftligt og elektronisk

- Fortegnelserne skal stilles til rådighed for Datatilsynet, hvis myndigheden anmoder herom

Brud på persondatasikkerheden



Brud på persondatasikkerheden

Anmeldelse til Datatilsynet

- I tilfælde af sikkerhedsbrud, hvor personoplysninger er blevet kompromitteret, skal vi uden unødig forsinkelse og om muligt inden **72 timer** underrette Datatilsynet efter at være kommet til kendskab med sikkerhedsbruddet
  - Ved databehandlerforhold skal en databehandler **øjeblikkeligt** 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

Brud på persondatasikkerheden

Underretning til de registrerede

- 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

- Form- og indholdskrav 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 forbindelse med brud på persondatasikkerheden er det en forudsætning, vi har et effektivt beredskab døgnet rundt

Databeskyttelsesrådgiver - DBR
Data Protection Officer - DPO

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

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

Databeskyttelsesrådgiver - DBR
Data Protection Officer - DPO

- Dertil skal DPO'en fungere som bindeled til Datatilsynet, og assistere når Datatilsynet udfører sine kontroller
- DPO'en er underlagt tavshedspligt f.eks. i forbindelse med identitet på anmeldere
- Organisationen må ikke instruere DPO'en i hvordan opgaverne skal udføres - armslængdeprincip
- Opgaverne skal udføres med direkte reference til den øverste ledelse
- DPO'en må godt udføre andre opgaver for organisationen, men der må ikke være interessekonflikt ift. DPO-opgaverne

Går jorden under?

Nyttige links

Informationssikkerhed ved AAU: www.informationssikkerhed.aau.dk/persondata

Datatilsynets hjemmeside: www.datatilsynet.dk/forside/

Datatilsynets GDPR hjemmeside: www.dbreform.dk/

Dokumenter:

Forslag til Databeskyttelsesloven

Databeskyttelsesforordningen

Betænkning nr. 1565 ligger på Justitsministeriets hjemmeside – kan gratis downloades i pdf format