TEMAMØDE – 16. MARTS 2016

INFORMATIONSSIKKERHED

Henrik Rask / AAU

DAGENS PROGRAM

Stil gerne spørgsmål undervejs

- ISO27001 m.fl., kort beskrivelse af hvad det er for noget
- Informationssikkerhed.aau.dk
- Sikkerhedshåndbog via informationssikkerhed.aau.dk
- Secureaware:

  a) Politikker
  b) Aktiver
  c) Risikovurderinger
  d) Beredskab
  e) Opgaver
  f) krav
  g) Quiz

- Powerpoint omkring EU´s persondataforordning, gennemgang og dialog.
- Pause i 15 minutter
- Opgave

  Brainstorm i mindre grupper: Hvilke udfordringer har vi omkring it-sikkerhed/informationssikkerhed? (15 minutter)

- De samlede input bringes op på tavlen og prioriteres i fællesskab (prioritet 1-5)

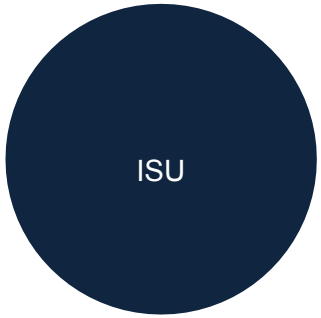
ISO 27001, 27002 M.FL.

Hvad er det for noget

Se nærmere her:

http://www.digst.dk/Arkitektur-og-standarder/Videnscenter-for-implementering-af-ISO27001/Implementering-af-ISO27001/Hvad-er-ISO27001

INFORMATIONSSIKKERHEDS-UDVALG PÅ AAU



- Informationssikkerhedsudvalg har følgende sammensætning:
- Overbibliotekar Niels-Henrik Gylstorff, Fælles Service, universitetsbiblioteket, formand
- Fuldmægtig Kathrine Tvorup Pajkes, Kontraktenheden
- Institutleder Kristian G. Olesen, Datalogi
- fg. IT-Direktør Per Hejgaard, Fælles Service, ITS
- Studiechef Lone Vestergaard, Fælles Service, Studieforvaltningen
- Studieleder Falk Heinrich, Skole for Kommunikation, Æstetik & Oplevelsesteknologi (Communication, Art & Technology)
- Studerende Johan Sørensen, studentersamfundet, jsore10@student.aau.dk
- Informationssikkerhedschef (CISO) Henrik Johannes Rask, sekretær og fast medlem.

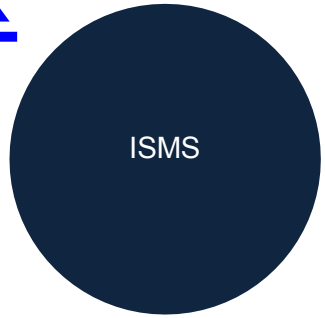
INFORMATIONSSIKKERHED PÅ AAU

http://informationssikkerhed.aau.dk

https://youtu.be/ySEh1VsS0Mw

Sikkerhedshåndbogen (politikker og bilag m.m.)

SECUREAWARE.AAU.DK



a) Politikker
b) Aktiver
c) Risikovurderinger
d) Beredskab
e) Opgaver
f) Krav
g) Quiz

EU PERSONDATAFORORDNING

GENNEMGANG AF OPGAVER PÅ OVERSKRIFTSNIVEAU

Henrik Rask / AAU

ER DE KOMMENDE KRAV NYE KRAV?

De grundlæggende beskyttelseskrav vil være de samme som i nuværende persondatalov, hvorfor det allerede nu vil være en god idé, at få skabt det fornødne overblik over behandling af persondata.

Kravene i den kommende forordning er for en stor dels vedkommende IKKE nye krav – men ”blot” flere krav om øget dokumentation, organisering, systematisering og processer.

CENTRALT OVERBLIK

Allerede i dag forventes det at vi har, eller kan skabe, et overblik over hvilke behandlinger vi foretager og hvilke typer af personoplysninger der behandles.

Forordningen opererer med, at vi skal have ét centralt sted, hvor der er overblik over alle de behandlinger vi har. (Datatilsynet har allerede pålagt dette til det enkelte universitet).

Det er også til dette centrale sted den enkelte skal anmelde sin behandling af persondata – det skal altså ikke længere foregå til Datatilsynet.

Datatilsynet kan til enhver tid rekvirere en oversigt (fra det centrale sted) over behandlinger på det enkelte universitet.

HVAD SKAL DER SÅ TIL?

Vi er bl.a. nødt til at skabe fuldstændigt overblik over, hvordan datastrømme med persondata flyder.

(Allerede i dag er det i praksis nødvendigt, at have dette overblik for at kunne leve op til persondataloven)

Arbejdet bliver meget omfattende – der findes uden tvivl mange tusinde datastrømme, der skal identificeres og dokumenteres.

Dokumentation som vi i dag kun har i meget begrænset omfang.

HVAD SKAL DER SÅ TIL?

En del af opgaven med identifikation af datastrømme vil kræve dokumentation af systemsammenhænge, hvilket i praksis også er gældende i nuværende persondatalov.

Hvilke data findes i hvilke systemer – og hvordan er disse data sikret? (det er nødvendig viden i det videre forløb – har vi den?)

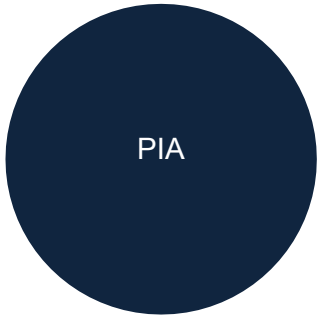
KLASSIFIKATION AF DATA

Hvilke data er almindelige persondata og hvilke er særlige persondata (f.eks. fortrolige og følsomme persondata)?

(Vi skal allerede i dag behandle persondata iht. hvilken type, der er tale om)

Klassifikation af data bliver et centralt og væsentligt element i kravene til fremtidige håndtering af data.

PRIVACY IMPACT ASSESMENT



Udarbejdelse af konsekvensanalyse vedrørende databeskyttelse – nyt i forhold til nuværende persondatalov.

Skal udarbejdes ved behandling af personoplysninger, som kan indebære specifikke risici for den registreredes rettigheder.

Behandling som kan indebære disse specifikke risici:

- Systematisk og omfattende evaluering af personlige aspekter om en persons økonomi, sundhed, præferencer mv. baseret på elektronisk databehandling, hvis konsekvens har retsvirkning eller berører vedkommende personligt.
- Omfattende registre vedrørende børn, genetiske data eller biometriske data.

En PIA udløser også krav til, at risikovurderinger skal inkludere persondata og risici forbundet med behandling heraf.

Eksempler på ”Code of practice” for PIA´s
https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

http://www.digst.dk/Arkitektur-og-standarder/Videnscenter-for-implementering-af-ISO27001/Konsekvensvurdering-for-privatlivet.aspx

RISIKOVURDERINGER

Der skal fremadrettet udføres risikovurderinger og i det omfang forretningen vurderer risici for store, skal der implementeres foranstaltninger, der nedbringer risici til acceptabelt niveau.

En fór optimistisk risikovurdering vil formodentlig blive taget med i betragtning ved fastsættelse af bødestørrelse i tilfælde af en sikkerhedsmæssigt hændelse.

PRIVACY BY DESIGN

Princippet om ”indbygget databeskyttelse” medfører, at myndigheder og virksomheder skal tænke persondatabeskyttelse ind i de tekniske løsninger.

Dette kan måske også medføre, at eksisterende tekniske løsninger skal ændres – over tid.

PRIVACY BY DEFAULT

Princippet om ”databeskyttelse via indstillinger” medfører, at persondatabeskyttelse skal være standarden for myndigheder, virksomheder og de systemer der anvendes til behandling af persondata.

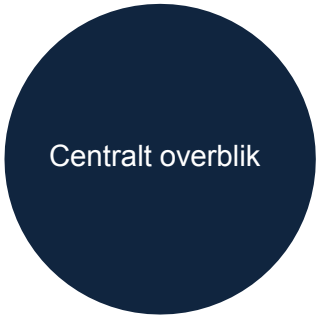
(dette betyder bl.a. at rettigheder til behandling af persondata aktivt skal tilvælges ligesom systemerne som udgangspunkt ikke tillader flere adgange, end de der aktivt er tilvalgt)

ÆNDRINGER AF NUVÆRENDE SYSTEMER?

Er der noget der indtil nu tilsiger, at vi skal ændre nuværende systemer på kort sigt eller på lang sigt?

(der vil formodentlig ikke være krav om udskiftning på kort sigt)

DOKUMENTATION



Der er allerede i dag krav om, at vi kan dokumentere samtykker fra den enkelte person, hvis data vi behandler!

Vi skal fremover sikre, at vi centralt har fuldstændig dokumentation over alle vore behandlinger af persondata.

Der kommer krav til, hvad der som minimum skal være inkluderet i dokumentationen.

Dokumentationen skal være i en form der er ”egnet til Datatilsynet”.

DATA PROTECTION OFFICER

Der skal udpeges en DPO – hvilket er en nyskabelse i forhold til nuværende persondatalov.

Der vil blive krav til faglige kvalifikationer og ekspertise på området

Der vil være krav om uafhængighed for en DPO (organisatorisk placering)

DPO vil få ansvaret for specifikke opgaver i forbindelse med databeskyttelse

Inspiration til kvalifikationer:
http://ec.europa.eu/dataprotectionofficer/docs/dpo_standards_en.pdf

https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/DPOnetwork

DATA PROTECTION OFFICER

Nedenstående er eksempler på opgaver der formodentlig lander på DPO´s opgaveliste:

Sikre at der forefindes nødvendige databehandleraftaler

Sikre gennemførsel af awareness træning

Skal udføre kontrol og audit af behandlinger

Skal sikre dokumentation for politikker, regler, procedurer

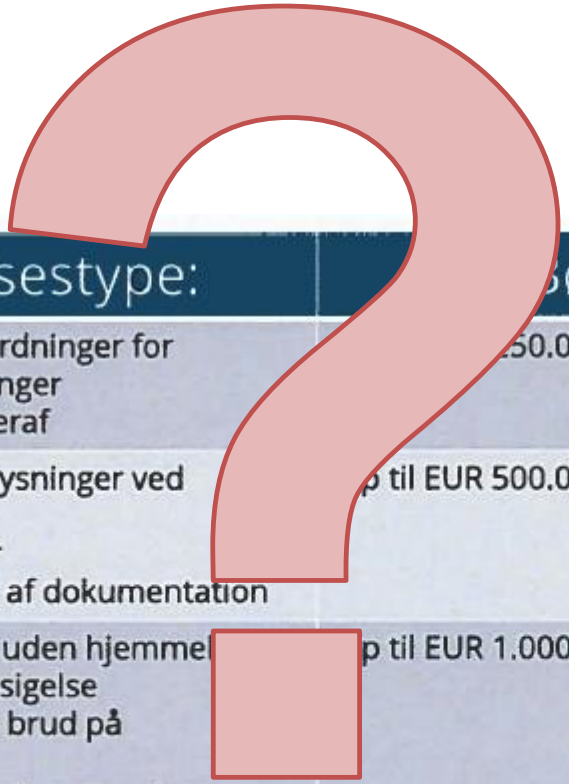
Skal sikre der forefindes et årshjul for arbejdet

Ansvarlig for underretning (til Datatilsyn m.fl.) ved brud på reglerne

14/3-2016: Rektoratet behandlede og godkendte på sit møde her til formiddag forslaget om indstilling af Henrik Rask som DPO.

FORSLAG OM BØDER OP TIL EUR 1.000.000 TIL OFFENTLIGE INSTITUTIONER

Sanktioner



Overtrædelsestype:	Bødeniveau:
• Ingen fastlæggelse af ordninger for registreredes anmodninger • Ej rettidig besvarelse heraf	50.000
• Ikke giver relevante oplysninger ved indsigtsanmodning • Ikke sletter oplysninger • Manglende ajourføring af dokumentation	p til EUR 500.000
• Behandler oplysninger uden hjemmel • Ikke respekterer en indsigelse • Ikke varsler tilsynet om brud på sikkerheden • Ikke gennemfører konsekvensanalyser • Ikke udpeger en DPO • Overfører oplysninger til tredjelande uden hjemmel	p til EUR 1.000.000

ADMINISTRATIVE BØDER?

Ikke i DK – men hvad så?

(120a) (new) The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark, the fine is imposed by competent national courts as a criminal sanction and in Estonia, the fine is imposed by the supervisory authority in the framework of a misdemeanor procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine.

In any event, the fines imposed should be *effective*, *proportionate* and *dissuasive* (afskrækkende)

”VI” SLIPPER FOR BØDER – MÅSKE!

Formodentlig ikke store bøder til det offentlige

Det der er besluttet er, at bødeniveauet hæves til 20 mio. euro – men i DK kan de danske myndigheder afgøre, hvilke regler og hvilket bødeniveau der skal gælde for ***offentlige*** virksomheder. (se nedenstående klip - artikel 79)

Artikel 79:

3b. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 53(1b), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

LIGE OM LIDT ER DER PAUSE I 15 MINUTTER

Pause

INDEN I GÅR TIL PAUSE – LIGE EN KORT INTRODUKTION TIL OPGAVEN EFTER PAUSEN

BRAINSTORM I MINDRE GRUPPER

Når I kommer tilbage fra pausen, skal I sætte jer sammen i mindre grupper (2-4 personer)

Brainstorm over spørgsmålet:

Hvilke udfordringer har AAU omkring it-sikkerhed?

Når der er gået 15 minutter samler vi alle input sammen, hvorefter vi i fællesskab forsøger at prioritere jeres input (prioritet 1-5, hvor 1 er vigtigst)