SMART LIBRARIES OG PERSONDATAFORORDNINGEN

- EN PRAGMATISK GUIDE

Mads Schaarup Andersen
Senior Usable Security Expert, Ph.d.
Smart Library seminar, 3/10-2017

ALEXANDRA
INSTITUTTET

Alexandra Instituttet er en **non-profit** virksomhed, der arbejder med **anvendt forskning**, **udvikling** og **innovation** inden for it

Vi er sat i verden for at skabe **værdi**, **vækst** og **velfærd** i det danske samfund.

HJÆÆÆÆLP!!! FORORDNINGEN KOMMER!!!

- Persondataforordningen ændrer alt!
- Persondataforordningen kommer til at koste os en masse penge!
- Hvis ikke vi overholder persondataforordningen falder der brænde ned!
- .... men er det nu helt så slemt?

ALEXANDRA INSTITUTTET

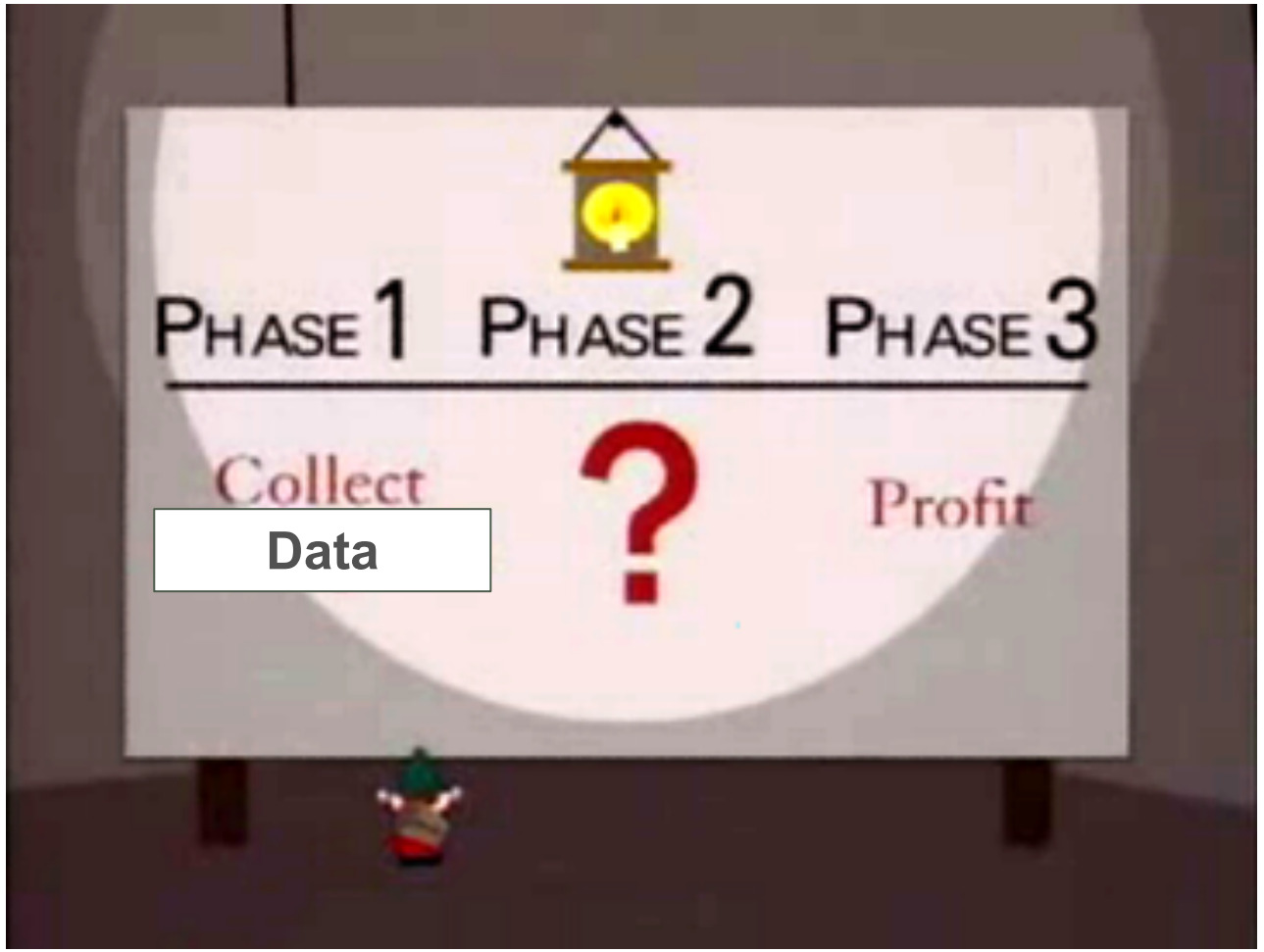
HVORFOR PERSONDATAFORORDNINGEN?

- ”Gratis” services er rigtigt meget værd.
- Gennemsnitsbrugeren har ingen ide om hvad der foregår.
- Virksomheder ved heller ikke helt hvad der foregår.
- Everything goes....

Det vilde vesten

ALEXANDRA INSTITUTTET

HVORDAN TJENER MAN PENGE PÅ DATA?



ALEXANDRA INSTITUTTET

TAKEAWAYS

- Hold formålet med forordningen for øje.
- Tænk over hvorfor I indsamler data.
- Tænk over hvilken type data I behandler.
- Få styr på data og dataflow.
- Dokumenter jeres indsats og overvejelser.

ALEXANDRA INSTITUTTET

HVEM ER JEG?

- Privacy entusiast.
- Ph.d. i lokations privacy.
- Vil gerne udbrede privacy og sikkerhedsløsninger der virker for *alle*.
- Er i gang med at undersøge danske virksomheders udfordringer med GDPR.

ALEXANDRA INSTITUTTET

HVAD KAN JEG FORTÆLLE JER I DAG

- Jeg kan fortælle jer nogen af de ting man skal være opmærksom på.
- Jeg kan fortælle jer lidt om hvad I kan tænke over i forhold til forordningen.
- Jeg kan *ikke* fortælle jer hvordan man skal tolke juraen i forordningen.
- Jeg kan *ikke* fortælle jer præcis hvordan det ender med at blive implementeret i dansk lov.

ALEXANDRA INSTITUTTET

SÅ HVAD ER "TILSTRÆKKELIGE FORANSTALTNINGER”?

- Juridisk kan jeg ikke svare....
- .... men det handler i stor grad om at tænke over og argumenterer for at man har overvejet det.
- Flere andre eksempler i forordningen som fx: ”informeret samtykke”,
- **Generelt: Dokumenter overvejelser!**

ALEXANDRA INSTITUTTET

MEN HVORFOR PERSONDATAFORORDNINGEN?

- Beskytte individets rettigheder.
- Privacy er ofte ikke en ting der bliver tænkt over.
- **Men også en mulig:**
  - Få styr på hvilke data man indsamler og er i besiddelse af.
  - Åbenhed fører til tillid.
  - *”Gøre tingene ordentligt.”*

ALEXANDRA INSTITUTTET

HVAD ER DET NYE I FORORDNINGEN?

- Meget af det folk tror er nyt eksisterer allerede i persondataloven.
- Mange overholder i dag ikke loven(!)
- Mere fokus på overholdelse og sanktioner end i dag.
- Stadig uklart hvordan offentlige organisationer vil blive sanktionerede.
- **Pragmatisk: Meget af det er nyt for de fleste!**

ALEXANDRA INSTITUTTET

OFFENTLIG VS PRIVAT ORGANISATION

- Der er forskel på offentlig og privat.
- Mange offentlige myndigheder har fx pligt til at gemme data.
- Dvs. man ikke nødvendigvis har ret til at blive slettet.
- Overholder man ISO27001 er man godt på vej.

PERSONHENFØRBARE DATA – OG HVAD SÅ?

- Skærpede krav til håndtering af personhenførbare data:
  - Dataminimalisering.
  - Nye regler for samtykker.
  - Transparens om databehandling.
  - Individet får stærkere rettigheder.
  - Dokumentation og impact assessments.

ALEXANDRA INSTITUTTET

VÆK FRA DATA-HORDER MENTALITETEN

ALEXANDRA INSTITUTTET

DATAMINIMALISERING

- Hvad er formålet med indsamling af data?
- Hvor meget (lidt!) data har vi brug for til det pågældende formål?
- I hvilken grad har vi brug for at kunne binde data til et individ?

ALEXANDRA INSTITUTTET

EKSEMPEL: TÆLLING AF BESØGENDE

- Full blown: Mads Andersen, Jens Pedersen, Anne Larsen.... var i møderum 4 på DOKK1 mellem 9:30 og 15.
- Medium: Der var 20 unikke besøgende på rampen mellem kl 9:30 og 15.
- Minimal data: Der var 100 besøgende på DOKK1 mellem 9:30 og 15.

ANONYMISERET DATA

- Data der ikke kan bindes til en bestemt person.
- Der skal være taget *"tilstrækkelige foranstaltninger"* for at undgå re-identifikation.
  - Dokumenter hvorfor I mener det ikke er tilfældet.
- Anonymiseret data er ikke personhenførbart og derfor gælder forordningen ikke!

ALEXANDRA INSTITUTTET

PERSONHENFØRBAR DATA

- Al information der kan sættes i forbindelse med et individ.
- Fx adresse, IP-adresse, telefonnummer, biblioteksbrugsmønster.
- Kan gøres ved at aggregere data. 10 personer i område X, i stedet for hvilke 10 personer der opholder sig i område X.
- Særligt følsomme persondata:
  - Religion, etnisk oprindelse, fagforeningstilhørsforhold.
  - DNA, biometrisk data.

ALEXANDRA INSTITUTTET

SAMTYKKE ELLER EJ?

- Er der lovlig hjemmel til at indhente og behandle persondata uden samtykke?
- Er det legitime formål? Eller: er det rimeligt forventeligt at I bruger persondata til et bestemt formål?
- Eksempel: En navigations app bruger lokation til at vise vej, men er det ok den også bruger det til at reklamerer for et produkt den mener du er interesseret i?

ALEXANDRA INSTITUTTET

SAMTYKKER I PERSONDATAFORORDNINGEN

- Der skal opnås *aktive*, *specifikke* og *informerede* samtykker.
  - En implicit privacy policy ikke er nok.
  - Et samtykke gælder ét formål.
  - Der skal kunne argumenteres for at samtykket er givet på informeret grundlag.
- Samtykker skal kunne trækkes tilbage.
- Og husk: børn kan *ikke* give samtykke! (13 år)
  - Samtykker skal indhentes ved forældrene.

ALEXANDRA INSTITUTTET

TRANSPARENS OM DATABRUG

- Fortæl hvad I laver. Kan være på hjemmeside/i app/på papir.
- Find inspiration til at designe privacy notices: https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub

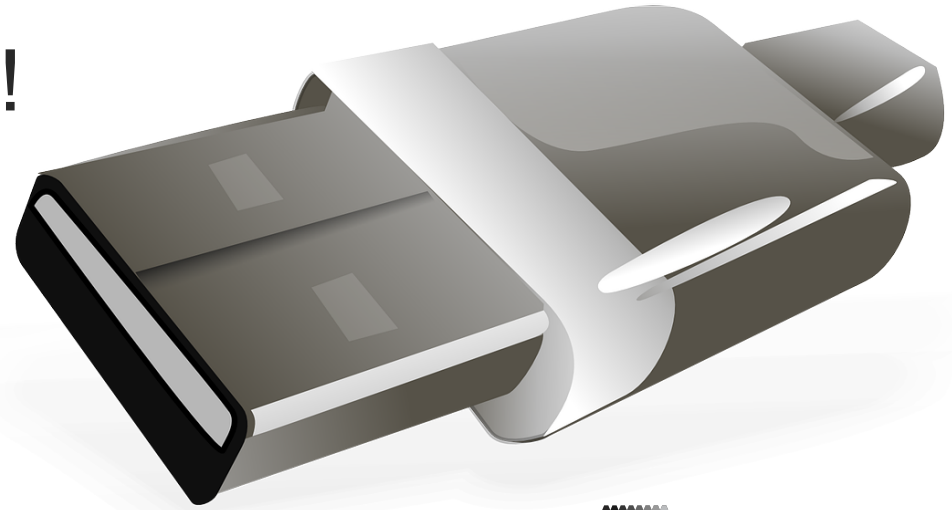
RETTEN TIL AT BLIVE GLEMT OG FÅ RETTET DATA

- Individet har ret til at blive glemt og få data slettet (der er undtagelser).
- Dette gælder *også* hos eventuelle underleverandører.
- Der er store (uafklarede) udfordringer i forbindelse med hvordan dette håndteres i backup.
- Selvom man ikke skal slette data skal man stadig understøtte ændringer i backup!

ALEXANDRA INSTITUTTET

DATAINDSIGT OG PORTABILITET

- Individer har ret til at få indsigt i hvilken data der ligger om dem.
- Der er i mange tilfælde også ret til at få udleveret data i standardiseret format.
- Tænk det ind i systemerne fra start!



ALEXANDRA INSTITUTTET

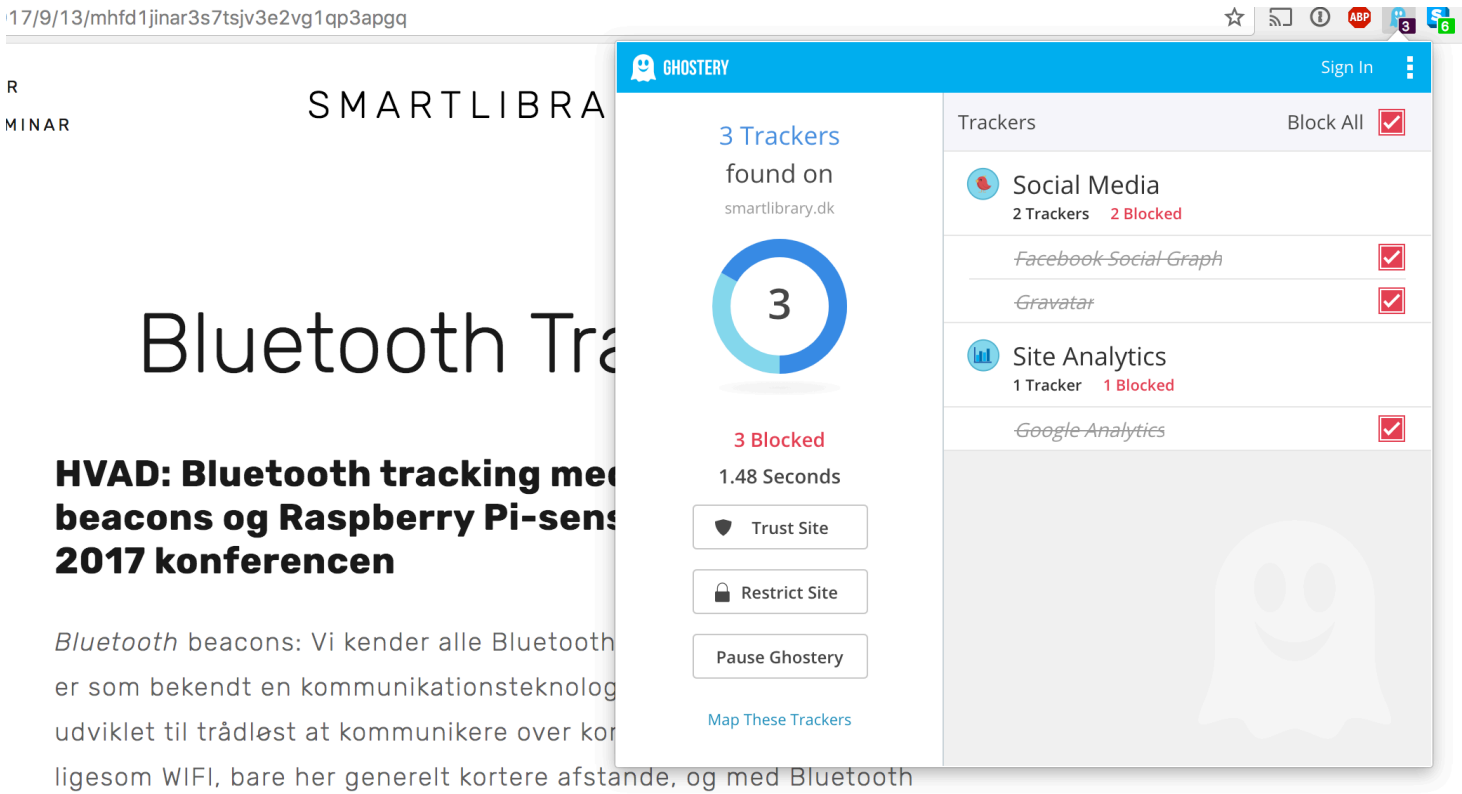
ER DER STYR PÅ DATA HOS JER?

- Hvilke data ligger der i systemet?
- Hvem har adgang til persondata?
- Bliver data videregivet?
- Hvilke systemer kører der?
- Bliver data slettet?
- Bliver data beskyttet?

ALEXANDRA INSTITUTTET

VIDEREGIVELSE AF DATA

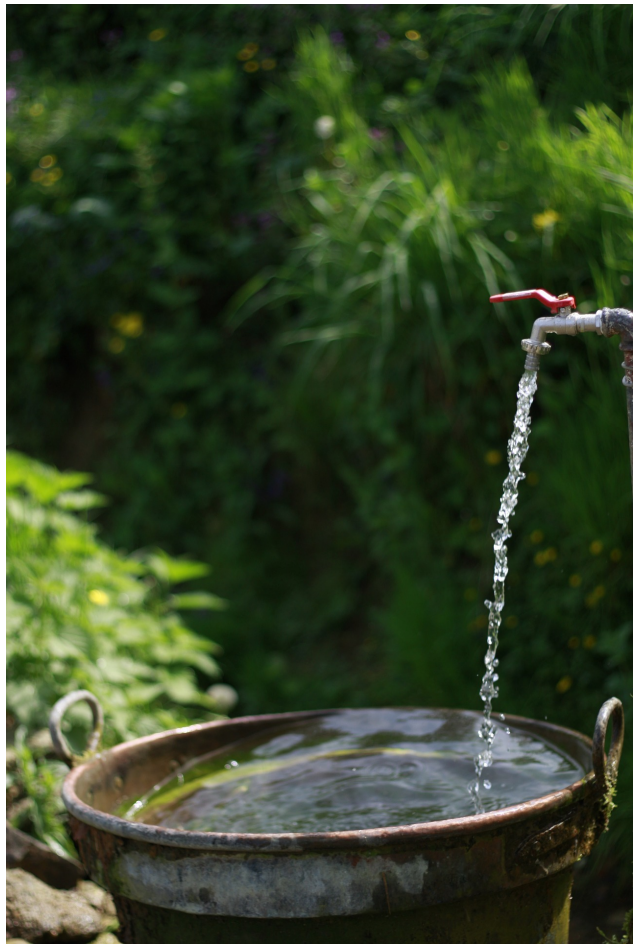
- Er der styr på databehandleraftaler hvis 3. parts leverandører/værtøjer bruges?
- Er Google Analytics eller Google Docs OK at bruge?
- Sendes der data til udlandet og ud af EU?



ALEXANDRA INSTITUTTET

IMPACT ASSESSMENTS

- Der skal laves en risikovurdering af persondata.
- Hjælper med at finde ud af hvor sensitivt det data man har er.
- Man kan finde inspiration i DIs guide.



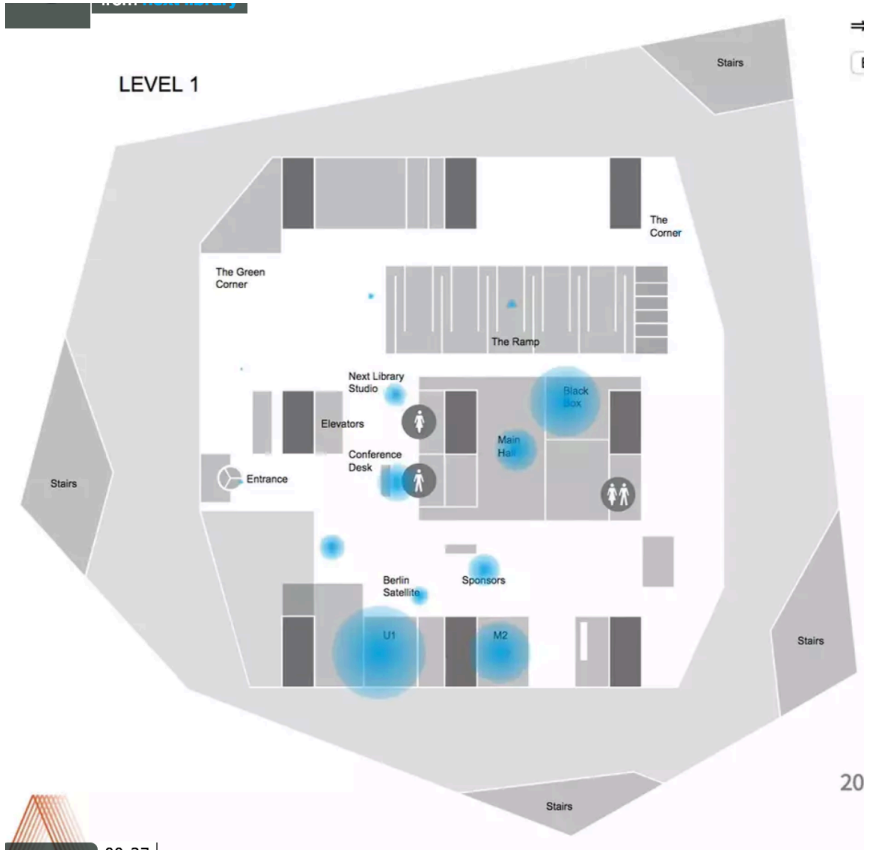
HVEM HAR ANSVARET?

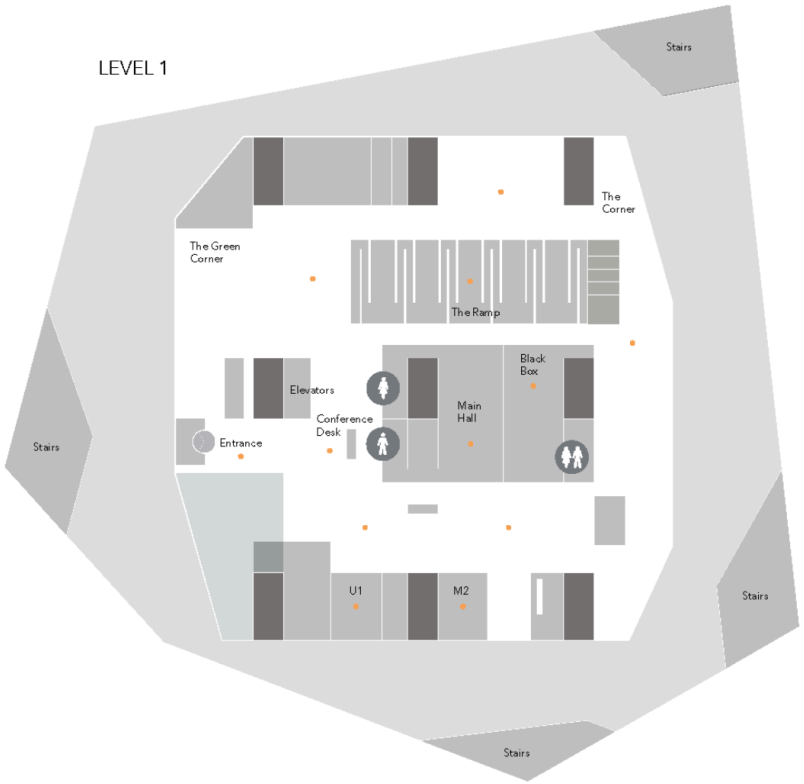
- *"Offentlige myndigheder og offentlige organer skal altid udpege en databeskyttelsesrådgiver, hvad enten de er dataansvarlige eller databehandlere."*
- Det er vigtigt at have sætte ressourcerne af.
- Det kan være nødvendigt at se på datakulturen.

CASE: INDHENTNING AF SENSORDATA

ALEXANDRA INSTITUTTET

HVORFOR SAMLES DER DATA IND?





ALEXANDRA INSTITUTTET

HVAD MED DATA?

- Skal der opnås nye samtykker for at bruge data på en ny måde?
- Hvor gemmes data?
- Benyttes der 3. parts leverandører af services?
- Er der styr på hvornår og hvordan data slettes?

ALEXANDRA INSTITUTTET

ER DER TILSTRÆKKELIG SIKKERHED?

- Hvem har adgang til data?
- Ligger data på devices og er de krypterede?
- Sender de eventuelt data?
- Kan man læse data ud ved at forbinde til et device der sidder i miljøet?

ALEXANDRA INSTITUTTET

ANDRE SMART LIBRARY PROBLEMSTILLINGER

- Hvordan og hvor gemmer man observationsdata?
- Hvis der tænkes andre typer biblioteksdata sammen med nye data, er det så lovligt og skal der opnås nye samtykker?
- Hvis der benyttes eksterne personer skal de også leve op til jeres krav, da I er dataansvarlige.
- Video, lydoptagelser af interview og nedskrivning der ikke er anonymiserede er personhenførbare data og skal behandles som sådant.

ALEXANDRA INSTITUTTET

RESSOURCER TIL VIDEN

- [1] Plan for justitsministeriets vejledninger om forordningen - http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/plan_for_vejledninger_om_forordningen.pdf
- [2] Justitsministeriets vejledning om databeskyttelsesansvarlige - https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Publikationer/Vejledning_DPO.pdf
- [3] DIs vedledning til data protection impact assessment - https://digital.di.dk/SiteCollectionDocuments/Vejledninger/Vejledning-DPIA-2016-Final.pdf
- Søg på: ”persondataforordning” og få inspiration.

ALEXANDRA INSTITUTTET

Tak for opmærksomheden!

ALEXANDRA
INSTITUTTET