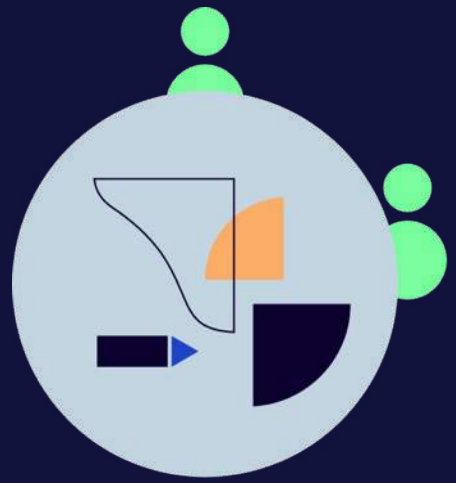
BESTE PRAKSIS FOR Å SKRIVE EN ~~DPIA~~ PERSONVERN KONSEKVENSVURDERING

Simen Sommerfeldt

Sikkerhetsfestivalen 2023



Simen Sommerfeldt - @sisomm

Bachelor of Engineering, University of Surrey
Tre barn
Role: CTO@Bouvet
En av grunnleggerne av «Lær Kidsa Koding»
Var med på å etablere GoForIT
Stedfortreder i personvernnemnda
Bidragsyter til personvernkommisjonen

GOFORIT

L K K Lær Kidsa Koding

bouvet

Dette er Bouvet

Vi er et norsk konsulentselskap, med 19 kontorer i Norge og Sverige med over 2100 ansatte

Stor fokus på delingskultur, troverdighet og jordnærhet

Vi leverer tjenester innen kommunikasjon, rådgivning og teknologi

bouvet

Visjon

Vi går foran og bygger fremtidens samfunn

bouvet

Hvorfor PVK er viktig

Brundtland-rapporten fra 1987

«Bærekraft er utvikling som imøtekommer dagens behov uten å ødelegge mulighetene for at kommende generasjoner skal få dekket sine behov»

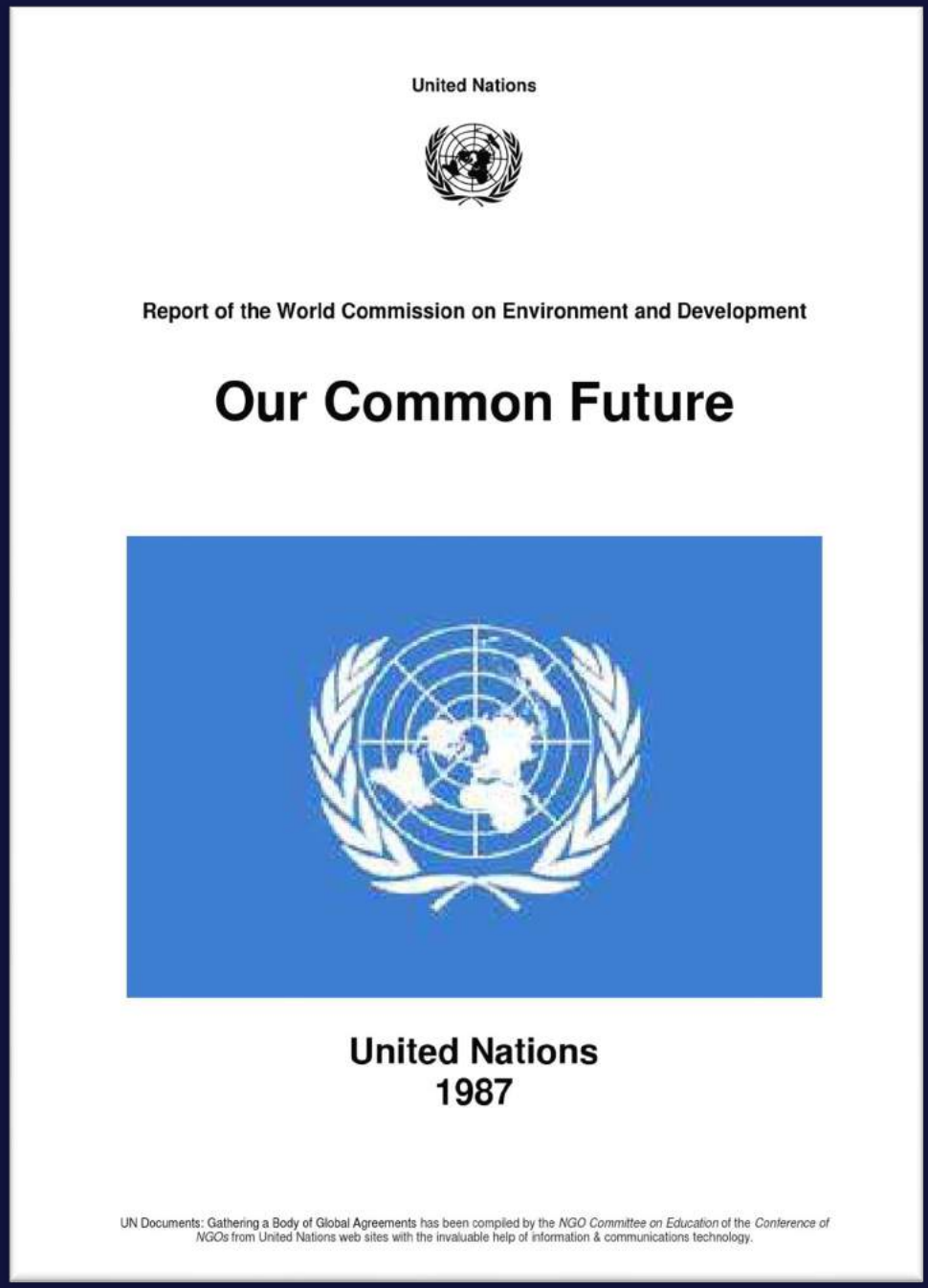


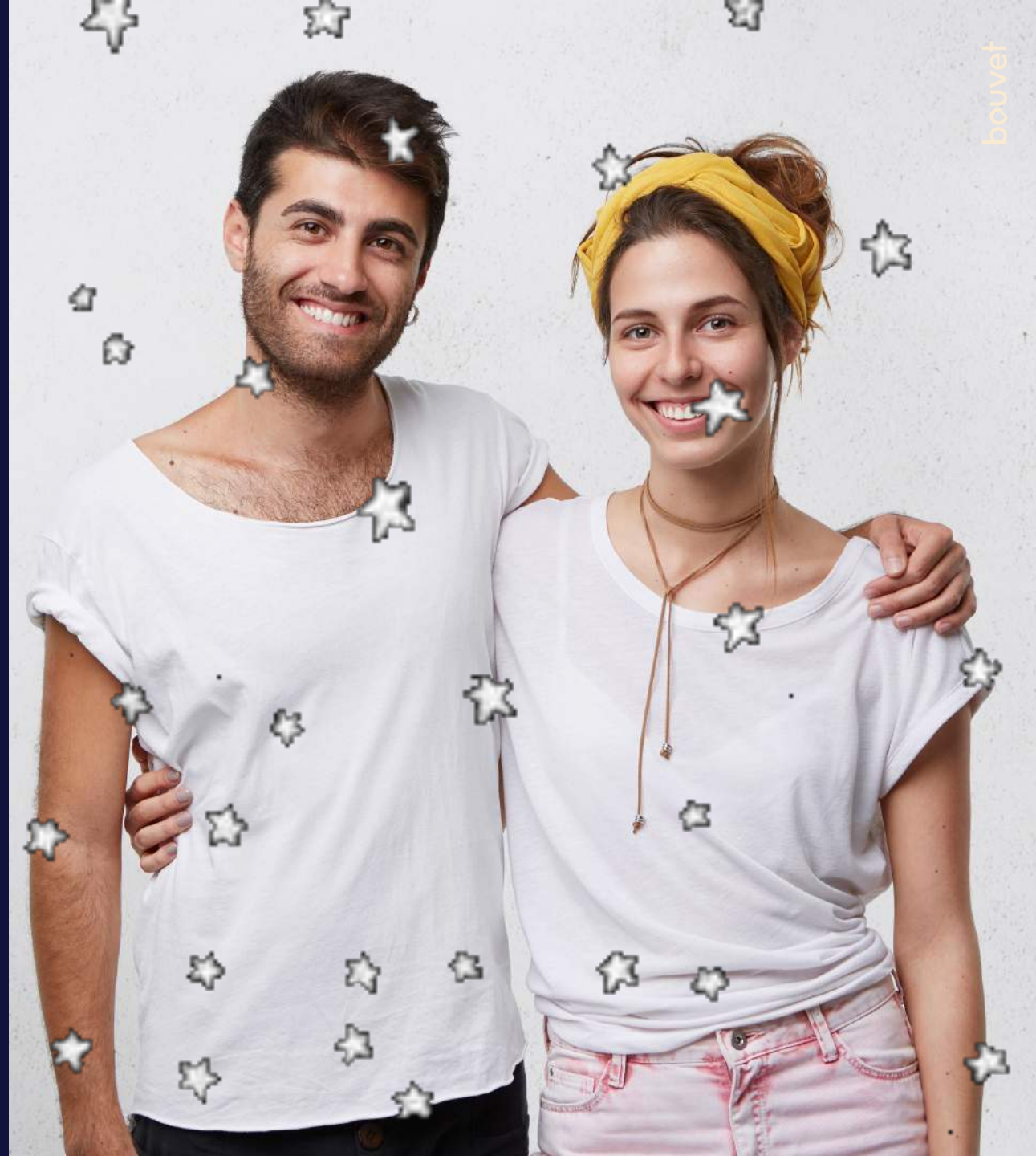
Foto: Gro Røsth

«Informasjon man ikke har, kan ikke misbrukes»

- Jon Bing

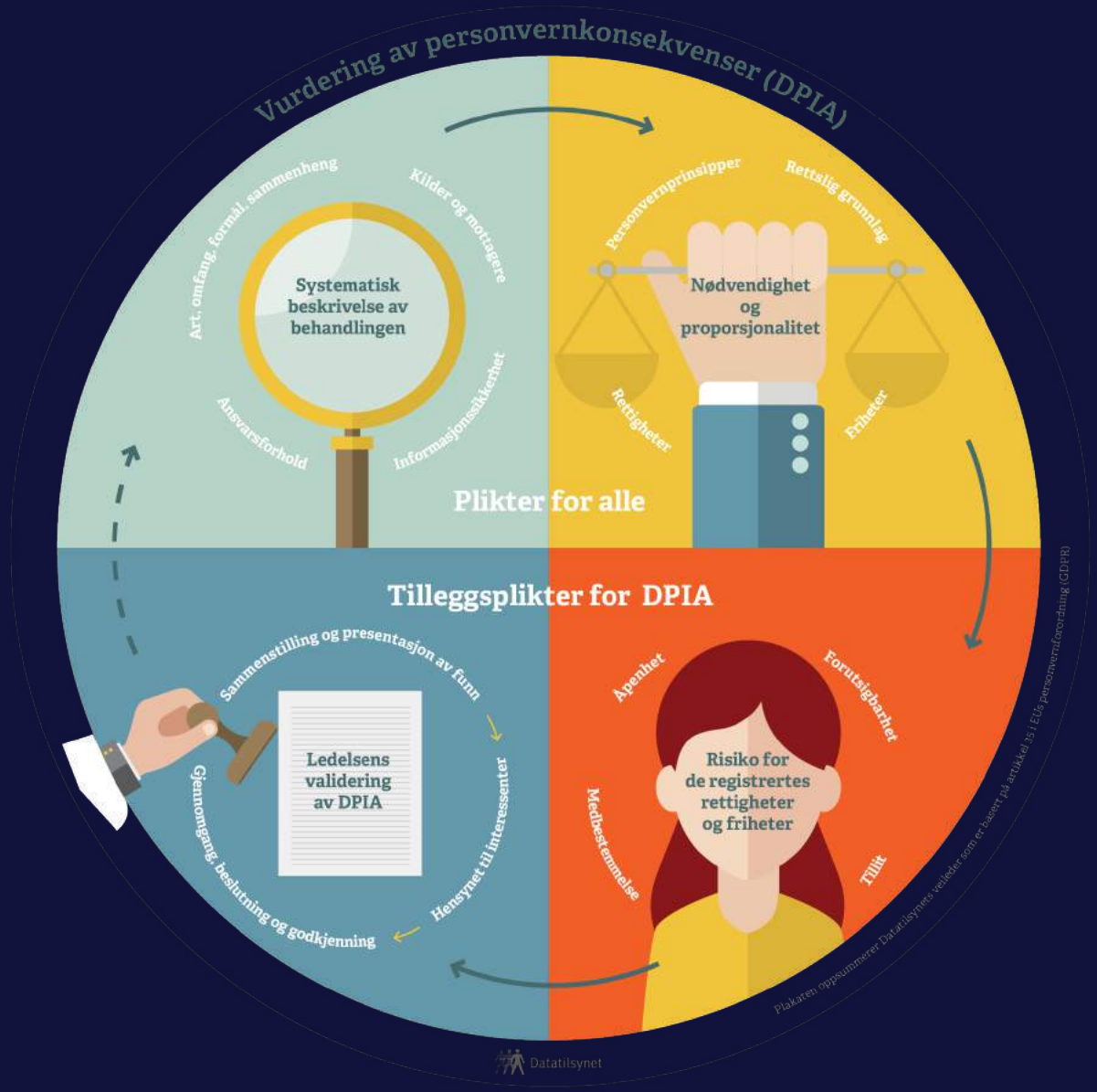
Hvorfor er det viktig?

- Menneskerettigheter: En av virksomhetens viktigste vurderinger, både overfor brukere og ansatte
- Lovlig overholdelse
- Risikostyring
- Intern klarhet i hvor personopplysninger flyter
- Om det skjer for mye avvik, mister vi tillit til det offentlige
- Megatrender: AI og Bærekraft



Hva er en god PVK?

- Forståelig språk
- Involvering av interessenter
- God vurdering av forholdsmessighet
- Riktig lovgrunnlag
- Realistisk risikovurdering
- Troverdig tiltaksplan
- Transparens
- Tverrfaglig tilblivelse
- Forvaltningsvennlig



Men det er vanskelig!

Photo by Gabriel Matula on Unsplash

bouvet

Bakgrunn og metode for denne presentasjonen


06:33
Chat
Personer
Hev
Reager
Visning
Notater
Rom
Apper
Mer
Kamera
Mikrofon
Dele
Forlat
Veronica (gjest)
Eva Jarbekk / Schjødt

World Café workshop hos Schjødt i april

- Rettigheter og friheter
- Konsekvens-skala
- 32 vs 35
- Maler og eksempler,
- Roller og ansvar
- Nødvendighetsvurdering

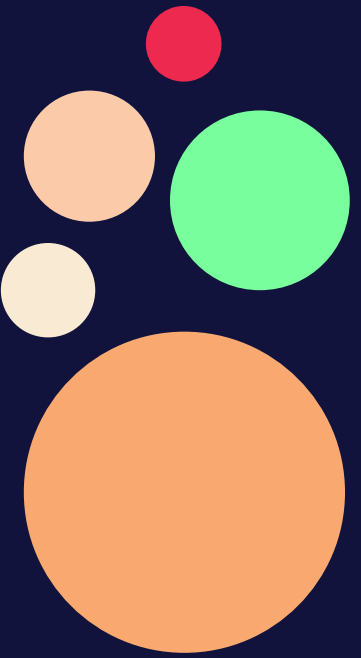
bouvet


Veronica Buer,
Datatilsynet
Kloke, erfarne folk
Eva Jarbekk,
Schjødt
Tone Hoddø Bakås,
Sparebank1

Anbefalinger

Behov og scope

- EDPB og Datatilsynet sine retningslinjer
- Bør forankres i hva folk *opplever*, helst match med behandlingsprotokoll
- Det anbefales å ha en mal for vurdering om når en skal foreta en PVK.



bouvet

32 vs 35!

- Det handler om risikoen for den registrertes friheter og rettigheter
- Alt for mange bruker ROS tankegang i vurderingene

bouvet

Når er risiko høy?

Art

Behandlingens iboende karakteristikk:

- Vanskelig å utøve sine rettigheter
- Uforutsigbarhet, liten åpenhet og usikkerhet om ivaretakelse av prinsipper
- Systematisk behandling
- Særlige kategorier
- Skjevt maktforhold
- Ny teknologi / gammel teknologi brukt på ny måte
- Kompleksitet
- Automatiske avgjørelser

Omfang

Behandlingens størrelse/rekkevidde:

- Antall registrerte involvert (tall eller %)
- Volumet av data (antall variabler, detaljer)
- Lagringstid (kort, tidsavgrenset, permanent)
- Geografisk omfang (lokalt, regionalt, nasjonalt, internasjonalt, globalt)

Formål

Hva skal personopplysningene brukes til:

- Kontrollformål
- Behandling med mål om å ta beslutninger som får betydning for den registrerte
- Å treffe avgjørelser om enkeltpersoner basert på systematisk og omfattende analyse av personopplysninger

Sammenheng

Hvilken forventning om personvern omgir den konkrete behandlingen:

- Forventning om konfidensialitet (helse, velferd, arbeidsforhold..)
- Forventning om privatliv (hjem, rekreasjon..)
- Behandling av personopplysninger fra ulike datasett som er innsamlet for ulike forhold
- Kjeden av aktiviteter i behandling
- Deling med andre behandlingsansvarlige eller virksomheter

Kilde: Datatilsynet

bouvet

Video by Nicky ❤️🌿🐞🌿❤️ from Pixabay

Image: Matthias Kost on Pixabay

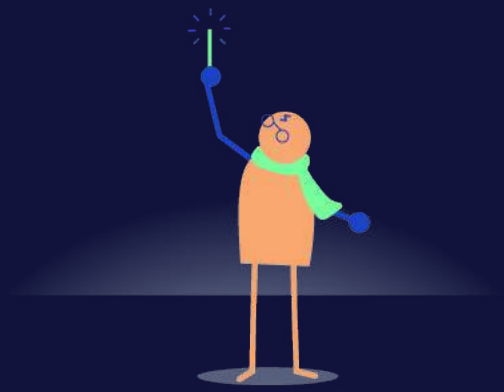
bouvet

Hva er det **verste** som kan skje med brukerne våre?

bouvet

Sannsynlighet

- Sannsynlighet påvirker OM vi skal gjøre en PVK
- Sannsynlighet er ikke så relevant for de enkelte risikoene i PVK. Tenk «Data IMPACT»
- Tiltakene kan redusere risikoen



bouvet

Rettigheter og friheter

- Åpenhet og tillit er viktig - beskriver hva som skjer - f eks. om analyse skal gjøres
- Unngå nedkjølingseffekt hos ansatte om apper skal lastes ned: Vær tydelig på hva en app gir av informasjon til arbeidsgiver, hva appen samler informasjon inn om, lurt å trygge ansatte på at overvåkning ikke skjer
- Listen over friheter bør skrives helt ut – hvilke friheter er det?
- KINS har en scenariobank for medlemmer. Det er bra!

bouvet

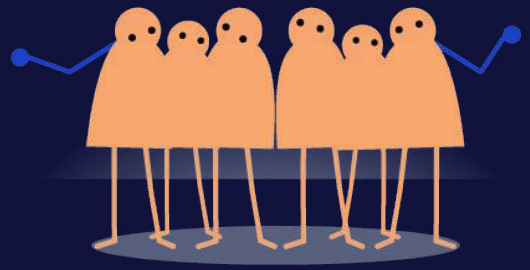
Friheter og rettigheter

Friheter: Privatliv, kommunikasjonsvern, personvern, ytringsfrihet, religionsfrihet, bevegelsesfrihet, bestemmelsesfrihet, retten til å organisere seg, retten til ikke å bli diskriminert

... Og så har vi Rettighetene i GDPR

Konsekvensvurderinger

- Det er viktig at skalaen er felles for virksomheten
- Husk at innvandrere ofte kommer fra annen kultur → andre konsekvenser
- Hva med barna?
- Velferdsteknologi omfatter ofte de svakeste



Creepy-skala

1 Personen er avslappet. Jeg blir overhodet ikke negativt berørt her

2 -Personen kjenner litt "uro". Er dette riktig?

3 - Personen er urolig. Vil dette gå bra? Omdømmetap som er ubehagelig

4. Nakkehårene reiser seg. Hvordan kan virksomheten gjøre dette mot meg

5- Personen blir kald og klam. Hvordan blir livet mitt etter dette?

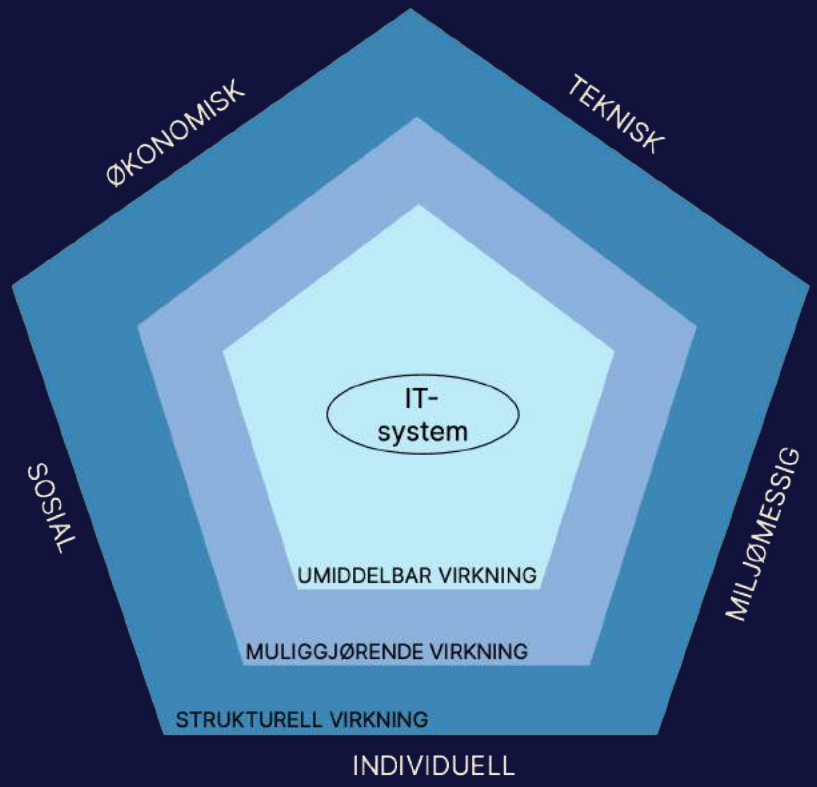
bouvet

Sosioteknisk kompleksitet:
Hvordan sosiale/organisatoriske og tekniske aspekter henger sammen/former hverandre

bouvet

Det finnes systemiske metoder og workshop-teknikker for dette

- SUSAF er en slik
- Designet for ivaretagelse av interessegrupper
- Konsekvenser for **individ** er gjerne forbundet med personvern, og kan føre til strukturelle **sosiale** virkninger som nedkjølingseffekt



https://www.suso.academy/en/sustainability-awareness-framework-susaf/

GoForIT

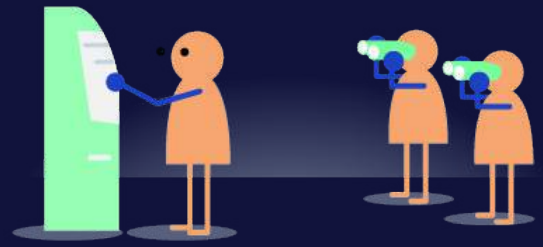
bouvet

Metode, malverk og forvaltning

- Veilederen er VIKTIG. Den bør inneholde noen betraktninger om hvordan en skal håndtere større og mindre sammenhenger
- Egen mal må sees i sammenheng med og avgrenses mot utenlandsoverføringer, ROS, og grunnvurderinger
- Å ha egen software for PVK er ikke viktig. Og det kan ha skape egne utfordringer. Men tenk struktur og moduler fra start
- Wiki kan være lurt!
- Metadata og sporing: Kan dere finne støtte for dette i f.eks lokal Sharepoint-konfigurasjon?

Metode, malverk og forvaltning

- Kompetanse: Tverrfaglig er viktigere enn juss
- Lettfattelig og tilgjengelig språk er viktig
- Det er et sunnhetstegn om omfanget minker, for da har man klart å fokusere
- Det er forbausende lite samarbeid rundt PVK'er. Noe i offsek (kommuner, større etater, KINS), og i innad konserner, men omtrent IKKE i privat sektor)



bouvet

Roller og ansvar

- Avhenger av bransje, størrelse, sentral/distribuert organisasjon, om man har et PVO, ressurser, kompetanse, og om en har eksterne samarbeidspartnere
- Ledelsen bør ha samme forhold til PVK som til Sårbarhetsanalyser
- Å definere eierskap og forvaltningsmodell kan være tidkrevende
- Internrevisjon og compliance: Det kan være utfordrende å håndtere flere roller, spesielt i mindre organisasjoner, fordi folk må ha på seg rett hatt i rett tid

Roller og ansvar

- Involvering av representanter for de registrerte:
  - Usikkerhet rundt når og hvordan, det kan være praktisk utfordrende
  - Skal de få den ferdige dokumentasjonen, eller skal de involveres i prosessen?
- PVO må sikre en armlengdes avstand til DPIA-vurderinger, men..
  - Det kan være utfordrende i mindre virksomheter eller der det er mangel på kompetanse
  - I praksis må PVO veilede en del der, og gode retningslinjer kan avhjelpe på dette
- Det kan oppstå uenigheter i tverrfaglige arbeidsmøter..
  - Dokumentér på en nøytral måte!

Kvalitet følger av forankring

bouvet

Hovedanbefalinger

Forankring i organisasjonen, både internt og med partnere

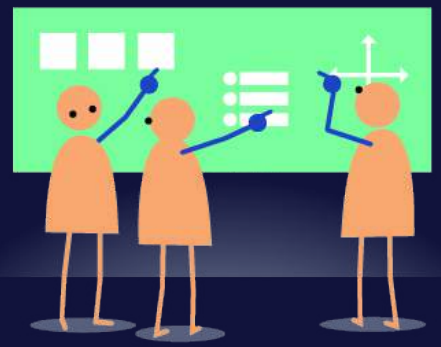
Ta utgangspunkt i rettigheter og friheter, ikke ROS for organisasjon

Gjør det enkelt å forvalte og forholde seg til den helt fra start

bouvet

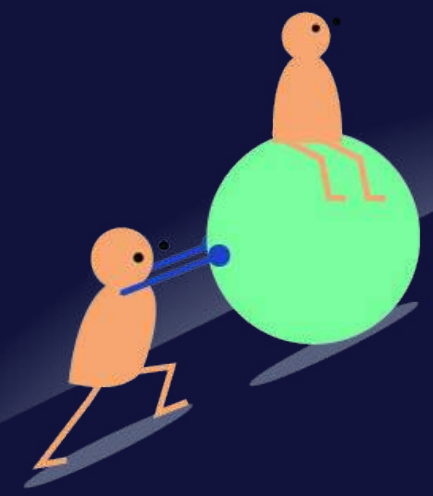
Hva kan hjelpe i virksomheten?

- Forankring, forankring, forankring
- ...fører til investering i oppmerksomhet, folk og tid
- Endringsledelse og kommunikasjon
- Hint: ADKAR (Awarenes, Desire, Knowledge, Ability, Reinforcement)
- Kan dere knytte det opp mot bærekraftarbeid?
- At du og jeg unngår stammespråk



Hva kan hjelpe i samfunnet?

- Bransjenormer
- En egen konferanse!
- ...at bransjeorganisasjoner arrangerer nettverksmøter om personvern
- Personvernpolitikk!
- At du og jeg unngår stammespråk



Takk til...

- Eva Jarbekk
- Tone Hoddø Bakås
- Veronica Buer
- Alle som kom på workshop

Takk for meg!

Simen.sommerfeldt@bouvet.no

Video: Compressorhead (https://www.youtube.com/watch?v=3RBSkq-_Sto)

bouvet