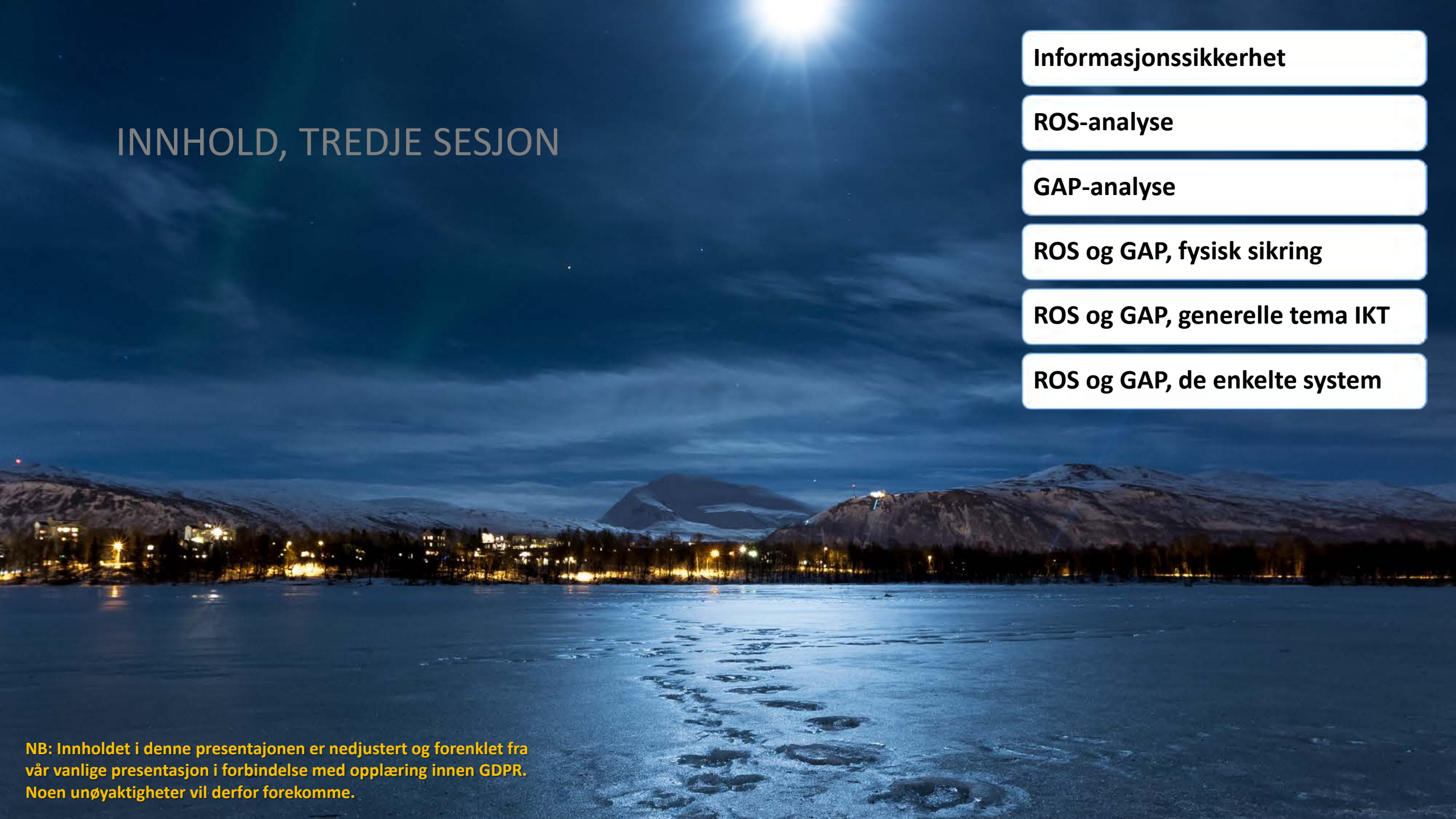

# Del 3 Fagdag GDPR - Arkiv Troms

Fokus på ny personopplysningslov og personvern

*Ole Mikalsen, GDPR-konsulent, IT Partner Tromsø AS*

# INNHOLD, TREDJE SESJON

- Informasjonssikkerhet
- ROS-analyse
- GAP-analyse
- ROS og GAP, fysisk sikring
- ROS og GAP, generelle tema IKT
- ROS og GAP, de enkelte system



**NB: Innholdet i denne presentajonen er nedjustert og forenklet fra vår vanlige presentasjon i forbindelse med opplæring innen GDPR. Noen unøyaktigheter vil derfor forekomme.**

# Styringssystem for informasjonssikkerhet

Styringssystemet er som en del av bedriftens kvalitetssystem, prosedyrer og retningslinjer for systematisk arbeide med å sikre data i bedriften

# Sikkerhetsforpliktelser

I tillegg til GDPR finnes det flere sikkerhetsforpliktelser (i EUs nye regler).

**Lov og forskrift**

- IKT-forskriften - «risiko styres innenfor akseptable grenser i forhold til foretakets virksomhet» § 3
- Arkivloven - «ordnet og innrettet slik at dokumentene er sikret som informasjonskilder for samtid og ettertid» § 6
- Arbeidsmiljøloven - på alle plan i virksomheten, herunder ved varsling
- Produktansvarsloven - «den sikkerhet som en bruker eller allmennheten med rimelighet kunne vente» § 2-1
- Helseregisterloven - «databehandlingsansvarlige og databehandler skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet» § 21
- Bokføringsloven - «betryggende sikret mot ødeleggelse, tap og endring» § 13
- Aksjeloven - «(1) [...]. Styret skal sørge for forsvarlig organisering av virksomheten.» § 6-12
- Andre regelsett omfatter kommunikasjonsverndirektivet (e-Privacy Direktive), som i disse dager overhales for å harmonere med GDPR. Se særlig artikkel 4, som setter krav til «appropriate technical and organisational measures to safeguard security of its services».

serit
IT Partner Tromsø

# Hva er informasjonssikkerhet?

Informasjonssikkerhet handler om å sikre at informasjonen:

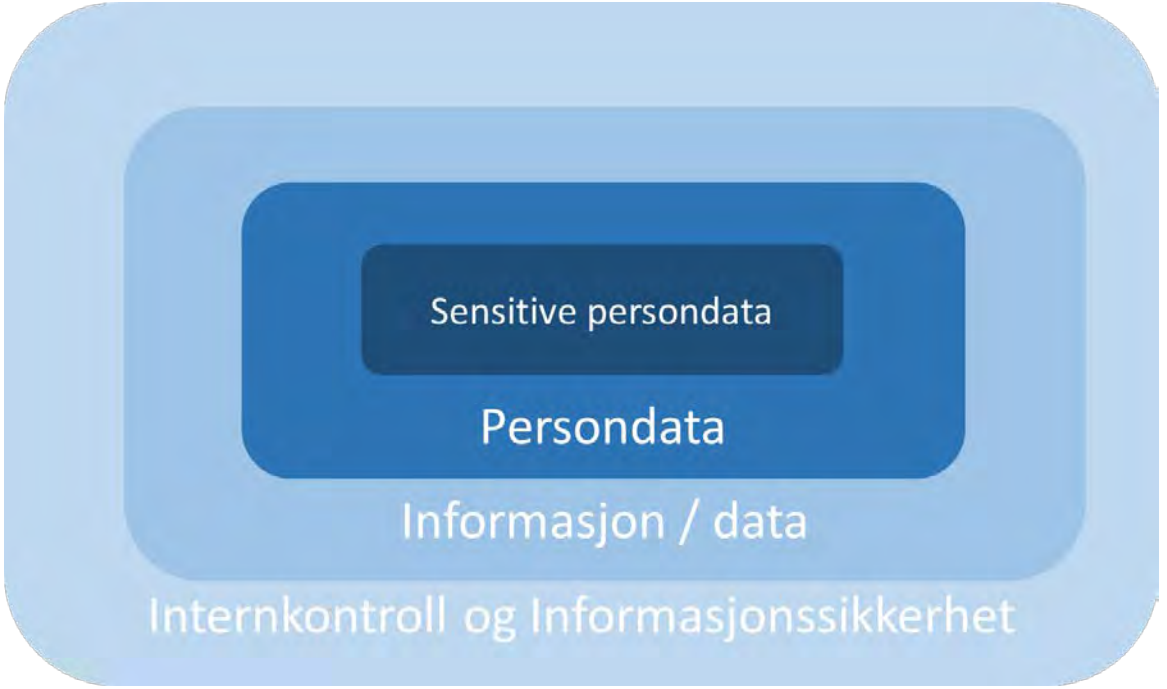
- ikke blir kjent for uvedkommende (konfidensialitet)
- ikke blir endret utilsiktet eller av uvedkommende (integritet)
- er tilgjengelig ved behov (tilgjengelighet)

Dette er også kjent som CIA (confidentiality, integrity, availability).

Et viktig verktøy for å oppnå dette er et styringssystem for informasjonssikkerhet, også kalt internkontroll-system.


# Informasjonssikkerhet og GDPR

- Personinformasjon utgjør bare en del av virksomhetens totale informasjonsmengde
- Ved å ha god generell informasjonssikkerhet, og tilpasse disse for kravene i GDPR så er man på god vei til å sikre at man behandler personinformasjon riktig




# Uønskede hendelser

Indentifiser uønskede hendelser:

- **Eksterne trusselaktører** – eksterne trusselaktører som gjennom bevisste handlinger prøver å få tilgang til systemer og informasjon
- **Egeneksponering** – en virksomhet gjør seg selv mer sårbar dersom egensikringen ikke fungerer tilfredsstillende. Mangelfullt sikkerhets-arbeid vil kunne medføre at skjermingsverdig informasjon og systemer blir eksponert for omverdenen. Dette vil eksempelvis ofte bli resultatet dersom regelverket som regulerer sikkerhetstjenesten fravikes
- **Utro tjenere –** egne ansatte kan utgjøre en risiko og kan under visse omstendigheter bevisst bidra til at informasjon kompromitteres. Drivkreftene kan være egen vinning eller komme som et resultat av press fra eksterne aktører


serit
IT Partner Tromsø

# Tiltak

- Iverksettes når risiko ikke kan aksepteres
- Kan benytte organisatorisk og/eller teknisk tiltak
- Kan være forebyggende eller skadebegrensende
  - Barriere – forhindre eller redusere mulighet
  - Deteksjon – avdekke hendelser
  - Reaksjon – handlemåte ved hendelse


# Retningslinjer og rutiner

Resultatet av arbeidet med kartlegging og risiko analyse vil danne grunnlag for arbeidet med retningslinjer og rutiner.

- Det utarbeides rutiner for varsling av mulige sikkerhetshendelser
- Det utarbeides sikkerhetsdokumentasjon med retningslinjer, rutiner, instruksjoner og veiledninger
- Det utarbeides en sikkerhetspolicy for bedriften

# Styringssystem og GDPR

Ved å bruke et styringssystem for informasjonssikkerhet i GDPR arbeidet sikrer man at man har nødvendig dokumentasjon på de tekniske og organisatoriske tiltak som er gjort, og at man har en risikobasert tilnærming

- Det er ikke noe krav i forordningen at et spesifikt styringssystem skal følges for å oppnå samsvar, men det poengteres at det skal gjøres nødvendige «technical and organizational measures »
- Loven poengterer behovet for risikobasert tilnærming
- De tiltak som gjøres skal dokumenteres

# Risiko og sårbarhetsanalyse

Alle virksomheter må vurdere informasjonssikkerhetsmessig risiko knyttet til behandling av personopplysninger

serit
IT Partner Tromsø

# ROS-ANALYSE

ROS: Risiko og sårbarhetsanalyse

I GDPR sammenheng gjør vi risiko og sårbarhetsanalyse med hensyn til personopplysninger

Alle virksomheter må vurdere informasjonssikkerhetsmessig risiko knyttet til behandling av personopplysninger

# Risiko og sårbarhetsanalyse

ROS-analyse består av å identifisere uønskede hendelser

- kartlegge sannsynlighet og konsekvenser av disse
- definere tiltak for å redusere eller forhindre konsekvens
- prioritere rekkefølge for tiltak

Eksempel på uønskede hendelser:

- strømbrudd, innbrudd, brann, flom, osv
- personellmangel pga sykdom, ulykker, dødsfall
- Datautstyr kommer på avveie
- Persondata kommer på avveie
- Data mistes ved virus, kryptering, osv


# Risiko-beregning

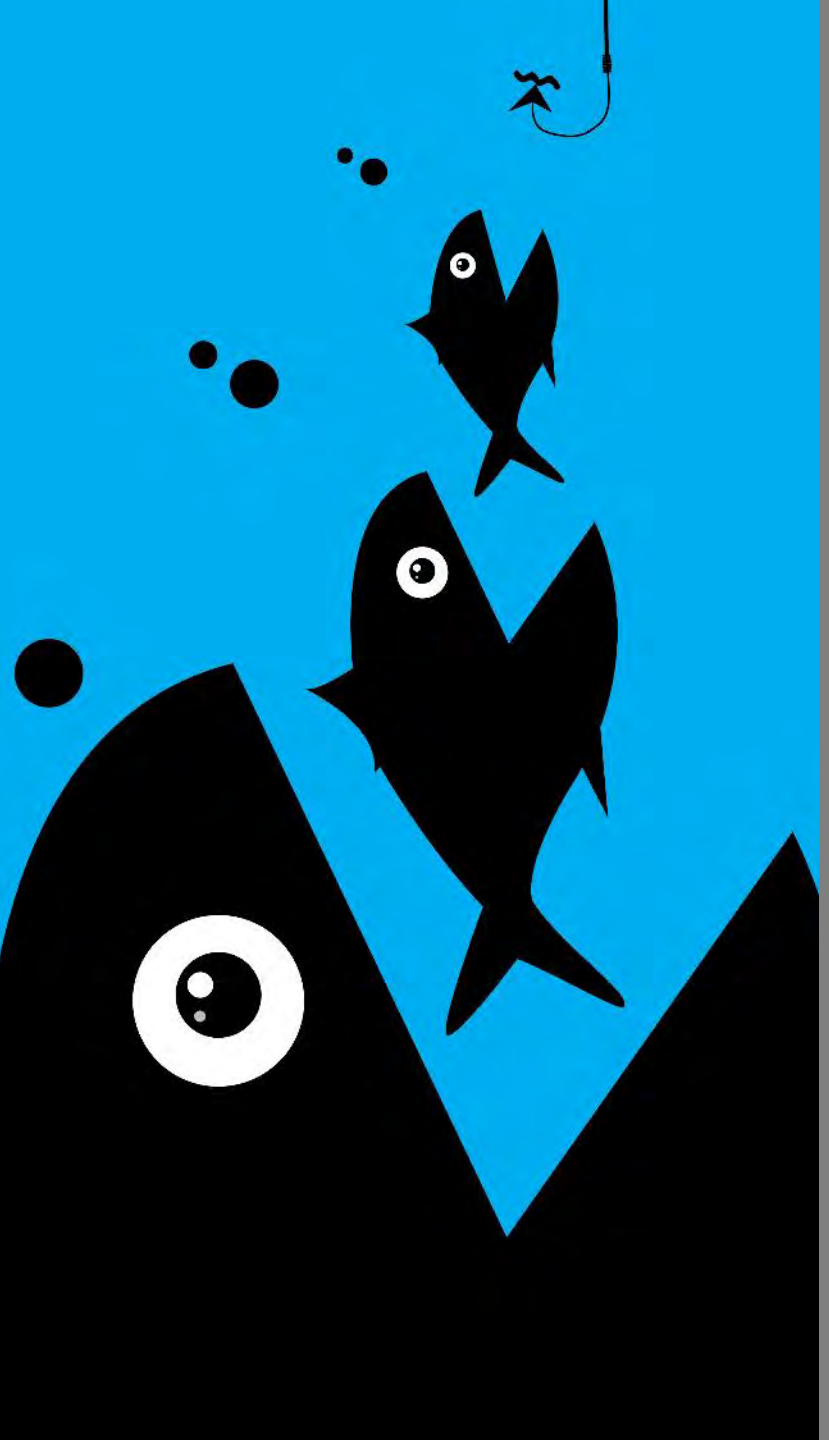
Risikoen beregnes i en tabell som Sannsynlighet x Konsekvens

| Konsekvens | | | | | |
|---|---|---|---|---|---|
| | 4 | 4 | 8 | 12 | 16 |
| | 3 | 3 | 6 | 9 | 12 |
| | 2 | 2 | 4 | 6 | 8 |
| | 1 | 1 | 2 | 3 | 4 |
| | | 1 | 2 | 3 | 4 |
| | | Sannsynlighet | | | |


# Risiko-beregning med 4 nivåer

Risikoen forenkles og betegnes ofte som
Liten, Middels eller Stor, - eller Lav, Moderat, Høy

| Konsekvens | | | | | |
|---|---|---|---|---|---|
| | Svært stor | Moderat | Høy | Høy | Høy |
| | Stor | Moderat | Moderat | Høy | Høy |
| | Middels | Lav | Moderat | Moderat | Høy |
| | Liten | Lav | Lav | Moderat | Moderat |
| | | Lav / sjelden | Moderat | Høy | Svært høy |
| | | | Sannsynlighet | | |



# Risiko, eksempel med akseptkriterier med 3 nivå

| Konsekvens | Sannsynlighet: Lav | Moderat | Høy |
|---|---|---|---|
| Stor | | | |
| Middels | | | |
| Liten | | | |


serit
IT Partner Tromsø

# Triggere for risikovurderinger

Risikovurdering bør gjennomføres

- Før behandling starter
- Ved endring i behandlingen
- Ved interne eller eksterne endringer som kan påvirke informasjons-sikkerhet og personvern


# Hvordan håndtere risiko

- Endre risiko
  - Implementere ytterligere eller fjerne eksisterende tiltak
- Akseptere risiko
  - Dersom innenfor akseptable grenser. Dokumenter aksept
- Dele risiko
  - Forsikring, databehandler. Ansvar forblir hos behandlingsansvarlig
- Unngå risiko
  - Slutte med aktiviteten


# Kategorier for tiltak

- Forebygge
  - Redusere sannsynligheten for at hendelsen inntreffer og/eller mulig konsekvens
- Oppdage
  - Sikre at hendelsen oppdages
- Reagere
  - Sikre at oppdagede hendelser håndteres og unngå gjentakelse

Tiltak kan være fra flere kategorier samtidig

# GAP - Analyse

Alle virksomheter bør gjøre en analyse på sin behandling av persondata for å avdekke om den er som de ønsker

# GAP analyse

I GAP analyse vil man av ut fra bestemte mål

- Sammenligne virksomhetens nåsituasjon og den ønskede fremtidige situasjonen
- identifisere forskjellene mellom dem (avviket)
- og lage en plan for å fylle gapet (tiltak)

Oftest vil det være naturlig å se på GAP også i forbindelse med ROS-analyser. Når man finner et problemområde, faller det naturlig å samtidig se etter løsninger

# Vurdering av informasjonssikkerhet for fellessystemer

I forbindelse med GDPR er det en del sikkerhets-faktorer som går igjen for mange systemer. Disse sikkerhetsfaktorene kan vi behandle og gjøre risiko og GAP analyse på en gang og dekke alle systemene

Selv om vi i GDPR sammenheng primært konsentrerer oss om personvern-faktorer så vil mange av de vurderingene vi gjør gjelde for store deler av virksomheten generelt sett

# ROS og GAP - Fysisk sikring

Overordnede analyser av tekniske og organisatoriske tiltak relatert til fysisk sikring av bedriftens verdier

serit
IT Partner Tromsø

# Eksempler på områder hvor vi kan gjøre felles ROS og GAP

- Klassifisering av lokaler
- Tilgangskontroll til lokaler
- Brannsikting av lokaler
- Sikring ved strømbrudd (UPS)
- Generell rollebasert tilgangskontroll

- Ser dere andre ytre faktorer dere vurdere?

# Klassifisering av lokaler

Man klassifiserer lokaler for å kunne definere retningslinjer og rutiner for databehandling som vil være forskjellig i forskjellige lokaler

Ved klassifisering av lokaler tar man hensyn til både egne lokaler og offentlige lokaler. Egne lokaler vil man ofte klassifisere i forskjellige nivå

Viktige faktorer å tenke på når man klassifiserer lokaler

- Hvordan opptrer man i de ulike typer lokaler?
- Hvem har tilgang til de forskjellige typer lokaler?
- Hva snakker du om til hvem i de ulike typer lokaler?
- Diskutere personer? Konkurrenter? Kollegaer?
- Hvor behandles sensitiv informasjon?
- Hvor behandles persondata?

# Tilgangskontroll til lokaler

## ROS

- Uvedkommende kommer seg inn i lokaler utenom arbeidstid?
- Uautorisert personell får tilgang til lokaler de ikke skal ha tilgang til f.eks regnskapskontor eller personalarkiv

## GAP

- Har vi klassifisert våre lokaler?
- Har vi kontroll med tilgang til våre lokaler?
- Har vi elektronisk logging av tilgang utenom normal åpningstid?
- Har vi kontroll med intern tilgang til lokaler med begrenset klassifisering?

# ROS og GAP - Generelle tema IKT

Noen generelle tiltak vil sikre mange av de ulike enkeltsystemer overordnet sett

# Områder innen IKT hvor vi kan gjøre felles ROS og GAP

- Backup/restore
- Antivirus-system på PCer og servere
- Brannmur med UTM teknologi
- Epost sending/mottak med sikkerhetssystem
- Eksternt tilgangssystem som f.eks VPN


# Antivirussystem på PCer og servere

## ROS

- Virus/malware skader data. F.eks ved kryptering
- Virus/malware fører til datalekkasje
- Virus/malware gjør systemer utilgjengelige eller ikke funksjonelle
- Antivirus system fungerer ikke pga manglende oppdatering eller lisens

## GAP

- Har vi antivirus system for PCer og servere?
- Har vi rutiner for drift og vedlikehold av disse systemene?
- Har vi rutiner for kontroll av disse systemene?


# Epost sending/mottak med sikkerhetssystem

ROS

- Epost med skadelige programvare eller linker til skadelig programvare slippes gjennom
- Epost systemet vårt blir svartelistet pga spam
- Epost  kommer ikke inn pga manglende drift og vedlikehold av systemet
- Epost sikkerhetssystem fungerer ikke pga manglende oppdatering eller lisens

GAP

- Har vi epost gateway med sikkerhetssystem som kontrollerer og evt filtrerer mail inn/ut?
- Har vi rutiner som sikrer at kun godkjente interne systemer kan sende epost ut?
- Har vi rutiner for drift og vedlikehold av disse systemene?
- Har vi rutiner for kontroll av disse systemene?


# System for ekstern tilgang som f.eks VPN

## ROS

- Uvedkommende får tilgang til interne system med stjålet brukernavn/passord
- Egne brukere kopierer data ut av huset
- Interne systemer blir eksponert pga for svak sikkerhet i f.eks kryptering eller sertifikater

## GAP

- Har vi rutiner for hvem som kan koble seg til eksternt? Både egne medarbeidere og leverandører?
- Har vi rutiner for når VPN skal brukes, f.eks ved bruk av usikrede trådløsnett
- Har vi tilstrekkelig autentisering av brukere som bruker ekstern tilkobling?
- Har vi rutiner for drift og vedlikehold av disse systemene?
- Har vi rutiner for kontroll av disse systemene?


# ROS og GAP - De enkelte systemer

Vurderinger å gjøre for de enkelte systemer vi kartlegger og dokumenterer i GDPR-sammenheng

# Analyse og dokumentering for de enkelte system

De enkelte systemer bør vurderes om de har egne risikoer via en ROS og GAP-analyse på systemet

ROS

- Vurder om dere finner spesielle risikoer og hendelser som påvirker det enkelte system
  - Er systemet mer utsatt enn andre?
  - Trenger det spesiell beskyttelse?

GAP

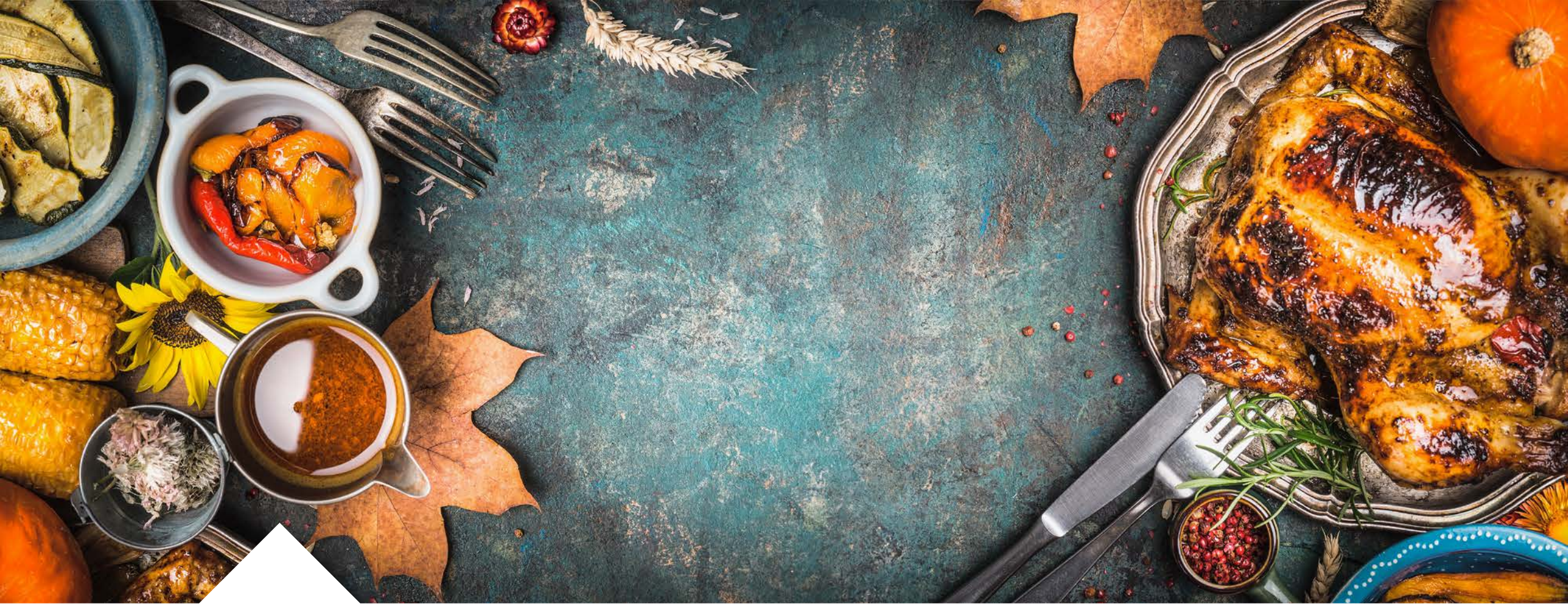
- Vurder om systemet kan gis bedre sikkerhet
- Spesifiser mulige forslag til forbedringstiltak

# Eksempel:
# Behandlinger, formål og grunnlag

Har vi fullført/definert/beskrevet:

- Formål og grunnlag spesifisert?
- Behandlinger avstemt med formål?
- aktuell behandling for grunnlag til databehandleravtalen?

# SPØRSMÅL TIL DENNE SESJONEN?



# Lunsj: 11.45 – 12.45

xxxx

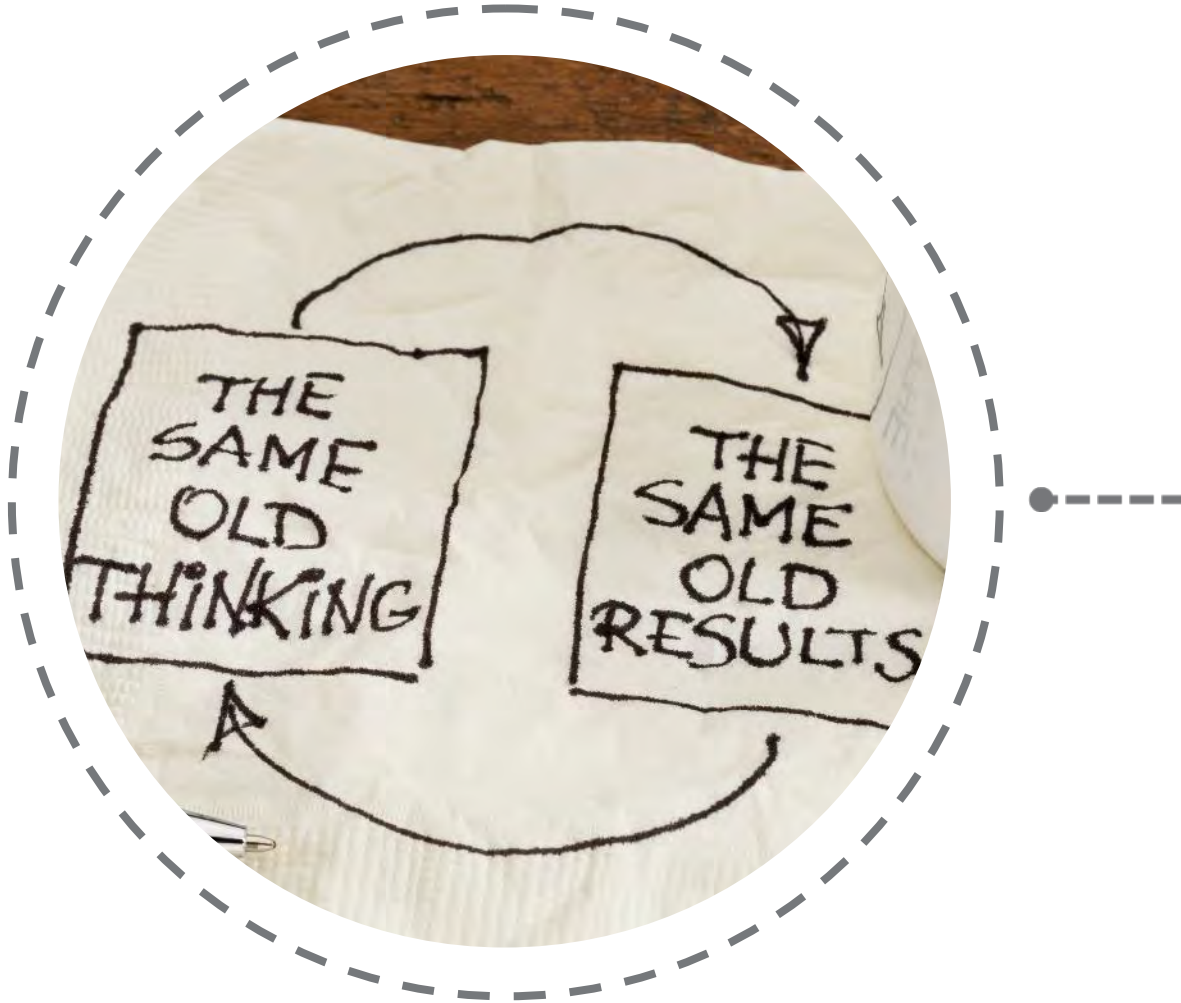

# Bevistgjøring og opplæring

Risikoområder, bevisstgjøring og opplæring i forhold til nytt regelverk

# Behov for informasjon

Det er alltid behov for opplæring, spesielt i det man ikke bruker mest tid på. For mange ansatte er personvern ikke det man tenker først på ved utøvelse av ens jobb

Når selskapet har vært gjennom en GDPR-prosess, vil det i de fleste tilfeller være behov for å informere og styrke de ansattes kunnskaper pga endringer i prosesser og prosedyrer



# Opplæring av ansatte

Nøkkelen til vellykket personvern er høyt kunnskapsnivå og bevissthet

# Hvilken opplæring og informasjon?

Hva ønsker dere så å gi opplæring i ?

- Informere om GDPR prosessen
- Informere om de registrertes (ansatte og kunders) nye rettigheter
- De nye policyer og rutiner utarbeidet/ endret i løpet av GDPR prosessen
- Ny personverkerklæring ansatte
- Nye samtykkeskjema kunder
- E-post policy
- Nye varslingsrutiner
- Øke generell bevisshet rundt personvern

# Grupper av ansatte

Hvem skal dere gi de ulike informasjoner til?

- Samme info til alle eller differensiert?
- Ulik info ut fra nivå i selskapet?
- Ulik info ut fra funksjon?
- Ulik info ut fra lokasjon?
- Osv…

# Aktuelle informasjonskanaler?

På hvilken måte vil dere gi økt kunnskap?

- Elektronisk eller papir?
- Mail
- Intranett
- Informasjonsskjermer
- Mobil
- Brosjyrer
- Møter
- Seminarer
- Kurs
- Holdningskampanjer
- Kulturbygging
- Annet?

# Aktivitetskalender

Planlegg kombinasjon av medier, kanaler, innhold og ansattegrupper, og sett opp en informasjonskalender

- Lag aktuelt informasjonsmateriell
- Sett av ressurser for gjennomføring
- Book evt eksterne forelesere
- Innkall de aktuelle grupper til riktig tid


# Diskusjon/planlegging

Hvordan ser dere for dere at det er aktuelt å gjøre dette i deres organisasjon?

- Styrker?
- Svake sider?
- Problemområder og utfordringer?
- Egnede arenaer og kommende events?

# Innhold workshop

Dere deles inn i grupper

Velg et par områder der dere mener dere kan ha utfordringer innen håndtering av personopplysninger

- Beskriv noen uønskede hendelser og konsekvensen av dette
- Beskriv nåsituasjonen og ønsket situasjon for disse
- Foreslå tiltak for å :
  - Unngå/håndtere uønskede hendelser
  - komme over til ønsket situasjon

Opplæring

- Lag en generell strategi og opplæringsplan innen personvern (håndtering av personopplysninger)
- Foreslå hvordan dere vil gi opplæring innen de områder dere så på ovenfor


# Takk for i dag!

En liten oppfordring til slutt:
Styrk kvaliteten på behandlingen av personopplysninger i din kommune!