Hvordan kan DU bidra til et sikrere næringsliv?

Gry Helene Stavseng

Gagn Consulting AS
www.gagn.no

GAGN

Christine Korme, Abelia
Debatten, NRK 02.02.2018

Vi **mangler kompetanse**, hos oss som allerede er i jobb.

Kriminelle vil alltid bruke det **svakeste leddet**. Det kan være din eller min mobiltelefon, om den ikke er **oppdatert**.

Man må følge **norsk lov**, og gjennomføre **risiko- og sårbarhetsanalyser**.

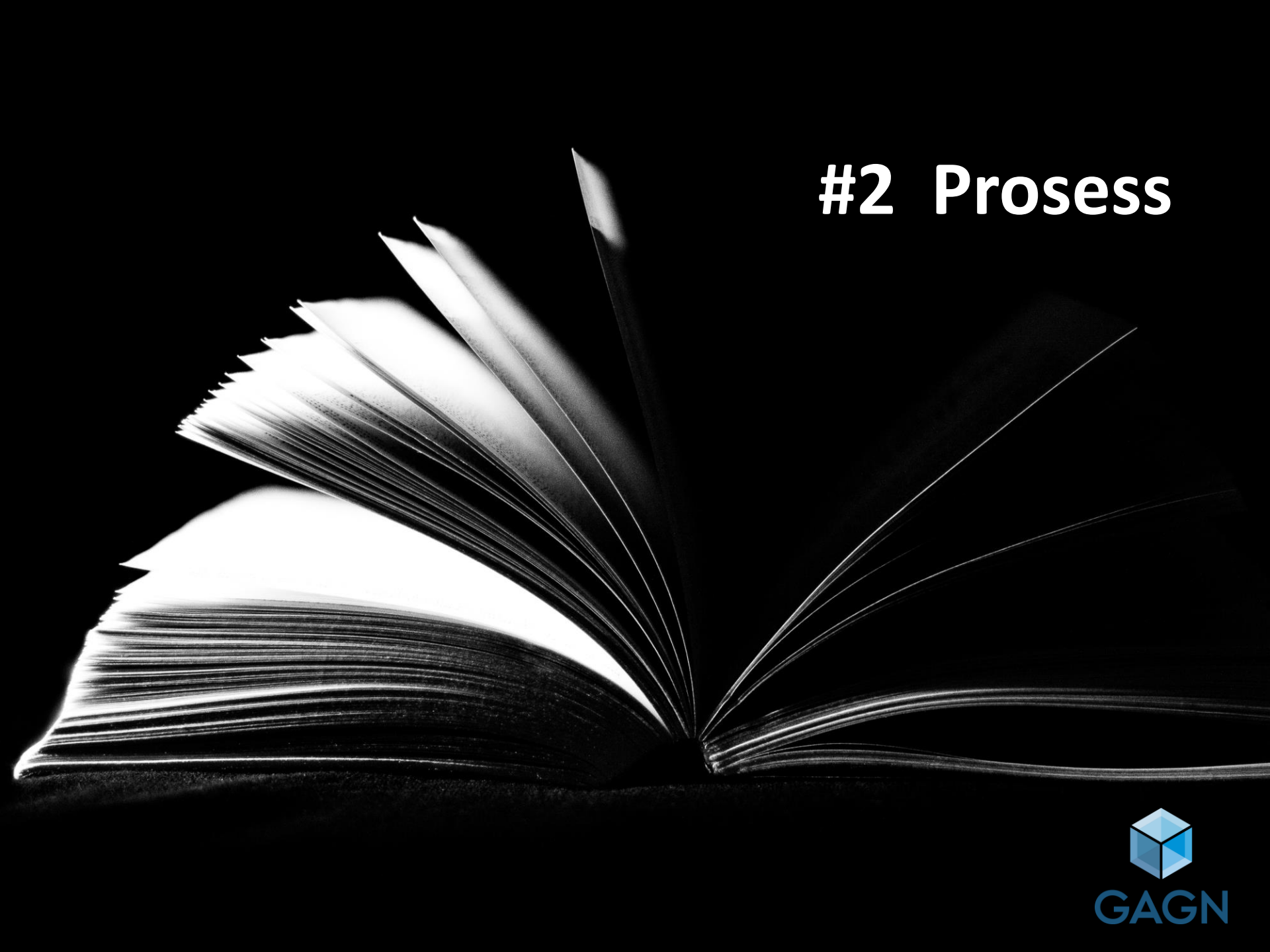
GAGN

Tre slags sårbarheter

#1 Tekniske

GAGN

#2 Prosess




#3 Menneske
GAGN

Prosedyrer og rutiner

GAGN

Organisasjonskultur og kommunikasjon

GAGN

Sikkerhetskultur

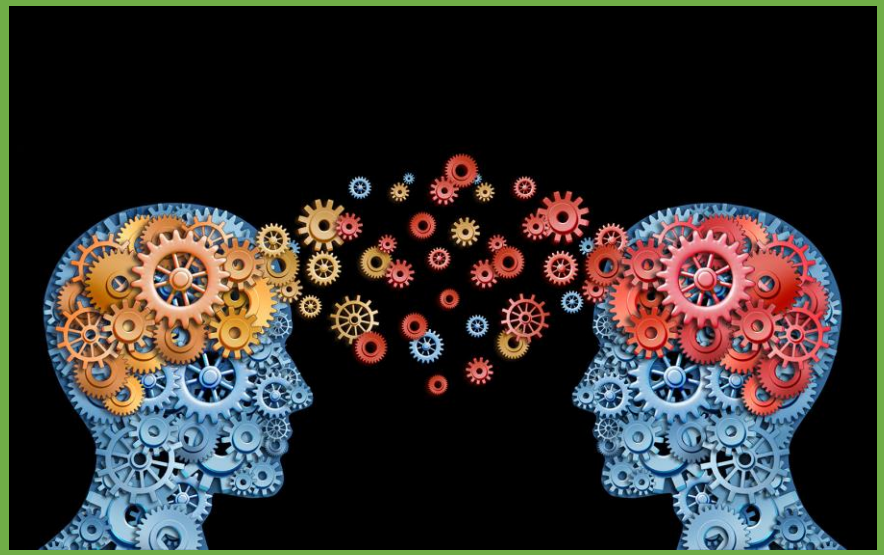
- Ikkje eksisterande
- Regelfokusert
- Promotering av bevissthet og endring
- Langvarig vedlikehald
- Måling

Security Awareness Maturity Model

GAGN

Bevisstgjerings-program

Opplæring og haldningsskapande arbeid for å gjere menneske klar over kva truslar som fins og korleis desse skal taklast



GAGN

Nasjonal sikkerhetsmåned i oktober

NorSIS tilbyr en ferdig opplæringspakke for alle bedrifter

Bidra i dugnaden og gje dei tilsette opplæring i informasjonssikring

www.norsis.no
www.sikkert.no

Du bruker ikke samme børste overalt,
hvorfor bruke samme passord?

STOPP TENK KLIKK

NorSIS
Norsk senter for informasjonssikring

sikkert.no

GAGN

Risiko- og sårbarhets-analyse

Risikovurdering

Norsk standard for risikovurdering NS-5814, Krav til risikoanalyser	ISO 27005 – Risk Management for information security	ISO 31000 – Risk management
Cobit 5 for Risk / Risk IT Framework fra ISACA	Datatilsynets veiledning	NorSIS veiledning

GAGN

GDPR
EU si personvernforordningslov

- I dag: Rutiner som gjeld personopplysningslova
- Ny lov = Nye plikter = Nye rutiner
- Verksemda si leiing har ansvar for å utforme rutiner. Alle må kjenne til og følge reglane
- Ressurskrevjande å sette seg inn i nye reglar, lage nye rutiner og lære opp tilsette.

Nye personvernregler fra 2018. Hva betyr det for din virksomhet?

Hva blir nytt?

lle norske virksomheter får ye plikter
lle virksomheter må sette seg inn den nye lovgivningen og finne ut vilke nye plikter som gjelder dem. edelsen må sørge for å få på plass tiner for å overholde de nye iktene. Alle ansatte må følge de e rutinene når reglene trer i kraft.

e skal ha en forståelig personvern-læring
rmasjon om hvordan din virksom-behandler personopplysninger skal lett tilgjengelig og skrevet på en elig måte. Det nye lovverket strengere krav til informasjonens g innhold enn dagens lovgivning. rmasjon som gis til barn, skal s barnas forståelsesnivå.

vurdere risiko og rnkonsekvenser
tiltak utgjør en stor risiko ernet, må virksomheten hvilke personvernkonse-an ha. Hvis utredningen en er stor og dere selv re den, skal Datatilsynet håndsdrøftelser.

onvern inn
krav til at nye til-arbeides på en ennlig måte. onvern. Den nstillingen emer.

Europa må også følge forordningen, dersom de tilbyr varer eller tjenester til borgere i et EU- eller EØS-land. Dette gjelder også om de ikke direkte tilbyr tjenester, men kartlegger adferden til europeiske borgere på nett. De som er etablert i flere land i Europa, skal bare trenge å snakke med personvern-myndighetene i det landet der de har sitt europeiske hovedkvarter.

7 Alle databehandlere får nye plikter
Databehandlere er virksomheter som behandler personopplysninger på oppdrag fra den ansvarlige virksomheten. Ofte er det snakk om leverandører av IT-tjenester. De nye reglene pålegger databehandlere å ha rutiner for innsamling og bruk av personopplysninger. Databehandlere skal også si ifra til oppdragsgiveren sin hvis de får instrukser som er i strid med loven. Oppdragsgiver skal også godkjenne databehandlerens underleverandører. Databehandlere kan også bli holdt økonomisk ansvarlig sammen med oppdragsgiver.

8 Alle bør samarbeide i egne nettverk og følge bransjenormer
De nye reglene oppmuntrer til sektorvis utforming av retningslinjer og bransjenormer. Om dere følger bransjenormer, vil dere ha de viktigste rutinene på plass. Datatilsynet skal godkjenne bransjenormene.

9 Alle får nye krav til avvikshåndtering
Reglene for håndtering av sikkerhetsbrudd blir strengere. Forordningen stiller krav til når det skal varsles, hva varselet skal inneholde og hvem som skal varsles. Kort sagt skal man si fra raskere og oftere enn man gjør i dag.

10 Alle må kunne oppfylle borgernes nye rettigheter
Den enkeltes rett til å kreve at hans er hennes personopplysninger es blir styrket. Dette kalles «retten glemt». Norske og europeiske il blant annet kunne kreve å ersonopplysningene sine r til en annen i et vanlig Dette kalles «data-n også motsette nvendelser fra en en måned.

Hva bør dere gjøre nå?

1 **Ha oversikt over hvilke personopplysninger dere behandler**
Alle virksomheter som samler inn eller bruker personopplysninger skal ha oversikt over hvilke personopplysninger det er snakk om, hvor de kommer fra og hva som er det rettslige grunnlaget for behandlingen. Sørg for å ha en slik oversikt. Det er et krav som gjelder også etter dagens lov.

2 **Sørg for å oppfylle dagens lovkrav**
Overgangen til de nye reglene blir lettere om dere etterlever kravene i personopplysningsloven, som gjelder i Norge i dag. Har dere gode rutiner for internkontroll som fungerer etter hensikten og er kjent i organisasjonen, er det lettere å få oversikt over hva dere må endre.

3 **Sett dere inn i det nye regelverket**
Dere finner forordningsteksten på Datatilsynets nettsider. Der fyller vi også på med artikler om de nye reglene etter hvert som vi utarbeider dem.

4 **Lag rutiner for å følge de nye reglene**
Gå gjennom rutinene dere har for behandling av personopplysninger. Oppdater dem etter nytt regelverk der det trengs. Dokumenter de nye rutinene, og legg en plan for nødvendige endringer. Er systemene deres laget for å ivareta kravet til innebygd personvern, dataportabilitet og personvern som standardinnstilling? Klarer de å fange opp og besvare b fra borgerne in Endringer i syst tar tid. Begynn

datatilsynet.no/forordning

GAGN

Til tilsette, leiinga og styre:
Diskuter cyber- og informasjonssikkerhet i det daglege

GAGN

Lukke til, og takk for meg

Gry Helene Stavseng

gry@gagn.no - Tlf 91 77 85 45
Gagn Consulting AS
www.gagn.no

GAGN