

Åpne formater, men ikke åpen dør – Datasikkerhet og internasjonal datalagring

bSNK26

Selmer

Astrid Stenersen og
Kine Emilie Helgeneseth
15. april 2026

AGENDA



Hva er sikkerhetsbrudd og hvilke konsekvenser kan sikkerhetsbrudd få?



Hvordan unngå sikkerhetsbrudd? Tiltak for datasikkerhet og tilgangsstyring



Nærmere om risikoen ved internasjonal datalagring



*Hva er et sikkerhetsbrudd og
hvilke konsekvenser kan et
brudd få?*

Hva er et sikkerhetsbrudd?

Definisjonen av sikkerhetsbrudd i ISO 19650-5:

"infraction or violation of security"

Definisjonen av sikkerhet:

"state of relative freedom from threat or harm caused by deliberate, unwanted, hostile or malicious acts"

Eksempler:

Brudd på reglene om tilgangskontroll og tilgangsstyring:
Uvedkommende får tilgang til modeller

Datainnbrudd:
Uautorisert tilgang til eller eksponering av data (målet er å stjele, kopiere eller lekke)

Ransomware-angrep:
Skadevare som krypterer filer (målet er typisk utpressing)

Hvorfor er BIM-modeller interessante for uvedkommende?

- Nasjonal sikkerhetsmyndighets trusselvurdering: Utenlandske etterretningsaktører forsøker å skaffe informasjon om norsk kritisk infrastruktur
- En BIM-modell inneholder (åpenbart) svært detaljert informasjon om et bygg (ventilasjonssystemer, strømforsyning, adgangskontroll, sikkerhetssystemer, tekniske rom)
- For enkelte bygg kan dette være sikkerhetskritisk informasjon
- En BIM-modell kan også inneholde personopplysninger

Rettslig rammeverk for kravene til datasikkerhet



Utgangspunkt:

Hva har man avtalt?

- Avtalen kan ha konkrete formulerte krav til sikkerhetstiltak
- Henvisninger til standarder (ISO 19650-5, POFIN, andre relevante standarder)



Ufravikelig lovgivning

- Sikkerhetsloven
- Digitalsikkerhetsloven
- Personopplysningsloven (GDPR)
- Osv.



Fremtidig lovgivning

- Cyber Resilience Act
- Data Act
- Åpne data-direktivet
- Dataforvaltningsforordningen
- Forordningen om datasett med høy verdi

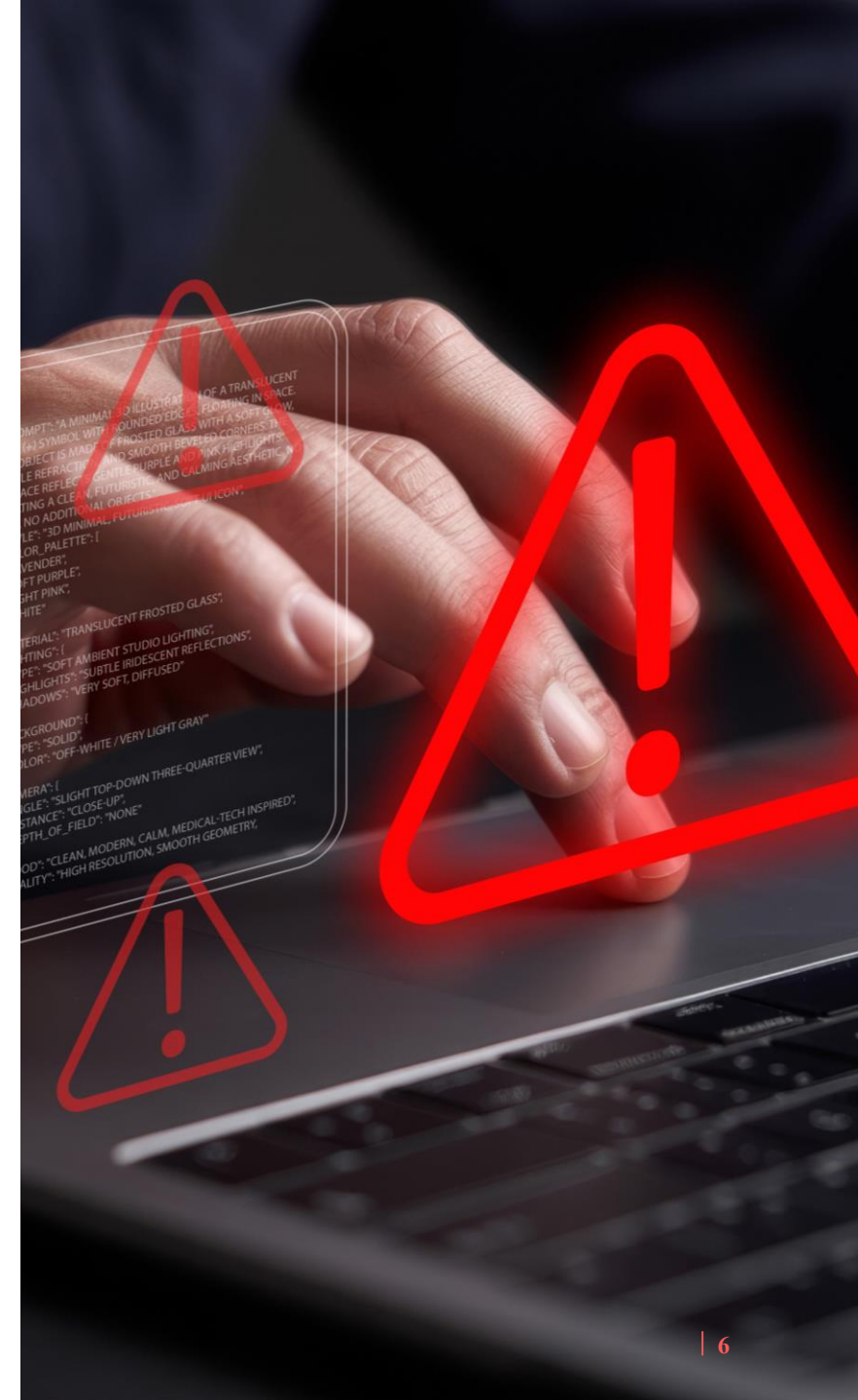
Hvilke konsekvenser kan sikkerhetsbrudd få?

- **Praktiske konsekvenser av sikkerhetsbrudd**

- Forsinkelse → økonomiske tap
- Sensitive data lekkes

- **Juridiske konsekvenser av sikkerhetsbrudd**

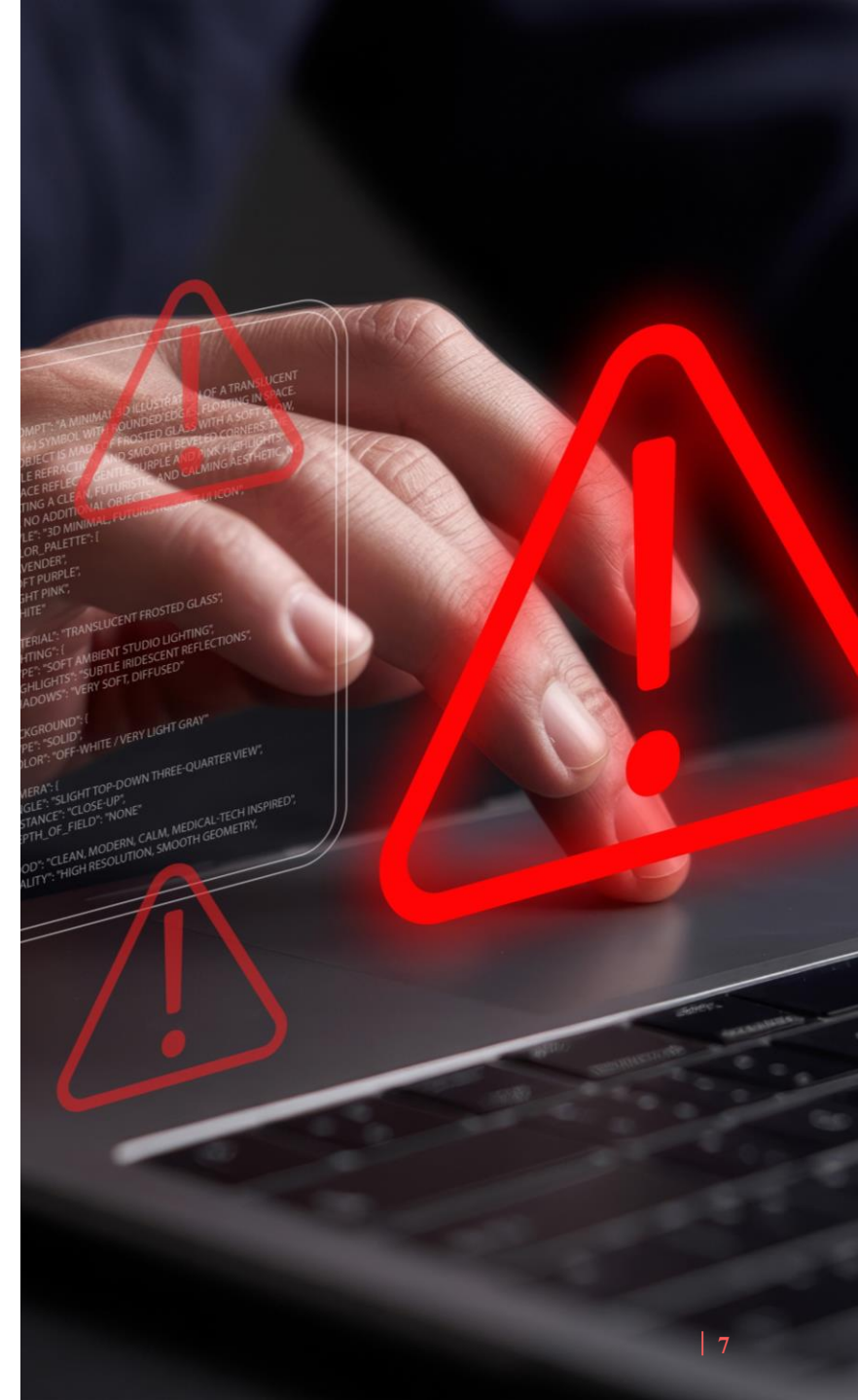
- For prosjekterende/entreprenør
 - o Ansvar som databehandler etter GDPR – kan bli ilagt bøter
 - o Dagmulkt/erstatning for forsinkelse, med mindre sikkerhetsbruddet kvalifiserer som force majeure eller skyldes oppdragsgiver
 - o Krav som følge av brudd på taushetsplikt
 - o Løsepengekrav
 - o Tap av omdømme



Hvilke konsekvenser kan sikkerhetsbrudd få?

- Juridiske konsekvenser av sikkerhetsbrudd

- For oppdragsgiver
 - Ansvar som behandlingsansvarlig etter GDPR – kan bli ilagt bøter
 - Eventuelt tap som ikke kan plasseres hos prosjekterende/entreprenør
- For skytjenesteleverandør
 - I praksis få konsekvenser – strenge ansvarsbegrensninger i lisensavtalene
 - Ansvar som databehandler etter GDPR – kan bli ilagt bøter



Hvordan unngå sikkerhetsbrudd?
Nærmere om datasikkerhet og tilgangsstyring

Generelle råd for håndtering av datasikkerhet

- Implementere tekniske, organisatoriske og kontraktsmessige tiltak

- Ivareta spesifikke krav

- Lovkrav
- Kontrakt
- Osv.

- Monitorere, revidere og evaluere



ISO 19650-5

- Fastsetter prinsipper og krav for en sikkerhetsbevisst håndtering av sensitiv informasjon som skapes, behandles eller lagres i tilknytning til prosjekter, byggevarer, produkter, tjenester eller bygg/eiendommer

- Rammeverk og verktøy for å identifisere sårbarheter og håndtere sikkerhetsrisiko effektivt og samarbeidsvennlig

- Hovedprosesser
 - **Sårbarhetsvurdering**
 - Kartlegge behovet for en sikkerhetsbevisst tilnærming, typisk via en følsomhets- eller risikovurdering
 - Hva slags informasjon håndteres? Hvilke trusler finnes? (cyberangrep, fysisk adgang, feilbruk)?
 - Hvilke konsekvenser kan feil håndtering få?
 - **Utvikle en sikkerhetsstrategi** og utarbeide en **security management plan**
 - **Igangsette** sikkerhetsstrategi med tydelig styring, roller og ansvar
 - **Samarbeide** med interne og eksterne parter for å **implementere** tiltakene i praksis
 - **Monitorere, revidere og evaluere** sikkerhetstiltakene over tid

(1) Tekniske sikkerhetstiltak

Tilgangskontroll og rollebasert tilgang

- Brukere får kun tilgang til de delene av modellen de trenger (f.eks. arkitekt får ikke tilgang til sikkerhetssystemer)
- Rolle- og rettighetsstyring (Role Based Access Control) i plattformene
- Store modeller kan deles opp i fagmodeller eller arbeidspakker, slik at ingen enkelt bruker har full innsikt

Autentisering og identitetsstyring

- Multifaktor-autentisering (MFA) for alle brukere
- Sentralisert identitetsforvaltning (f.eks. Azure AD eller SAML-integrasjon)
- Krav til sterkt passord i systemet

Kryptering

- Kryptering av data i ro (lagret) og/eller i transitt (under overføring)

Logging og overvåking

- Alle hendelser logges (hvem har åpnet, endret, eksportert, lastet ned)
- Varsling ved unormal aktivitet

Sikkerhetskopi og redundans

- Hyppige sikkerhetskopier, gjerne i separate geografiske lokasjoner
- Mulighet for rask gjenoppretting

(2) Kontraktsmessige tiltak

- **Sikkerhetskrav i kontraktene**
 - Tekniske krav
 - Responskrav
 - Krav til interne rutiner, retningslinjer osv.
- **Tydelig ansvarsfordeling**
- **Databehandleravtale som del av kontrakt der BIM inneholder personopplysninger**
- **Avtalt sanksjonssystem ved brudd**
 - Dagmulkt, heving og erstatning



(3) Organisatoriske tiltak



- **Sikkerhetspolicy og opplæring**
 - Krav til sikkerhetstiltak internt og eksternt
 - Krav til håndtering, lagring og deling av informasjon
 - Responsplan og hendelseshåndtering



- **Sikkerhetsrevisjoner**
 - Interne og eksterne



- **Avklarte roller og ansvar**

Nærmere om risiko ved internasjonal datalagring

Risiko #1

– Utenlandske myndigheters tilgang til data

- **Hvilket lands lovgivning gjelder når data lagres i tredjeland? Spørsmål om såkalt lovvalg og verneting**
 - Avtaleverket avgjør ofte lovvalg og hvor tvister skal behandles
 - Mange amerikanske plattformer (Autodesk, Trimble, Bentley) spesifiserer i sine vilkår at tvister skal avgjøres etter amerikansk lovgivning og i amerikanske domstoler
 - Norske aktører kan i prinsippet gå til sak i Norge, men domstolen vil da måtte vurdere avtalevilkårene – og ofte avvise eller si at saken må føres i USA
- **Utenlandske myndigheters tilgang til data**
 - Utenlandske selskaper med tilgang kan bli pålagt utlevering av data under eget lands rett
 - Uavhengig av lovvalg og verneting
 - U.S. CLOUD Act - gir amerikanske myndigheter rett til å kreve utlevert data fra amerikanske selskaper, uansett hvor i verden dataene fysisk ligger
- **Konsekvens for nasjonal sikkerhet**
 - Kritisk infrastruktur (sykehus, regjeringsbygg, forsvarsanlegg) – risiko da sensitive BIM-data kan avsløre svakheter, adgangssystemer, rømningsveier osv.

**NSM (Nasjonal
sikkerhetsmyndighet)**

- Kritiske data bør lagres
i løsninger underlagt
norsk eller europeisk
jurisdiksjon

!

Risiko #2

– Personvern

- **Overføring av personopplysninger til land utenfor EØS krever overføringsgrunnlag etter GDPR kapittel V**
- **Adekvansbeslutning**
 - Storbritannia
 - USA -Selvsertifiserte amerikanske selskaper
- **SCC og TIA**
 - Standardkontrakter og transfer impact assessments



Risiko #3

– Tap av tilgang og tap av data

Problem

- Sikkerhetsbrudd kan gi midlertidig manglende tilgang til data, men også tap av data
- Gjelder både prosjekteringsverktøyet/samhandlingsverktøyet, men også i CDE
- Som nevnt innledningsvis – begrenset mulighet for å videreføre ansvar til skytjenesteleverandør

Tiltak

- Versjonskontroll og back-up løsninger
- Ikke bare i CDE, men også lokalt
- Sikre plattformer og nasjonale plattformer for kritisk informasjon?

Fem praktiske råd for god datasikkerhet

1

Kartlegg data og dataflyt

2

Ha kontroll på kravene til sikkerhet

3

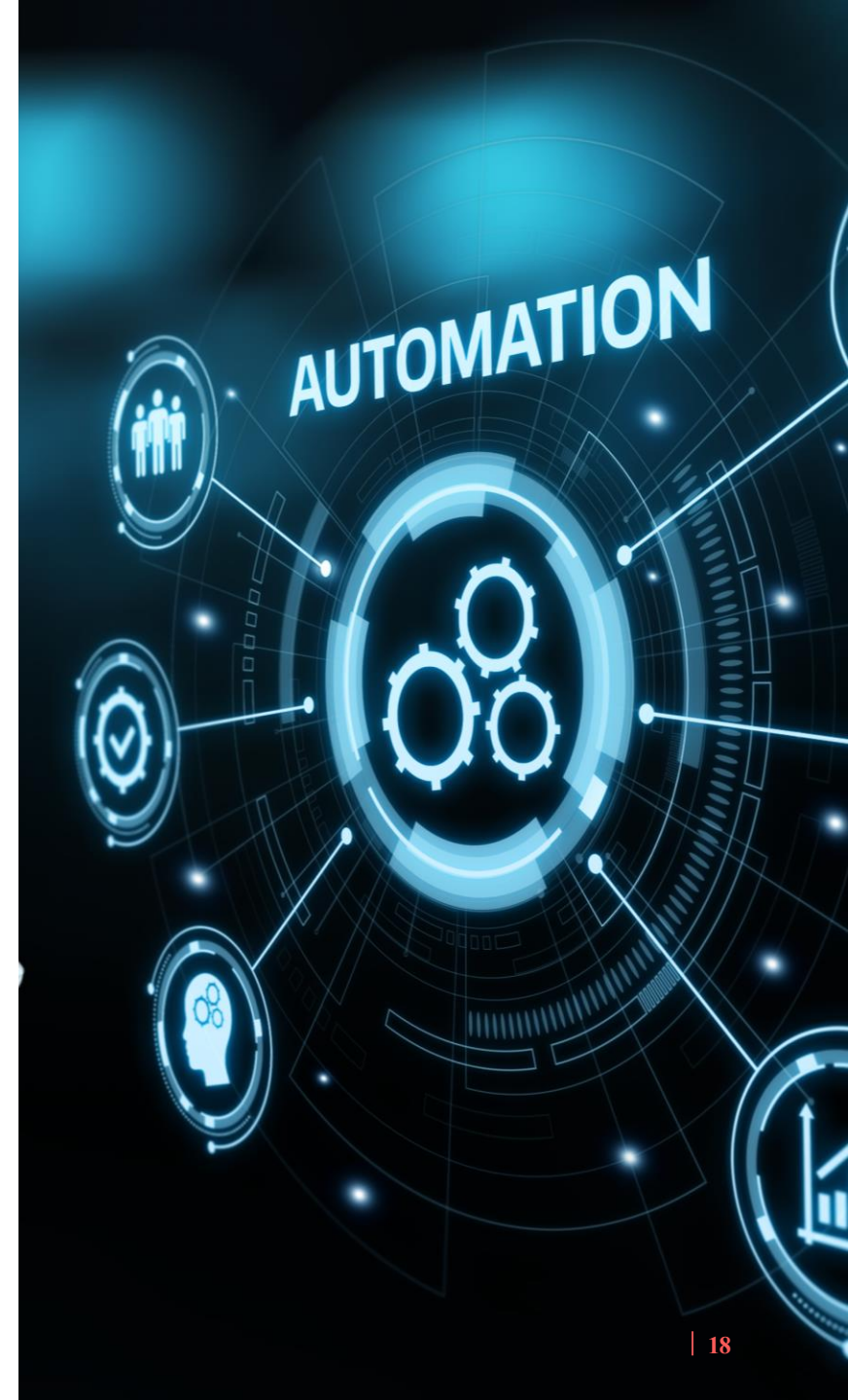
Sørg for implementering av sikkerhetstiltak

4

Sørg for backup og exit-strategi

5

Varsle umiddelbart ved mistanke om sikkerhetsbrudd



Takk for oss!



Kine Emilie Helgeneseth

Fast advokat

k.helgeneseth@selmer.no

+47 92 81 20 80



Astrid Stenersen

Partner, advokat

a.stenersen@selmer.no

+47 91 35 28 61

Selmer

selmer@selmer.no

selmer.no