



Personvernombud – Data protection officer

Rolf Jegervatn



before I take your order I am required to explain how we use that data and ask you to sign our new privacy policy



© MARK ANDERSON

WWW.ANDERTOONS.COM



"Before I write my name on the board, I'll need to know how you're planning to use that data."

GDPR TOONS

COPYRIGHT 2018 B.DREYER GDPRTOONS.COM



Privacy and GDPR have public interest

10:05:07 Rogaland TV Radio Tysdag

Datatilsynet oppretter tilsynssak etter NRK-avsløring

Røntgengiganten Unilabs lot romensk klinikk få tilgang til titusener av norske undersøkelser. Nå vil Datatilsynet finne ut om pasientopplysningene ble godt nok sikret.



Magna Dahl Müller
Rita Christian Tapdel
Lars Næss
Datatilsynet

Publisert på 11.10.2020
Oppdatert på 14.10.2020

Både Pubstiftelsen og Datatilsynet ber Unilabs forklare seg.
Foto: NTB Scanpix/NTB/NTB Ulf Hete

Sjekker Grimstads personvernspraksis etter flere klager og avvik

Etter flere avvikelser og klager fra pasienter, sjekket Datatilsynet i samarbeid med kommunen personvernspraksis i Grimstad kommune.



DATATILSYNET GRANSK

14.10.2020 NYHET

Korona-listen:

Registreringsnummer
Ettersnavn
Fødselsnummer
Prøvedato
Telefon

Info for å prioritere

Her er feilene som førte til Vigilo-skandalen

HØRING I MORGEN // Ved skolestart i 2019 tok Bergen i bruk en ny skoleapp som skulle gjøre kontakten med foreldrene tryggere.

I appen var opplysninger om alle barn i offentlige skoler og barnehager i Bergen lastet inn.

Kommunen gjorde en rekke feil, slik at foreldre som ikke skal ha tilgang til egne opplysninger fikk tilgang til alle barns opplysninger.

– Det er ingenting som styrker tilliten til byråden

22-åring erklærer straffskyld for drap



Datatilsynet håvet inn på personvernsbrudd i fjor

I år er det fem år siden personvernforordningen (GDPR) fortsatt synder både offentlige og private virksomheter. I fjor ut samlet overtredelsesgebyrer på nærmere 100 millioner kroner for brudd på personvernlovgivningen.

Gebyr til Trumf

Datatilsynet har fattet vedtak om overtredelsesgebyr på fem millioner kroner til Trumf. Bakgrunnen for gebyret er at Trumf-medlemmer kunne registrere andres kontonummer på medlemsprofilen og dermed skaffe seg tilgang til andres handlehistorikk.

Sjefen sjukom 400.000

Krever erstatning etter hendelsen i klasserommet: - Hun var helt knust

Etterforskes av politiet:

KAN HA «SNOKET» I JOURNALER I FLERE ÅR

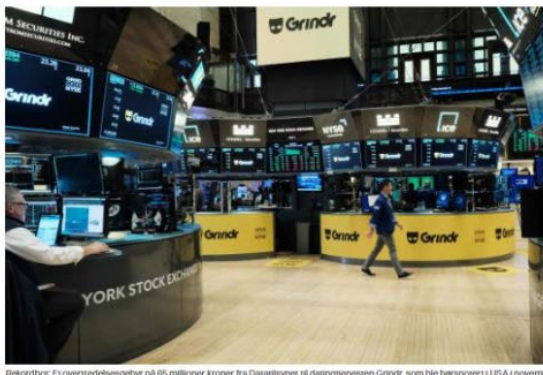
Sendte sensitiv info om eleven til foresatte for elever i hele klassen

Læreren skulle bare varsle foreldrene.

Sensitive opplysninger om Silje Johanne lå strødd: - Jeg er sjokkert!

Får smekk for IKT-sikkerheten: En hadde passordet «Sommer2022»

Digitalisering i skolen



YORK STOCK EXCHANGE

Overtredelsesgebyr til Stortinget

Høsten 2020 ble Stortinget utsatt for datainnbrudd og Datatilsynet varslet i januar et gebyr på to millioner kroner for manglende sikkerhetsnivå. Vi har vurdert Stortingets merknader og sendt vedtak der vi opprettholder det varslede gebyret.

Moss Avis

Mosseskole fellsendte e-poster om elev i lang tid: - Ikke akseptabelt

Sensitive opplysninger om brukere lå tilgjengelig for ansatte

- Et alvorlig brudd Straffes med gebyr

Tingvoll kan ikke dokumentere at alle avvik følges opp

Revisjonsrapport:

Et alvorlig avvik

22 personlige opplysninger brettet ut på storskjerm foran hele klassen

Brudd på personvern = 6,6 millioner kroner i gebyr

Kommuner har fått totalt 6,6 millioner kroner i gebyr for brudd på personvern i skoler skolen 2018. Det er viktig å erkjenne at det er et FAKTISK RISIKO for barn og unge.

Datatilsynet har vedtatt et gebyr på 65 millioner kroner til datingappen Grindr

Vår konklusjon er at Grindr har utlevert personopplysninger om brukerne til tredjeparter for adferdsbasert markedsføring uten rettslig grunnlag, sier Bjørn Erik Thon, direktør i Datatilsynet.



Datatilsynet gir Nav 5 mill. kroner i gebyr CV-delning

Datatilsynet varslet et gebyr på 5 millioner kroner fordi de mener NAV ikke hadde tilstrekkelig sikkerhet for CV-er slik at alle arbeidsgivere kunne se dem.

Ble hacket med noen ukers mellomrom - én av dem får millionbot

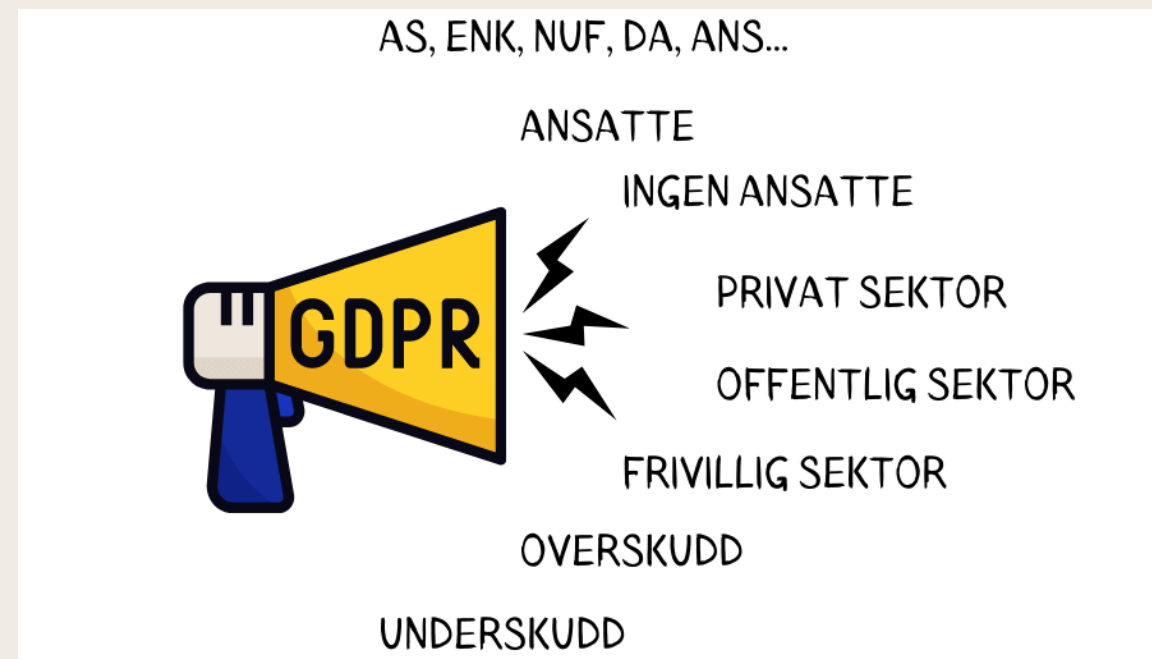
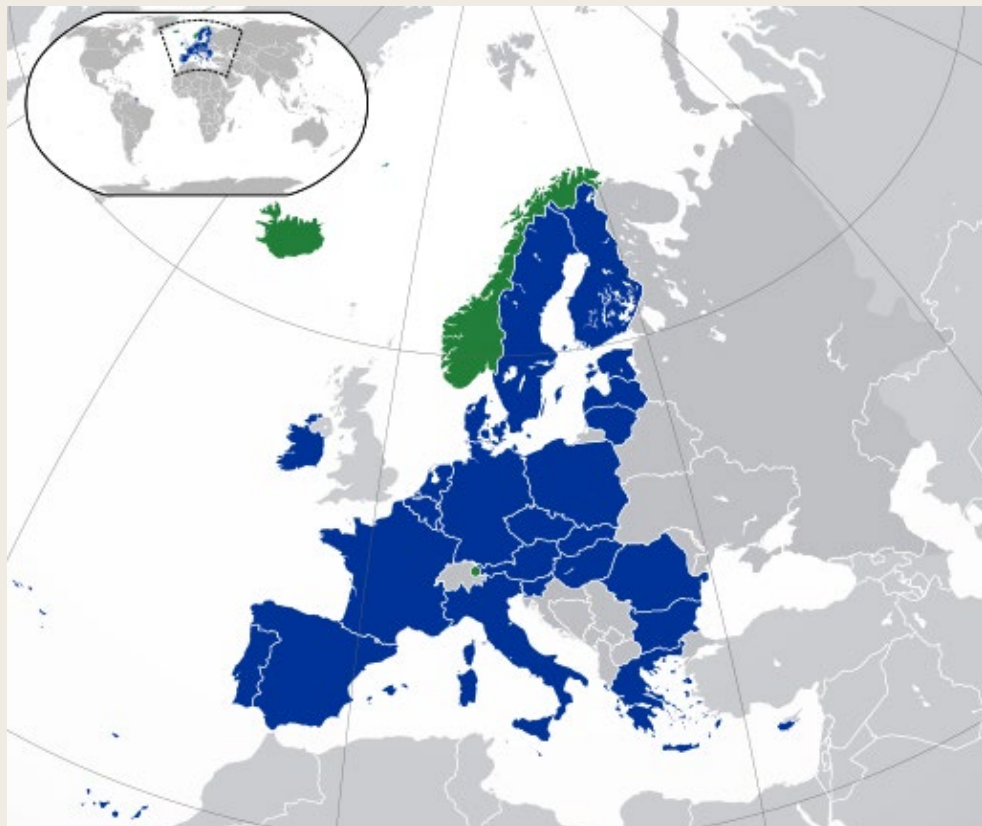
DATAANGREP NORDLAND FIKSDEKORPUSNE DATATILSYNET

Konfidensielle opplysninger om flere hundre brukere lå tilgjengelig for ansatte i kommunens «system. Avbror.

Et alvorlig avvik

22 personlige opplysninger brettet ut på storskjerm foran hele klassen

Ble hacket med noen ukers mellomrom - én av dem får millionbot



GDPR og geografisk område

For hvem gjelder GDPR?

GDPR: Types of Data under Protection

Personal Data

Sensitive Personal Data



Names



Location Data



Identification Numbers



IP Addresses



Cookie Data



RFID Tags



Health Data



General Data



Biometric Data



Racial or Ethnic Data



Political Opinions



Sexual Orientation

Pseudonymization vs Anonymization: Key



Personal data

Name: Jane Doe
 Birth: 13.07.1975
 Email: j865@mail.com
 Medical data: migraine

Pseudonymous data

Name: 764566
 Birth: x1.j4.874f
 Email: ████████████████████
 Medical data: migraine

7 Principles of data protection law

Protecting personal data:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

The requirements in the GDPR framework are based on the 7 principles – the core of GDPR.

- The key principles related to the processing of personal data are further described in GDPR Art. 5



Legal basis for processing personal data

- Article 6 - GDPR defines the six lawful bases that data controllers can leverage for the processing of personal data.
- Legal basis 1: Informed consent (Art. 6(1)(a) – often used in research

What is Needed to Process Data?

- A “lawful basis” for doing so
- A “lawful basis” can be:
 - When required for a contract
 - When required for public interest
 - When required to comply with a law
 - When required to protect an individual’s life
 - When required for the legitimate interests of a third party (*no sensitive data*)
 - When freely given consent for a specific purpose has been provided
- If sensitive data is being processed, explicit consent for those data elements is required.



What is Needed for Legally Effective Consent?

- Must be in clear and plain language, intelligible, and easily accessible
- Must be specific about the purpose of the data processing
- Must be distinguishable from other matters
- Must be given by a clear act or statement
- Must be an unambiguous indication
- Must fully inform the data subject
- Must be freely given



What is Data Processing?

- Processing of data involves any and all of the following:

- Adapting
- Altering
- Collecting
- Combining
- Consulting
- Destroying
- Disclosing



- Erasing
- Organizing
- Recording
- Retrieving
- Storing
- Structuring
- Using

Recommendations from DPO

- Define the purpose of collecting and using personal data and know what the legal basis for processing is.
- Process personal data only with a legal basis
- Be transparent about how you process your data
- Act in line with the rights of data subjects – Respondents, rights?
- Classification of what you are processing, and knowledge of storage tools, is important before collecting data.
- Good planning and familiarity with guides/intranet resources facilitate secure data management.
- Ensure protection of your data, wherever stored, minimise where you can and share under the right conditions
- Nettskjema is the primary data collection tool for surveys and audio recordings, up to sensitive data (red category).
- Remember to delete personal data after the intended purpose is fulfilled.
- Report deviations!
- Thank you for your attention!



Useful Sources

- [UiS intranet](#)
- [Datatilsynet](#)
- [SIKT](#)

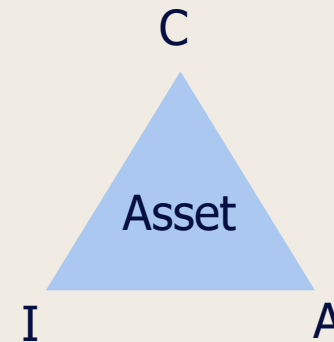


Information security at UiS

Christian Sommer
Senior Advisor Information Security,
Section for Information Management

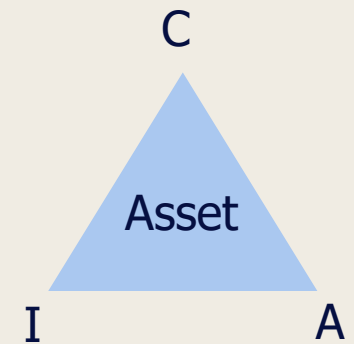
Information Security

- Protecting information and information systems (assets) through out the assets lifetime.
- We use three key principles:
 - *Confidentiality*
 - *Integrity*
 - *Availability*



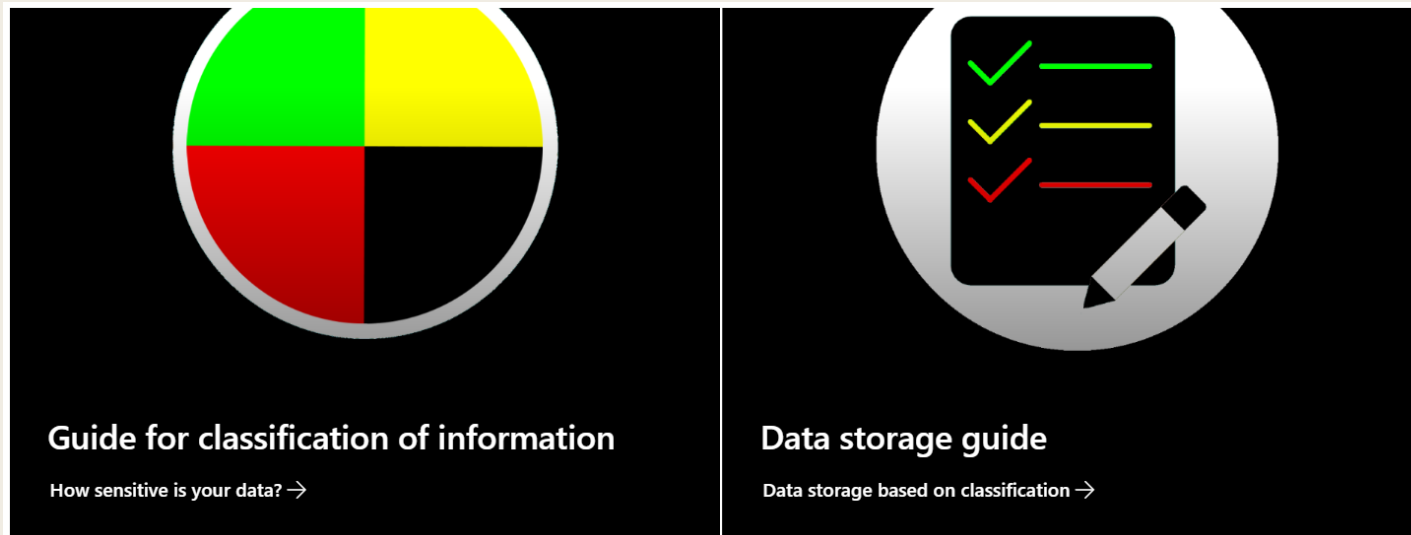
What is an information asset?

- Your research project
 - Publications / Library books
 - Insight private company
 - Register data (SSB)
 - Questionnaires
 - Interview / recordings
 - Identifier key



Classification- and storage guide

- [Classification guide](#) – what data are you handling?
- [Storage guide](#) – find appropriate tools for collecting, processing and storing.



Classification

- Open (**Green**) – Websites, publications.
- Internal (**Yellow**) – Non-published material, personal data (name, phone number, e-mail)
- Confidential (**Red**) – Special categories of personal data (race, religion, health data etc.)
- Strictly confidential (**Black**) - Data with high commercial value, data with high impact on individual or group.

Åpen
(Grønn)

Intern
(Gul)










Fortrolig
(Rød)

Strengt fortrolig
(Svart)

- Your research project

- Publications
- Insight private company
- Register data (SSB)
- Questionnaires
- Interview / recordings
- Identifier key

Åpen (Grønn)	Intern (Gul)	Fortrolig (Rød)	Strengt fortrolig (Svart)
-----------------	-----------------	--------------------	------------------------------

System	Godkjent for	Krav til lagring av fortrolig data
UiS-driftet maskin	  	Røde data kan lagres på maskin med fullkryptert disk. Røde data skal ikke flyttes til lagringsområder som ikke er godkjent for det.
UiS OneDrive	  	<p>Lagring av røde data i OneDrive krever at dokumenter og filer settes til følsomhet <i>fortrolig</i>. Se veiledning for lagring av røde data i Teams og OneDrive.</p> <p>Bruk OneDrive til filer som ikke krever samhandling. For samhandling, bruk Teams.</p> <p>OneDrive kan brukes for deling med eksterne. Dette gjelder også hvis følsomhet <i>fortrolig</i> er satt på dokumentet, men da må noen enkle steg følges av den eksterne.</p>
UiS Teams	  	<p>Røde data i Teams krever at teamet er satt som fortrolig. I tillegg må alle filer som inneholder rød data være merket med følsomhet <i>fortrolig</i>. Se veiledning for lagring av røde data i Teams og OneDrive.</p> <p>Bruk Teams når du skal samarbeide og dele filer med andre. For dokumenter og filer som er tiltenkt deg selv, bruk OneDrive.</p>

Data collection: Audio & Questionnaire

(red):



Nettskjema

+ Nettskjema diktaphon-app

Recommended tools

Processing (yellow/red):

(With UiS account)



Storage (yellow/red):



OneDrive

(With UiS account)

Intra.uis.no

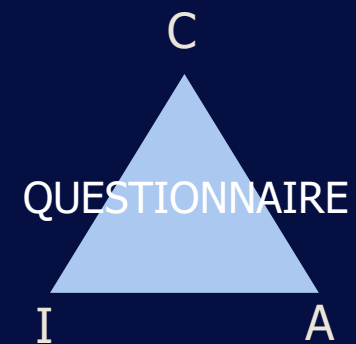
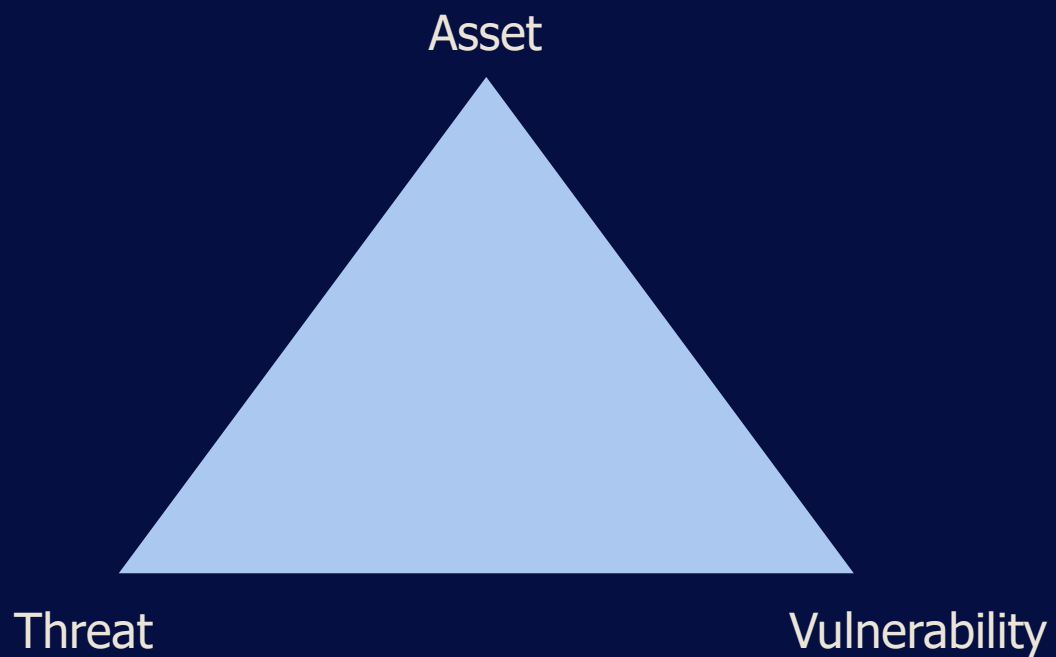
Look up «Informasjonssikkerhet og
personvern»

CONSENT / INFORMATION LETTER

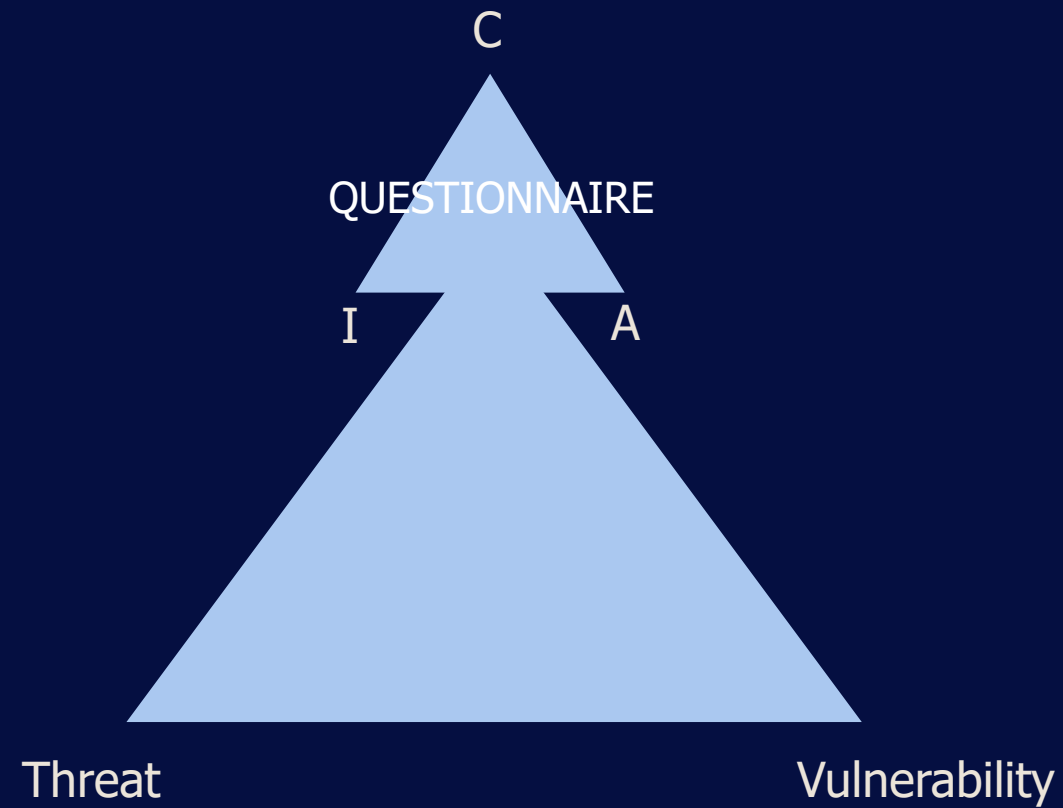
QUESTIONNAIRE

AUDIO RECORDING

Information Security & Risk



Information Security & Risk



Report deviations

- Deviations in data handling
 - Information security
 - Privacy
- Report to
 - it-hjelp@uis.no
 - personvernombud@uis.no



Takk for meg!