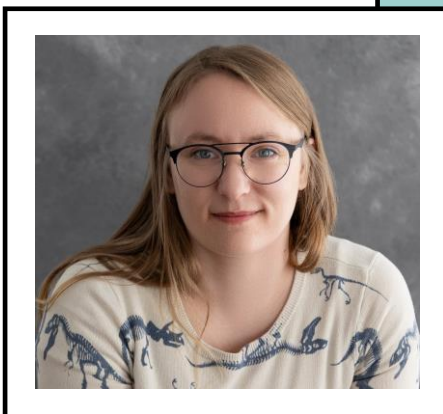




EDPS' BESLUTNING OM FORBUD MOT EU- KOMMISJONENS BRUK AV M365

Ida Thorsrud

OM MEG

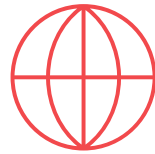


Ida Thorsrud er en **jurist** og har en master i rettsvitenskap fra Universitetet i Oslo. De siste 10 årene har hun arbeidet med **personvern** og informasjonssikkerhet både i offentlig og i privat sektor. Hun omtaler seg selv som en personvern-**nørd**, og du kjenner henne kanskje fra **LinkedIn** hvor hun regelmessig skriver om personvern. Akkurat nå er hun prosjektleder for **en nasjonal DPIA for bruk av Google Workspace for Education** i skolen i regi av KS og Bergen kommune.

KONSTATERTE BRUDD



Formålsbegrensning



Overføringer til
tredjeland



Konfidensialitetsbrudd

FORMÅLSBEGRENSNING

Mangler oversikt over hvilke **personopplysninger** som behandles og til hvilket **formål**

EUs GDPR art. 4(1) b)

Ikke tydelig instruert MS om hvilke personopplysninger som skal behandles

EUs GDPR art. 29(3) a)

Kommisjonen har ikke sikret at MS bare behandler pii i tråd med **dokumentert instruks**

EUs GDPR art. 4(2), 29(1), 30

Har ikke vurdert om MS **viderebehandler** pii på en måte som ikke er i tråd med opprinnelig formål

EUs GDPR art. 6

Har ikke vurdert om **overføring** til MS Irland og underdatabehandlere er **nødvendig** og **proporsjonalt**

EUs GDPR art. 9

OVERFØRINGER TIL TREDJELAND

Mangler oversikt over hvilke personopplysninger som overføres og hvilke land de overføres til

EUs GDPR art. 29(3) a)

Har ikke vurdert eller implementer supplerende tiltak for overføringen

EUs GDPR art. 4(2), 46, 48

SCC uten oversikt over pii
Mangler godkjenning fra EDPS for annet overføringsgrunnlag

EUs GDPR art. 4(2), 46, 48(1) og (3) a)

Har ikke sikret at overføringer bare skjer "to allow tasks within the competence of the controller to be carried out"

EUs GDPR art. 47, jf. 4, 5, 6, 9 og 46

KONFIDENSIALITETSBRUDD

Har ikke sikret at det bare er EU-lovgivningen som kan forhindre MS fra å varsle om utleveringer
Har ikke sikret at inngrep i varslingsplikten er "nødvendig" og "proportional"

EUs GDPR art. 29(3) a)

Har ikke gjort tredjelandsvurderinger for å sikre at uovlige tleveringer ikke skjer
Har ikke iverksatt supplerende tiltak

EUs GDPR art. 4(1) f), 33(1), 36

HVA ER DE TINGENE SOM BARE MÅ VÆRE PÅ PLOSS

Hva kan DU ta med de deg fra denne beslutningen?

Roller og ansvar MÅ være klinkende klart!

Faktiske forhold skal legges til grunn

Når databehandleren din har en egeninteresse av behandlingen, taler det for at DE er behandlingsansvarlig

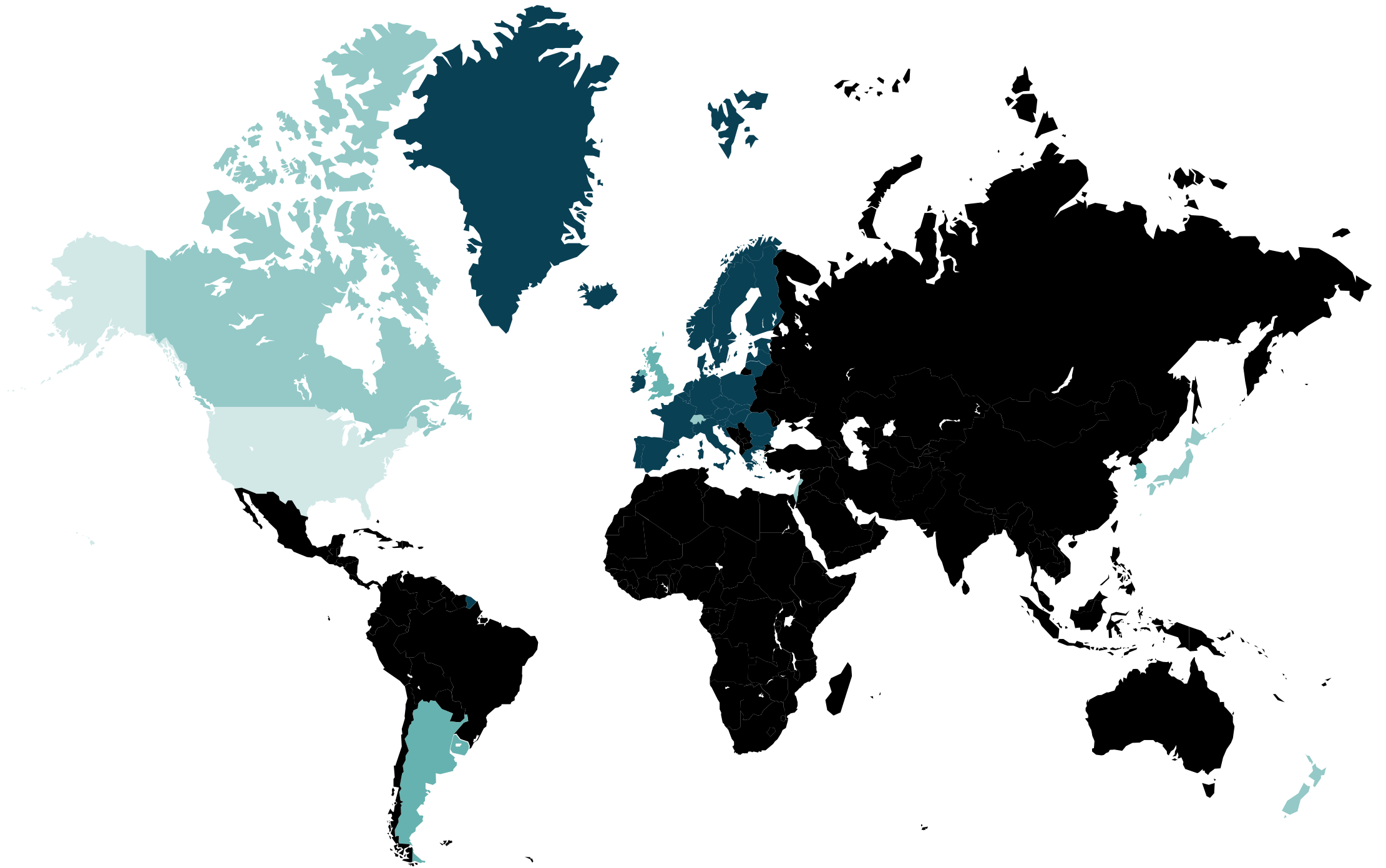
Pseudonymiserte opplysninger er pii

Terskelen for når noe er en personopplysning er LAV.

Du må ha oversikt over alle kategorier av pii som behandles til de forskjellige formålene.

Viderebehandling til kompatible formål

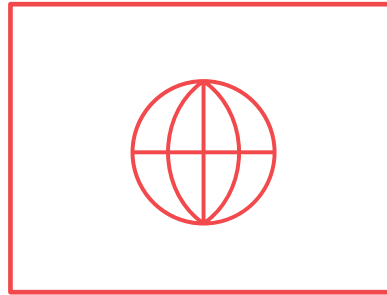
Tydeliggjøring av forpliktelsen du som behandlingsansvarlig har til å sørge for at databehandleren din ikke viderebehandler pii til andre formål enn de du først samlet dem inn for.



ANDRE POENGER



Det er så mye enklere for DT å vurdere DIN etterlevelse enn MS sin



MS innrømmer ikke at de er behandlingsansvarlig for noen ting



EU-kommisjonen har i stor grad ikke gjort vurderinger eller mangler dokumentasjon

TUSEN TAKK!

Hvis du liker hvordan jeg snakker om personvern?



Abonner på nyhetsbrevet mitt!

