Hva betyr Personvernforordningen for næringslivet?

Erfaringsutveksling og praktiske eksempler

Advokat Cecilie Rønnevik - Simonsen Vogt Wiig

Anette Hansen og Niall Merrigan – Capgemini Norge

NOKIOS, 23.oktober 2018

Capgemini

simonsen vogtwiig

Dagens agenda

01 GDPR frem til i dag - Cecilie Rønnevik

02 To rådgivere møtes hos kunde – Anette Hansen og Cecilie Rønnevik

03 GDPR and the ease of hacking – Niall Merrigan

Anette Hansen (Capgemini)

- Senior Consultant @ Capgemini
- Community of Practice Lead: Information Privacy
- Compliance-rådgiver: AML, KYC, FATCA og GDPR

Anette.a.hansen@capgemini.com

https://www.capgemini.com/no

Cecilie Rønnevik (SVW)

Datatilsynet – 12 år

Juridisk fagdirektør med overordnet ansvar for juridisk kvalitetssikring

Advokatfullmektig/advokat siden 2015

Medforfatter

"Personvernforordningen – kommentarutgave"

Universitetsforlaget (2018)

"Personopplysningsloven og personvernforordningen – kommentarutgave"

Universitetsforlaget 2019

Kurs- og foredragsholder

Juristenes Utdanningssenter, Advokatforeningen, RegnskapNorge, mfl.

Niall Merrigan (Capgemini)

- Head of CyberSecurity Norway @ Capgemini
- Microsoft Most Valuable Professional
- ASPInsider
- Microsoft Azure Advisor

@nmerrigan

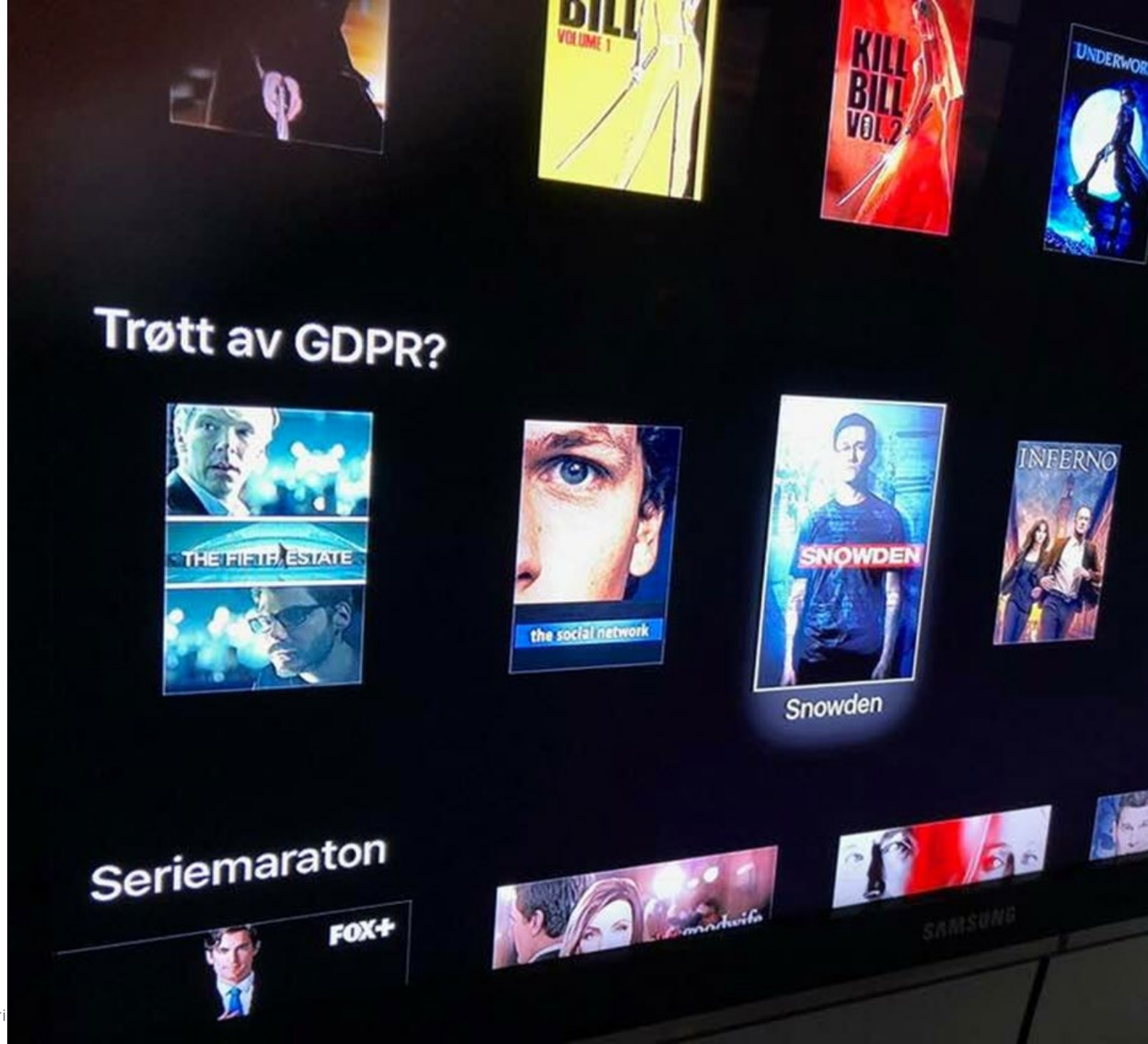
niall.merrigan@capgemini.com

https://www.capgemini.com/no

https://www.certsandprogs.com

"Jeg er ikke alene!"

Viaplay til meg, 2. juni 2018



Hvorfor er vi trøtte av GDPR?

- Januar 2012
  - EU kommisjonens forslag til ny forordning
- Januar 2012 – April 2016
  - Forhandlinger Rådet og Parlamentet
- April 2016
  - GDPR vedtas
- Mai 2018
  - GDPR får virkning i EU
- Juli 2018
  - GDPR "gjelder som lov" i EØS (Norge)

Hvorfor er vi trøtte av GDPR?

- "Alle" snakker om GDPR

- GDPR gjelder overalt – angår alle
  - Som registrerte
  - Som ansatt/konsulent/rådgiver hos pliktsubjektene

- GDPR er gjort til en "hype"
  - Massiv markedsføring på sosiale medier: kurs, it-systemer, rådgivning, litteratur mm

- GDPR har utløst en "tsunami" av pop-ups og eposter til oss forbrukere
  - Nye brukervilkår og personvernerklæringer

Hvorfor er vi trøtte av GDPR?

- GDPR blir, ofte ufortjent, "syndebukken" for upopulære beslutninger
  - "På grunn av GDPR kan vi ikke lengre motta helseopplysninger på epost...«
  - "GDPR krever at vi henter inn samtykke fra deg...«
  - "På grunn av GDPR må vi ha et prosjekt...."

Hvorfor er vi trøtte av GDPR?

- GDPR er et evighetsprosjekt (faktisk!)
  - Sett delmål og delprosjekter
  - Unngå set-back: tenk forvaltning og kontroll i etablerings og implementeringsfasen
  - Ikke iverksett tiltak som ikke fungerer i praksis, eller som ikke lar seg kontrollere
- GDPR er vanskelig…!

Hvorfor er GDPR så vanskelig?

- Mye overlates til de ansvarlige

- Svært skjønnsmessige bestemmelser, få klare regler:
  - Hva er "nødvendig"?
  - Hva er en "berettiget interesse", og hvor mye veier den?
  - Hva er et "egnet" sikkerhetsnivå?
  - Hva er "egnede" tekniske og organisatoriske tiltak?
  - Er det "sannsynlig at bruddet på personopplysningssikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter"?

- Konsesjonsinstituttet er bortfalt (forhåndskontroll)

Hvorfor er GDPR så vanskelig?

- Få rettskilder (foreløpig)
  - Forordningen med fortalen
  - Veiledere fra WP29/EDPB (teori)
  - Lite relevant forvaltningspraksis
  - Ingen relevante dommer fra nasjonale domstoler
  - Få relevante dommer fra EU-domstolen
  - Teori

Hvorfor er GDPR så vanskelig?

- Gjennomføres/presiseres i mange nasjonale lover – uoversiktlig
  - Personopplysningsloven 2018
  - Diverse særlovgivning på ulike livsområder:
  - Arbeidsmiljøloven med forskrifter
  - Pasientjournalloven og helseregisterloven

- Krever kompetanse
  - Jus, teknologi og revisjon
  - Kompetanse om den aktuelle behandlingen
  - Kommunikasjon
  - Prosjektledelse
  - Virksomhetsarkitekter

Hvorfor lykkes vi *ikke* med GDPR?

- Vi begynte for sent
  - Til tross for en implementeringsperiode på nesten 2,5 år er det fremdeles noen som "sitter på gjerdet"

- Vi engasjerer oss ikke
  - Man "setter ut" jobben med å etablere og implementere GDPR
  - Manglende forankring hos de ansatte
  - Manglende tilpasning til virksomhetens art, størrelse og organiserng
  - Mangelfull forvaltning og kontroll når de eksterne "er ute"

- Vi er "låst i det etablerte"
  - Man har problemer med å tenke nytt mht. organisering og arbeidsprosesser
  - "Vi jobber med å kryptere epostene våre, i stedet for å utrede alternative kommunikasjonsformer"
  - "Vi kan jo ikke legge ned call-senteret vårt!"

Hvorfor lykkes vi *ikke* med GDPR?

- Vi mangler vilje eller evne til å bruke ressurser
  - GDPR koster, på samme måte som andre forpliktelser koster
  - Har man ikke "råd" til å oppfylle kravene, så må man finne på noe annet å gjøre

- Vi prioriterer feil
  - Kartleggingsverktøy og crawlere er bare hjelpemidler

- Vi begynner "i feil ende"
  - Enkeltproblemer tar opp all tiden i arbeidet, og man kommer ikke i mål
    - "Når må jeg slette notater fra jobbintervjuer?"
    - "Vi lager en ny personvernerklæring"

Hvorfor er GDPR så viktig?

- Overtredelsesgebyr og andre sanksjoner fra Datatilsynet – behandlingsansvarlig og databehandler
  - Lav sannsynlighet – tilsynet er relativt lite og har stor arbeidsbelastning
    - Med mindre det kommer en klage eller lignende som gjør at tilsynet fatter interesse
  - Stor konsekvens – gebyrer inntil 20 mill. euro/4% av global årsomsetning

- Erstatningskrav fra de registrerte – behandlingsansvarlig og databehandler
  - Lav, men økende sannsynlighet – svært får saker etter gammel lov,
    - større bevissthet nå
    - forordningen legger til rette for gruppesøksmål
  - Konsekvensene foreløpig uklare – økonomisk tap og oppreisning
    - Rettspraksis etter gammel lov
      - Oppreisning: inntil kr 50.000
      - Økonomisk tap: ingen dommer

Hvorfor er GDPR så viktig?

Erstatningskrav fra kunde – aktuelt for databehandler (inkl. underdatabehandler)

- Regress: kunden er ilagt overtredelsesgebyr eller erstatningsplikt
- Avtalebrudd: for eksempel manglende sletting, uautoriserte utleveringer, osv.
  - Svært sannsynlig med de kontrollpliktene som pålegges den behandlingsansvarlige
- Konsekvensen foreløpig uklar
  - Ansvarsbegrensningsklausuler

Konkurransedyktighet – aktuelt for databehandler

- Behandlingsansvarlige forutsettes å kreve fremlagt dokumentasjon på at databehandlere gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning og vern av den registrertes rettigheter (art. 28 nr. 1)
- Databehandlere som ikke kan dokumentere skal heller ikke engasjeres
- Svært sannsynlig

Hvorfor er GDPR så viktig?

Konkurransedyktighet – relevant for andre leverandører enn databehandlere

- Noen kunder har etiske retningslinjer eller forpliktelser som tilsier at de kun benytter leverandører som opptrer lovlig (herunder i samsvar med GDPR)
- Leverandører som ikke kan dokumentere etterlevelse kan risikere å bli avvist, selv om kunden ikke får noe direkte ansvar
- Sannsynlig

Hvorfor er GDPR så viktig?

- GDPR styrker europeiske virksomheters stilling i det digitale verdensmarkedet
  - Kravene skaper tillit mellom tilbyder og kunde, en konkurransefordel
  - Kravene er så strenge at tilbydere i tredjeland ofte ikke vil kunne oppfylle disse

- Personvern er en menneskerett
- "Alt er mulig" med dagens teknologiske utvikling
  - Lovgiver må sette grensene for hva teknologien skal brukes til
- Personvern (EMK art. 8)
  - Positiv og negativ plikt for staten
- Hvorfor er personopplysningsvern så viktig?
  - Individuell rettighet, men også en nødvendig garanti for det frie demokratiet
  - Kunnskap er makt:
    - Cambridge Analytica (Trump og Brexit)
    - Kinas overvåkning og rangering av "gode borgere"

DEL 2: En advokat og en IT konsulent

Cecilie Rønnevik og Anette Hansen

En advokat og en IT konsulents erfaringer hos en kunde innen Finans og Forsikring

Et praktisk eksempel: endring av salgsportal på web

To ulike interesser – IT implementering og lovteksten (GDPR)

Oppgave: å skulle endre salgsportalen hos en kunde innen Finans & Forsikring

Hva skulle vi levere?

Mål: å ha en salgsportal i henhold til GDPR

Utfordring: forretning hadde begrenset kunnskap innen GDPR

Hva gjorde vi?

- IT løsningsforslag sendt til juridisk (Cecilie) for vurdering
- Tilbakemeldinger
- Justering av løsningsforslag
- «Final OK»
- Løsningsforslag sendt til utviklere

Hvordan løste vi det – suksesskriterier for å lykkes

- Klar dialog med forventninger
- Juridisk har ikke teknisk/forretningskunnskap innen forsikring – se an mottakeren
- Visuelle fremstillinger – kan hjelpe mye
- Løse det tekniske i etterkant – når ting er avklart

Utfordringer vi møtte på

- Hva sier lovteksten mot mandatet i prosjektet?
- Tidsfrist – 25.mai
- Tverrfaglige rådgivere med «egne» interesser
- Ingen har tidligere erfaringer med GDPR
- Ingen klar fasit eller rammeverk
- Kommunikasjon på tvers av fag, kompetanse og land

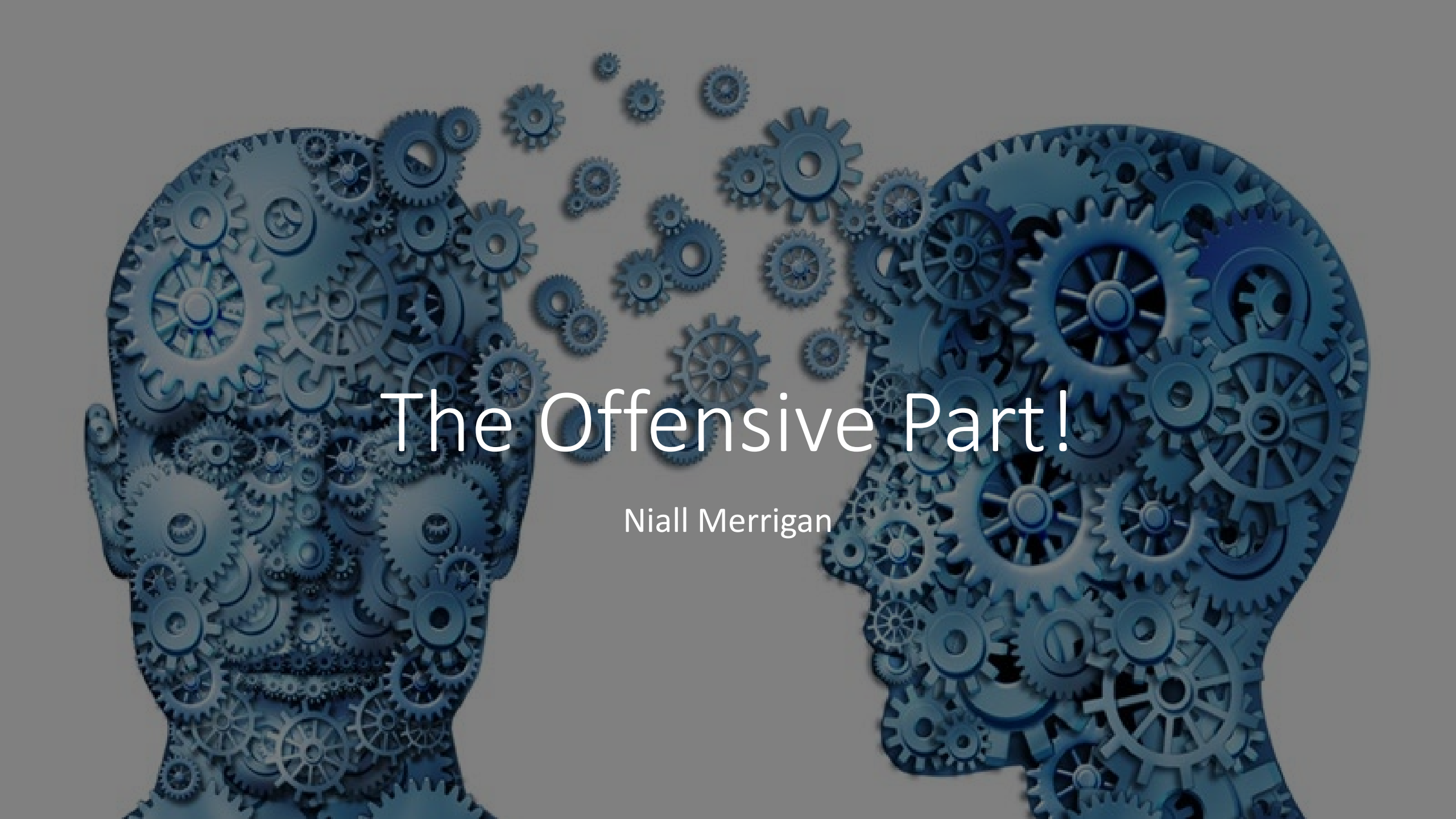
Anbefalinger og erfaringer

Tverrfaglig samarbeid

Diskusjon – hvordan har *dere* løst GDPR?

DEL 3: Niall Merrigan

Cyber Security and the ease of hacking



The Offensive Part!

Niall Merrigan

GhostProject

The total amount of credentials (usernames/clear text password pairs) is 1,400,553,869..

Click here to follow us on Twitter! @GhostProjectME

Search by full email address or username. Example: user@test.com, usertest..

Search term

Search Email

Search

Follow @GhostProjectME

simonsen vogtwiig

Search for a database..

Name	Last Modified	Collection	Bytes	Download
Myspace.com.txt.7z (12.22 GB)	22/05/2017	Large DBs	13117982617	DOWNLOAD
Exploit.in.7z (8.46 GB)	22/03/2018	Large DBs	9079378731	DOWNLOAD
edmodo.7z (5.21 GB)	06/03/2018	Large DBs	5595572787	DOWNLOAD
linkedin_all.7z (4.22 GB)	22/05/2017	Large DBs	4535170532	DOWNLOAD
patreondump.tar.gz (3.72 GB)	22/05/2017	Large DBs	3997819699	DOWNLOAD
modbsolutions.rar (2.61 GB)	22/05/2017	Large DBs	2799583102	DOWNLOAD
fling.com_40M_users.sql.7z (2.42 GB)	10/04/2018	Large DBs	2594113915	DOWNLOAD
lastfm-thesle3p.rar (2.01 GB)	22/05/2017	Large DBs	2162247227	DOWNLOAD

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address

pwned?

Generate secure, unique passwords for every account

Learn more at 1Password.com

Why 1Password?

314	5,555,329,164	80,702	87,977,243
pwned websites	pwned accounts	pastes	paste accounts