Personvernbrudd og risikovurdering

Fagseminar – Finans Norge

2. september 2020

Advokat Kristin Haram Førde

BULL&CO

ADVOKATFIRMA

Grunnleggende krav i GDPR

- Art 32: «Organisatoriske tiltak» - organisatorisk sikkerhet
  - ❑ Måten virksomheten er organisert – personer og rutiner – registrertes rettigheter
  - ❑ Instrukser i hvordan oppgaver skal løses for å sikre vedvarende fortrolighet (konfidensialitet), integritet, tilgjengelighet og robusthet
  - ❑ Bygge sikkerhetskultur

Personvernbrudd – krav til virksomhetene

- Identifisere hendelsen
- Analysere risikoen
- Varsle
- Åpenhet

- Prinsippet om ansvarlighet i Art 5: dokumentasjon

- Artikkel 33 og 34: hvordan reagere når et personvernbrudd inntreffer

- Forberedelser og rutiner
- Forebyggende tiltak

Hva er et personvernbrudd?

- Art 4 (12) Brudd på sikkerheten som fører til:
  - Utilsiktet eller ulovlig tilintetgjøring av
  - Tap av
  - Endring av
  - Ulovlig spredning av
  - Ulovlig tilgang til

personopplysninger (som er behandlet)

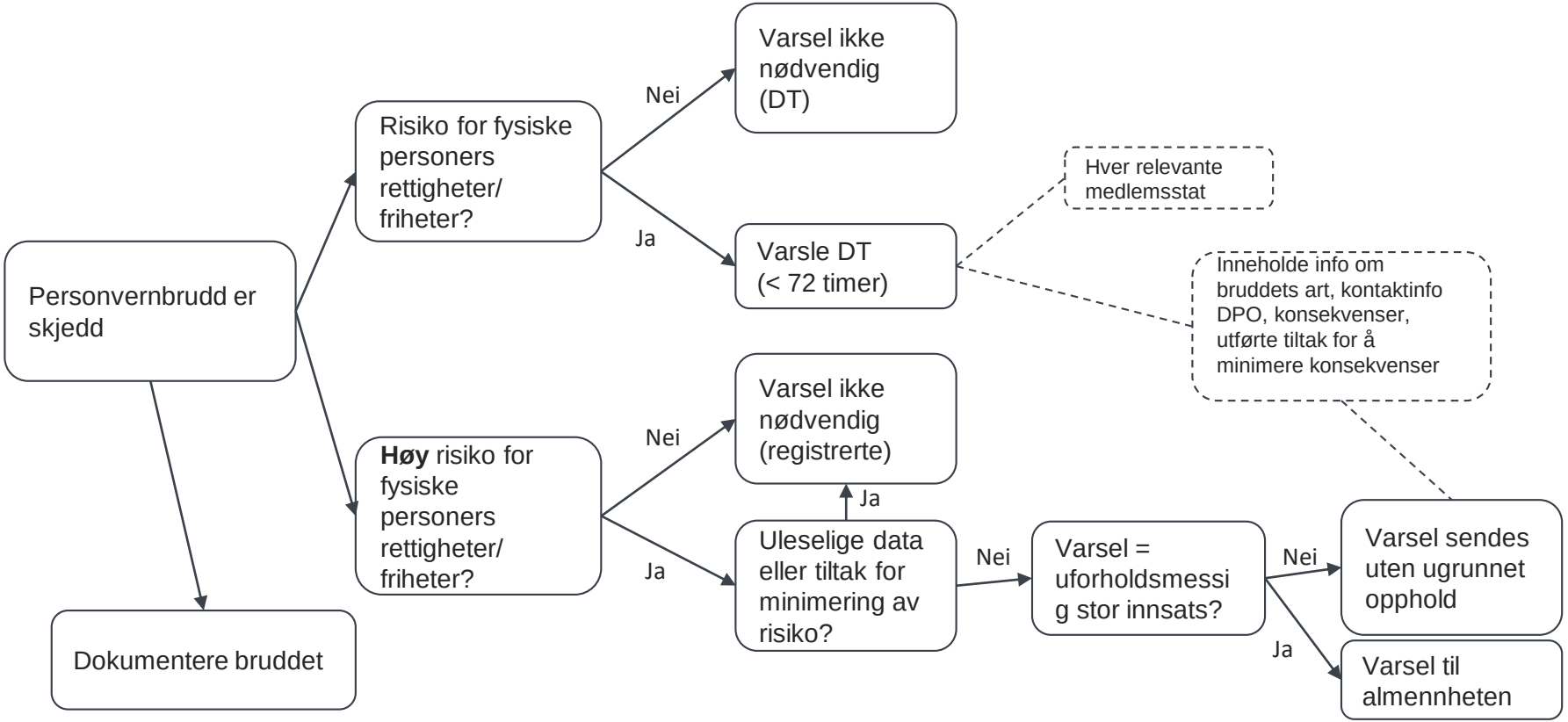
- …som betyr:
  - Brudd på konfidensialitet
  - Brudd på integritet
  - Brudd på tilgjengelighet

Hva skal meldes og når?

- Uten ugrunnet opphold etter å ha fått kjennskap til bruddet
- Innen 72 timer til Datatilsynet
- Uten ugrunnet opphold – dersom høy risiko for fysiske personers rettigheter og friheter – de registrerte
- Unntak: dersom bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter

Personvernbrudd GDPR – når varsle?

GDPR art. 33 & 34



DPIA vs risikovurdering ved brudd

- Forskjellig fokus når bruddet faktisk har skjedd
- DPIA:
  - Risiko ved behandlingen av personopplysningene, og
  - Risiko ved et eventuelt brudd - hypotetisk sett
- Når bruddet har inntruffet:
  - Har allerede inntruffet, og
  - Kun fokus på konsekvensene og faktisk innvirkning på de registrerte

Risikovurdering ved brudd

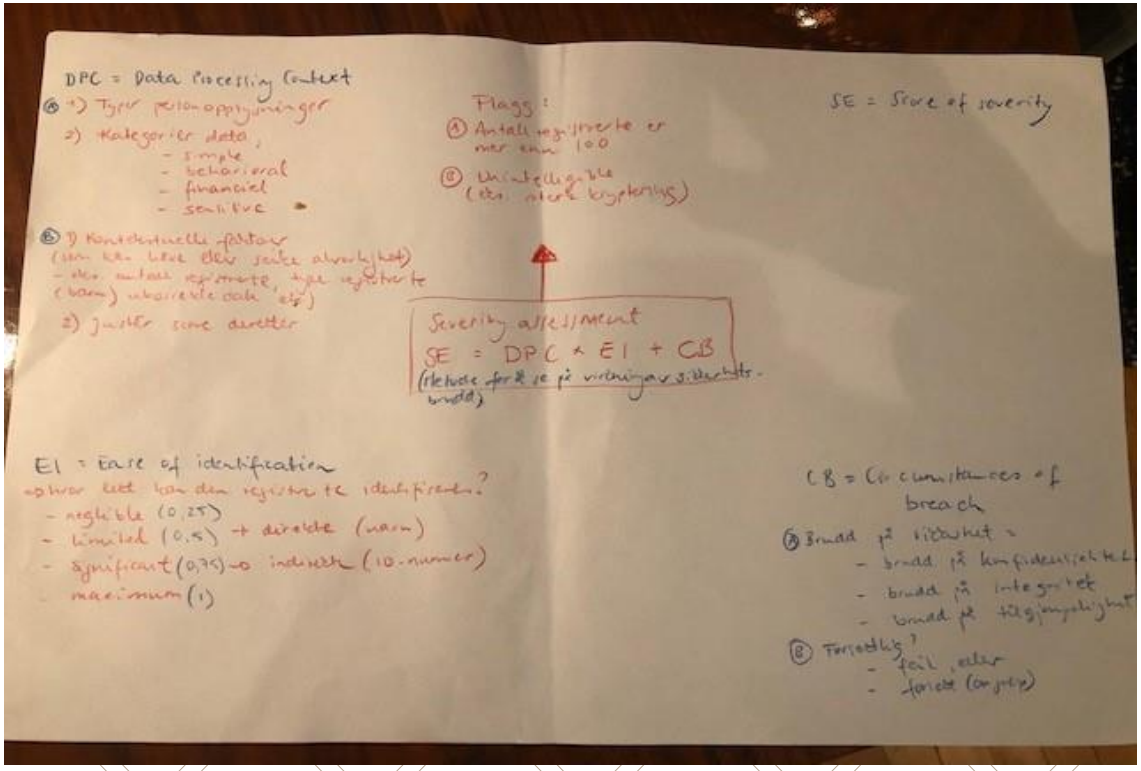
- Involverer bruddet personopplysninger?
- Er det en *sannsynlighet* for at bruddet har konsekvenser for personers rettigheter og friheter?
- Er det en *høy sannsynlighet* for at bruddet har konsekvenser for personers rettigheter og friheter?

- ICO: “This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached”
- ICO: “A ‘high risk’ means the threshold for informing individuals is higher than for notifying the ICO.”

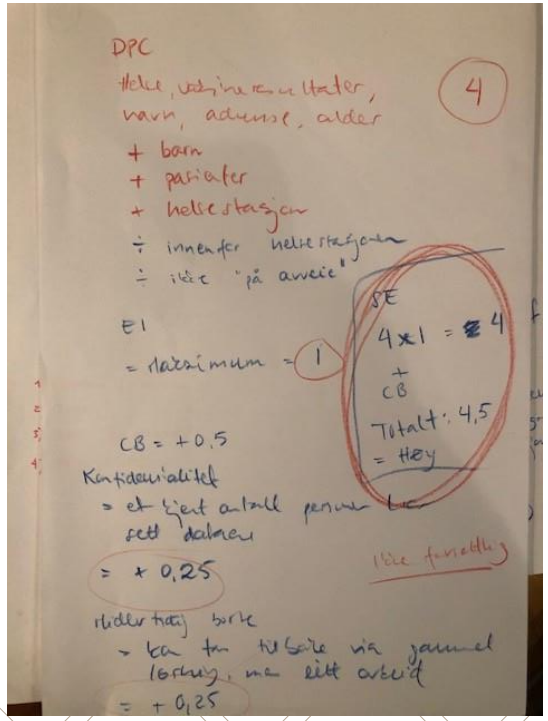
Risikovurdering ved brudd

- «risiko for fysiske personers rettigheter og friheter»
- Objektiv vurdering:
  - Type brudd
  - Hva slags personopplysninger, og hvor mye
  - Hvor lett er det å identifisere den registrerte?
  - Konsekvenser for de registrerte (alvorlighetsgrad/severity)
  - Hva slags registrerte - kategorier
  - Hvem er behandlingsansvarlig - kategorier
  - Hvor mange er rammet av bruddet?

Enisa: Severity assessment



- Enisa Europe
- Vurdering av alvorligheten av databrudd



Praktiske råd – ved personvernbrudd

- Vi har rutine for å vurdere sannsynligheten for konsekvenser for den registrerte
- Vi vet at Datatilsynet er rette myndighet i Norge
- Vi kjenner til fristene for varsel til DT og de registrerte
- Vi har på plass rutiner for varsling av DT, og hva varselet skal inneholde
- Vi har på plass rutiner for varsling av de registrerte, og hva varselet skal inneholde
- Vi vet at vi bør gi de registrerte råd om hvordan de kan minimere konsekvensene av bruddet
- Vi har rutiner for dokumentasjon av alle brudd

Risikoen ligger vel i boten?

- Uforutsette konsekvenser av å bli dratt inn i en lang og kostbare tilsynsprosess
  - Ressurskrevende
  - Kostbart internt og eksternt
  - Konsekvenser for omdømmet i markedet
- Gjenopprette sikkerheten
- Avbrudd i drift

Kultur internt

- Hvordan skape en kultur som oppfordrer til rapportering av brudd?
  - Ledelsen må være tydelig
  - Oppfordre til rapportering
  - Åpenhet om hva som gjøres for å forbedre personopplysningssikkerheten
  - Skape bevissthet og læring

Personvernbrudd må gjøres forståelig

- Personopplysninger tapt, endret, ødelagt, skadet eller spredt
- Utarbeide eksempler i egen bedrift:
  - Menneskelige feil
  - Svikt i retningslinjer eller rutiner
  - Tekniske feil
  - Cyberangrep

Virksomheten er avhengig av et visst kunnskapsnivå om personvern og en sikkerhetskultur i hele sin drift.

Praktiske råd- vurdering og innsending

- Opplæring i å identifisere personvernbrudd
- Ha på plass rutiner for databrudd med respons-plan og ansvarsfordeling
- Ansatte vet hvem de skal varsle internt og eskaleringsprosess
- Rollen som «utfyller/innsender» i Altinn er fastsatt
- Analyse av årsak, behov for tekniske eller organisatoriske endringer

Brannøvelse – hvilke steg?

Personvernbruddet - konsekvenser

- Følge rutine for sikkerhetsbrudd
- Hvem ansvarlig?
- Hvem skal ha beskjed?
- Hvem skal vurdere konsekvensene av bruddet?
- Hvordan vurdere konsekvensene av bruddet?
- Hvem skal varsle?

Praktiske råd - for alle

- Kunnskap
- Kultur
- Rapporterings-mal
- Brevmal til de berørte registrerte
- Brannøvelse, NB! kort frist
- Kort sjekkliste lett tilgjengelig

Takk!

BULL&CO

ADVOKATFIRMA