



simonsen  
vogtwtig

# Sanksjoner ved overtredelse av personvernforordningen

Senioradvokat (PhD ) Thomas Olsen  
Personvernkonferansen 2. desember 2016

[www.svw.no](http://www.svw.no)

# Oversikt

- Overblikk forordningen
- Klagemulighet til Datatilsynet
- Klagemulighet domstolene
- Rett til å kreve erstatning
- Datatilsynenes sanksjonsmuligheter

# Ny personvernforordning

*Forordning 2016/679/EU – General data protection regulation ("GDPR")*

- Forordning med direkte effekt (ikke direktiv)
- Viderefører dagens grunnprinsipper
- Økte dokumentasjonskrav (sml. internkontroll)
- Vurdering av personvernkonsekvenser (DPIA)
- Innebygd personvern (Data protection by design and by default)
- Ikke lenger meldeplikt (men konsultasjonsplikt i visse tilfeller)
- Data protection officer (DPO) i større grad obligatorisk
- Nye/skjerpede rettigheter
  - informasjon og samtykke
  - dataportabilitet
  - sletting ("right to be forgotten")
  - Varsling av registrerte ved sikkerhetsbrudd
- Strengere sanksjoner (20 M Euro / 4 % av årlig omsetning)

# Rett til å klage til Datatilsyn

*Art 77*

- Den registrerte kan klage til Datatilsynet der
  - den registrerte er bosatt
  - den registrerte arbeider
  - der krenkelsen finner sted
- Datatilsynet skal informere klager om
  - fremdriften
  - resultatet
  - muligheten for å påklage vedtaket

# Rett til effektiv klageadgang

*Art 78*

- Fysiske og juridiske personer har rett til effektiv rettslig overprøving av rettslig bindende beslutninger fra Datatilsyn som berører vedkommende
- Også dersom Datatilsynet ikke håndterer klagen eller ikke informerer registrerte innen 3 mnd om progresjonen eller resultatet av klagen
- Sak mot Datatilsynet skal fremmes for domstol i den staten hvor tilsynet er etablert
- Datatilsynet skal oversende evt. vurdering eller beslutning fra "the Board" til domstolen

# Rett til å saksøke BA og DB

*Art 79 og 81*

- Registrerte kan kreve domstolsprøving av hvorvidt det har skjedd en krenkelse av registrertes rettigheter som følge av overtredelser fra BA eller DB
- Saken kan bringes inn for domstolen i den staten
  - hvor BA eller DB er etablert, eller
  - der den registrerte er bosatt
    - (med mindre BA eller DB er offentlig myndighet under utøvelse av offentlig myndighet)
- Domstolen skal ta initiativ til å få bekreftet hvorvidt saken er til prøving i en annen stat
  - Kan suspendere videre prosess
  - Kan avstå fra å behandle sak dersom den andre domstolen er kompetent

# Rett til å kreve erstatning

*Art 82*

- Enhver person kan kreve erstatning fra BA eller DB for økonomisk og ikke-økonomisk tap (oppreisning) som følge av krenkelse av forordningen
- DB er ansvarlig for tap knyttet til behandling bare i den grad DB
  - Ikke har overholdt forpliktelser som spesifikt gjelder DB
  - Har handlet utover eller i strid med lovlige instruksjoner fra BA
- BA/DB går fri fra ansvar hvis de kan bevise at de "ikke på noen måte" var ansvarlig for hendelsen som var årsak til tapet
- Av effektivitetshensyn kan hver involvert BA/DB holdes ansvarlig for hele tapet
  - Presisert at BA/DB kan kreve regress av "medskyldige" BA/DB

# Representasjon av registrerte

*Art 80*

- Registrerte kan gi ideell organisasjon (non-profit) mandat til å føre sin sak overfor Datatilsyn/domstolene og til å kreve erstatning
  - Forutsatt at organisasjonen er stiftet i tråd med lokal rett
  - Lovfestet formål om å ivareta allmenne interesser
  - Er aktiv i arbeid med å ivareta personverninteresser
- Medlemsstatene kan også bestemme at ideelle organisasjoner på eget initiativ kan klage til Datatilsyn/domstolene



# Datatilsynenes sanksjonsmuligheter

*Art 58 og 83*

- Veiledning og informasjon
- Gi ulike typer godkjenninger (bl.a. standardkontrakter, BCR, sertifiseringsordninger mv.)
- Kompetanse til å føre tilsyn
  
- Vidt spenn av sanksjonsmuligheter mot BA og DB:
  - Advarsler om sannsynlige fremtidige overtredelser
  - Reprimande for begåtte overtredelser
  - Pålegg, bl.a. vedr. varslings av sikkerhetsbrudd eller å endre/opphøre med behandling

# Overtredelsesgebyr

- Datatilsynet skal vurdere konkret om det skal ilegges overtredelsesgebyr
  - Tillegg eller som alternativ til andre sanksjoner
  - Overordnede hensyn: effektiv, forholdsmessig og preventiv/avskrekkende
- Nasjonal lovgiver kan bestemme hvorvidt offentlig myndigheter kan ilegges gebyr
  - 1) 10 mill. Euro / 2 % av global omsetning (høyeste beløp av de to)
  - 2) 20 mill. Euro / 4 % av global omsetning
- 2 og 4 % referer til forrige års globale omsetning for "undertaking" / foretak
  - Begrepet "undertaking" (konkurranseretten, saker CJEU C-159/91 og C-160/91)
    - Enhver enhet involvert i økonomisk aktivitet, uavhengig av rettslig status og finansiering

# Vurderingsmomenter for gebyr/størrelse

*Art 83*

- Alvorligheten av overtredelsen (varighet, antall berørte, påført tap mv)
- Skyldgrad
- Tiltak fra BA/DB for å begrense tapet/krenkelsen
- Graden av ansvarlighet for BA/DB i lys av tiltak knyttet til sikkerhet og innebygd personvern
- Relevante tidligere overtredelser
- Graden av samarbeid med tilsynsmyndigheten for å rette avviket og dets konsekvenser
- De aktuelle kategoriene av opplysninger
- Hvordan overtredelsen ble kjent for tilsynet, særlig hvorvidt tilsynet ble varslet
- Hvorvidt det er gitt advarsel, reprimande eller pålegg, og om disse er blitt fulgt
- Etterlevelse av code of conduct eller sertifiseringsmekanisme
- Andre faktorer, for eksempel økonomisk fordel (profitt/unngå tap)

# (1) 10 mill. Euro / 2%

*Art 83 nr. 4*

- Behandling av personopplysninger vedr. barn (samtykke 16/13 år)
- Innebygd personvern
- Databehandleravtale
- Oversikt over behandlinger (internkontroll)
- Samarbeid med tilsynsmyndigheter
- Sikkerhet
- Varsling av sikkerhetsbrudd til tilsyn og registrert
- Konsekvensutredning (DPIA)
- Konsultasjonsplikt med tilsynet
- Oppnevning og oppfølging av data protection officers oppgaver
- Manglende etterlevelse av sertifiseringsordning

## (2) 20. mill. Euro / 4 %

*Art 83 nr. 5 og 6*

- Grunnvilkår for behandling av personopplysninger
- Den registrertes rettigheter
  - Informasjon
  - Innsyn, retting og sletting ("right to be forgotten")
  - Begrensninger på behandlingen
  - Varsling til mottakere om retting, sletting og begrensninger
  - Motsette seg behandling (bl.a. markedsføring og profilering)
  - Automatiserte beslutninger, inkl. profilering
- Overføring til tredjeland
- Særlige nasjonale regler (bl.a. ytringsfrihet, fødselsnummer, arkiv og arbeidsliv)
- Overse pålegg fra tilsynsmyndigheten

# Mulighet for nasjonale straffesanksjoner

*Art 84 "Penalties"*

- Medlemslandene kan vedta regler om andre sanksjoner, særlig for overtredelser som ikke er gjenstand for overtredelsesgebyr
- Spørsmål om videreføring av regler om
  - Dagmulkt
  - Fengsel og/eller bøter

# Avsluttende kommentarer

- Harmoniseringsnivå
  - Fortalen nr. 11: "equivalent sanctions"
  - Etablering av faste satser?
- Svært mye strengere sanksjoner – start forberedelsene nå!
- "Dokumentere compliance" (sml. internkontroll eller norske regler)
- Kartlegg avvik og risiko
- Regulering av ansvar i kontrakter
- Mer utbredt med forsikringsordninger?



Personvern-  
håndboken

En praktisk bok om personvernregelverket

Malin Tønseth, Marit Stubø,  
Thomas Olsen og Rune Ljostad



simonsen  
vogtviig

Takk for oppmerksomheten!



Thomas Olsen  
Senioradvokat (PhD)

tol@svw.no

T: +47 21 95 57 55

M: +47 922 56 404