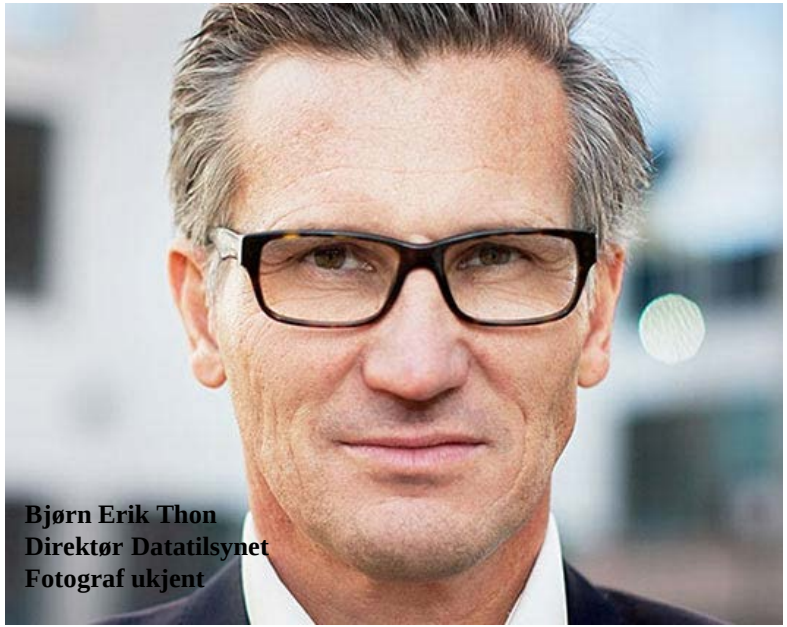
NORWEGIAN
BUSINESS SCHOOL

Stiftelser og GDPR
- noen vesentlige endringer i kravene til personvern?

Retningslinjer for nye personvernkrav

- datatilsynet har utarbeidet retningslinjer



Bjørn Erik Thon
Direktør Datatilsynet
Fotograf ukjent

Hva skal jeg snakke om?

- Litt historikk - intro
- Foreliggende personvernforpliktelse
- Innholdet i GDPR
- Noe spesielt for stiftelser?

Litt historikk– intro

GDPR-forordningen

- vedtatt av EU 27. april 2016
- «forordning» – betyr at teksten er den samme i hele EU–harmonisering
- skal gjennomføres i norsk rett innen 25. mai 2018
- bygger på
  - personverndirektivet (directive 95/46/EC) og personopplysningsloven av 14.4. 2000 nr. 31
  - nyere rettspraksis. Etablerer nye prinsipper
- bedrifter/organisasjoner som var «compliant» etter ppl. også i stor grad «compliant» etter GDPR

Definisjoner – GDPR art. 4

- **personopplysninger**;
  - enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»)
- **behandling**;
  - enhver operasjon som gjøres med personopplysninger
- **pseudonymisering;**
  - opplysningene ikke lenger kan knyttes til en bestemt registrert
- **behandlingsansvarlig;**
  - fysisk eller juridisk person som bestemmer formålet med behandlingen
- **databehandler**;
  - fysisk eller juridisk person som behandler personopplysninger på vegne av den behandlingsansvarlige

Personopplysningsloven – nåtilstand

Prinsipper under EU-direktivet av 1995
- proporsjonalitet mellom sikkerhet og risiko

- Bare databehandlingsansvarlige hadde forpliktelser etter direktivet
  - Databehandler bare ansvarlig gjennom databehandleravtalen– kontraktsansvar

- Formålet med direktivet; var å sikre «forsvarlig behandling» av personopplysninger
  - fokus på tekniske og organisatoriske forhold
  - ikke på legitimitet og konsekvenser av behandlingen i seg selv

- Sårbarhet knyttet til sikkerhet
  - risiko sett ifh. til at opplysninger skulle tilfalle offentlighet eller i gale hender
  - desto mer sensitive data- desto større krav til sikkerhet

Forskriften til personopplysningsloven
- som hadde hjemmel i ppl. § 3, 2. ledd

- skulle sikre proporsjonalitet (§ 2-1)
- sikkerhet (§ 2-3)
- risiko analyse (§ 2-4)
  - skal dokumenteres skriftlig
  - gjelder all behandling (!)
- jevnlige sikkerhetsrevisjoner (§ 2-5)
- krav til forsvarlig adferd ved sikkerhetsbrudd (§ 2-6)
  - restart normale prosessser, finne årsak og unngå gjentakelse
  - varsle DT hvis brudd på konfidensialitet
- krav til etablering av systematisk internkontroll (§ 3-1)

Norsk lov har vært strengere enn direktivet!

Norsk lov strengere enn direktivet fra 1995!

- overgangen derfor enklere

- forpliktelser gjelder både databehandler og data-ansvarlige
- dokumentasjonsplikt for gjennomført risikoanalyse
- krav til etablering, vedlikehold og dokumentasjon av internkontroll
- gjelder all form for databehandling!
- Eksempel: Gjensidige forsikring (PVN-2013-27)
    - Forsikringsselskap fikk NOK 600 i bot for å mangle internkontrollsystemer
    - Opplysninger om personers krav om dekning av kostnader for medisinsk behandling tilgjengelig for *alle i selskapet*

GDPR– innhold

Det nye personvernregelverket

Justis- og beredskapsdepartementets høringsnotat av 6. juli 2017 (Snr.17/4200)

- GDPR– general data protection regulation
- informasjonssikkerhet et grunnprinsipp
- krav til proporsjonalitet teknisk og organisatorisk- egnet sikkerhetsnivå for å ivareta registrertes rettigheter og friheter
- altså som i direktivet, men mer fremtredende
    - art. 5 (1) f) (ved behandling av personopplysninger)
    - art. 24 (1) (behandlingsansvarliges ansvar)
    - art. 25 (1) og (2) (innebygd personvern og personvern som standardinnstilling)
    - art. 28 (1) (databehandleravtale med klare vilkår om forpliktelsen)
    - art. 32 (egnet sikkerhetsnivå i forhold til risikoen for registrertes rettigheter og friheter)

Det nye personvernregelverket

Personopplysningsloven av 2018

- EUs personvernforordning "gjelder som norsk lov" (§ 1)
- norsk oversettelse av forordningen blir vedlegg til loven
- nasjonale bestemmelser på visse områder (§§ 2-23) – herunder arbeidsliv

- Særlovgivning
  - pasientjournalloven
  - helseregisterloven
  - arbeidsmiljøloven
  - ulike taushetspliktregler i annen lovgivning

Det nye personvernregelverket
- anvendelsesområde

Regler for vern av fysiske personer (art. 1)

- «sikring av grunnleggende rettigheter og friheter»
- ved helt eller delvis automatisert behandling av personopplysninger (art. 2)
- også ikke-automatisert behandling, dersom inn i register

Bakgrunnen for endring

Økt risiko for personvernkrenkelser på grunn av

- teknologisk utvikling
- internasjonalisering

Vil sikre EUs posisjon i "den digitale tidsalder"

- bygge tillit hos forbrukerne/kundene

Fullharmonisering (forordning vs. direktiv)

- begrense byråkratiet (hos virksomheter og medlemsstater)
- hindre forumshopping (etablering i land med lavt vern)

Personvernprinsippene videreføres
- artikkel 5

- **Lovlighet**: rettslig grunnlag
- **Rettferdighet**: krav til forholdsmessighet mellom inngrep og formål
- **Gjennomsiktighet**: informasjonsplikt og innsynsrettigheter
- **Formålsbegrensning**: spesifikke, uttrykkelig angitte og berettigede, forbud mot uforenlige formål
- **Data minimering**: opplysningene skal være adekvate, relevante og nødvendige
- **Kvalitet**: opplysningene skal være korrekte og oppdaterte

Personvernprinsippene videreføres

- artikkel 5

- **Lagringsbegrensning:** opplysningene skal anonymiseres eller slettes når behandlingen er ferdigstilt (formålet)
  - unntak: arkiv/forskningsformål
- **Integritet og fortrolighet**: må sikre tilstrekkelig sikkerhet mot uautorisert eller ulovlig behandling og utilsiktet tap, ødeleggelse eller skade
- **Ansvarlighet**: den behandlingsansvarlige er ansvarlig for og skal kunne påvise at prinsippene overholdes

Sentralt å avklare for virksomheter

1. Hvorfor behandler vi personopplysninger?
2. Hvilket ansvar har vi for behandlingen?
3. Har vi lov til å behandle personopplysningene?
4. Hvilke lovbestemte plikter har vi ved behandlingen?
5. Hvordan skal vi sørge for at vi oppfyller pliktene?

1. Hvorfor behandler vi personopplysninger?
- art. 5, 1 b)

Formålet må defineres på forhånd!

Lovligheten avhenger av formålet/ene med behandlingen:

- foreligger behandlingsgrunnlag?
- hvilke opplysninger er nødvendige og relevante?
- hvilke formål er uforenlige?
- når skal opplysningene slettes?

«Spesifikke, uttrykkelig angitte og berettigede formål»

- "spesifikke": så spesifikt at man kan vurdere lovligheten av bruken
- "uttrykkelige": angis med klart språk, forståelig både for de registrerte og tilsynsmyndigheten
- "berettigede": formålet i overensstemmelse med "gjeldende rett"

2. Hvilket ansvar har vi?

«Behandlingsansvarlige»

- den som bestemmer formålet med behandlingen og hvilke midler som skal benyttes
- den ansvarlige skal påvise at behandlingen skjer i samsvar med loven
- arbeidsgiver er vanligvis behandlingsansvarlig ved behandling av opplysninger om ansatte

« Databehandler»

- behandler personopplysninger på vegne av en behandlingsansvarlig
- begrensede plikter, men flere etter forordningen enn etter gjeldende rett
- typisk ansvar for drift og vedlikehold av HR-systemer, adgangskontrollsystemer
- tidsregistreringssystemer osv.

3. Har vi lov til å behandle?
- spørsmål om grunnlag

Lovens utgangspunkt: Det er forbudt å behandle personopplysninger!

Krav til behandlingsgrunnlag
- samtykke; fra den registrerte selv
- lovhjemmel; lovgiver, eks. lov om hvitvasking, lov om finansielle instrumenter
- nødvendighetsgrunner: den behandlingsansvarliges egen beslutning

Noe strengere krav til behandlingsgrunnlagets klarhet og tyngde enn gjeldende rett
- krav om lovhjemmel i flere sammenhenger
- skjerpede krav til samtykke

Fremdeles skjerpede vilkår ved behandling spesielle kategorier personopplysninger

«Samtykke»
- art. 5 jf. art. 4 (definisjoner)

Samtykke:

- "enhver frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder" (art. 4)

- Uttalt presumpsjon for at samtykke ikke er frivillig når det er en klar ubalanse mellom partene, typisk arbeidsgiver og ansatt (fortalen til forordningen)

- Samtykke antagelig ikke anvendelig ved behandling av sensitive opplysninger

- Ved behandling av ikke-sensitive opplysninger – må være utvilsomt frivillig

Lovlighet
- art. 6

Lovhjemmel

- av hensyn til at den behandlingsansvarlige eller den registrerte skal kunne oppfylle sine forpliktelser og utøve sine særlige rettigheter
- nødvendig for at arbeidsgiver skal oppfylle arbeidsavtalen med den ansatte. Eks. betale ut lønn
- nødvendig for å ivareta andre berettigede interesser. Kun dersom ikke hensynet til den ansattes personvern går foran (interesseavveining)

NB! Ikke ved behandling av sensitive opplysninger, se art. 9 for definisjon

Nødvendighetsgrunner
- Art.6

Nødvendig for å fastsette, gjøre gjeldende eller forsvare rettskrav

- Oppbevaring etter arbeidsforholdets opphør dersom det er sannsynlig at det oppstår en konflikt i etterkant, for eksempel diskriminering, urettmessig avskjed osv.

- Granskninger og miljøkartlegginger

4. Hvilke plikter har vi?

- Begrense behandlingen til opplysninger som er nødvendige og relevante
- Holde opplysningene korrekte og oppdaterte
- Ivareta de registrertes rettigheter

Immanuel Kant, Gary Brown

De registrertes rettigheter

- Innsynsrett, art. 15
- Rett til korrigering, art. 16
- Rett til sletting ("retten til å bli glemt"), art. 17
- Rett til begrensning av behandling, art. 18
- Rett til dataportabilitet, art. 20
- Innsigelsesrett ("right to object"), art. 21
- Rett til å ikke være gjenstand for automatiserte individuelle avgjørelser, herunder profilering, som har rettsvirkning, art. 22

5. Hvordan sikre etterlevelse?

Etablere tekniske og organisatoriske tiltak

- som står i forhold til behandlingens art og omfang
- som er tilpasset virksomheten størrelse og organisering
- som er dokumenterte og kan presenteres for Datatilsynet ved en kontroll

a. Organisatoriske tiltak

Hvem skal har det interne ansvaret for å påse at behandlingen er lovlig?

Skal eller må vi ha en personvernrådgiver (ombud)?
Absolutt plikt for:

- alle offentlige organer og myndigheter
- selskaper, når kjernevirksomheten involverer
  - storskala behandling av sensitive personopplysninger
  - storskala monitorering/profilering av individer

b. Instruksjon av egne ansatte

- Enhver person som behandler personopplysninger på vegne av en behandlingsansvarlige må gjøre dette etter instruks fra den behandlingsansvarlige

- Interne rutiner: Hvem, hva, når, hvordan og hvorfor?

- Gjennomførende og kontrollerende
  - revisjoner
  - avvikssystemer

c. Databehandleravtaler

- med andre enn egne ansatte som behandler personopplysninger på behandlingsansvarliges vegne

- Formål
  - etablere instruksjonsmyndighet og rådighetsforbud
  - gi instrukser for hvordan behandlingen skal gjøres

NB! Utvidede og strenge krav til databehandleravtaler, jf. opplisting i artikkel 28

d. Innebygd personvern

- Plikt til å iverksette *forholdsmessige* tiltak for å implementere personvernprinsipper i informasjonssystemene, for eksempel:
  - unngå *overskuddsinformasjon* ved å unngå fritekstfelt
  - sikre informasjonssikkerhet gjennom tilgangsbegrensninger
  - sikre kvalitet gjennom automatiserte rutiner for vask av opplysninger mot for eksempel offentlige registre
  - sikre sletting gjennom automatiserte rutiner
  - gi de registrertes adgang til å ivareta rettigheter, gjennom "min side-løsninger" (innsyn, informasjon, tilbaketrekking av samtykke, retting, mm.)

6. Hva er risikoen ved lovbrudd?

Manglende dokumentasjon er tilstrekkelig til å konstatere lovbrudd

Sanksjoner fra Datatilsynet

- administrative bøter på inntil 20 millioner Euro
- irettesettelse ved ulovlig behandling
- advarsel ved planlagte ulovlige behandlinger
- pålegg, herunder forbud mot videre behandling

Erstatning og oppreisning

Omdømmetap

Noe spesielt for stiftelser?

Stiftel. § 1: «formuesverdi som ved testament, gave eller annen rettslig disposisjon selvstendig er stilt til rådighet for et bestemt formål av ideell, humanitær, kulturell, sosial, utdanningsmessig, økonomisk eller annen art»

Stiftelser forts.
- noe å tenke på

- Er det ansatte ?
- Søknader om støtte?
- Enkeltpersoners henvendelse til stiftelsen?
  - er formålet med innhentingen fastlagt og formidlet?(art. 13, 1 c)
  - hva er nødvendig personopplysninger for søknadsbehandling?
  - fremgår informasjon om den behandlingsansvarlige og ev. personvernombud på tidspunktet for innhentingen av opplysningene? (art. 13)
  - er opplysningene korrekte? (art. 16)
  - er det etablert rutiner for sletting av personopplysninger etter beslutning om utdeling (art. 17)

Takk for meg!

Irina.e.toien@bi.no