NTNU

Kunnskap for en bedre verden

Kontraktsmessige følger av at personopplysninger skal inngå i prosjektet – ny personvernforordning

6. Mars 2018 NARMA

Av Åshild M. Revhaug, NTNU

GDPR – ny personvernforordning

- Personvernforordningen (2016/679) trer i kraft 25. mai 2018.
- Erstatter direktiv 95/46/EF.

- **MÅL:**
- harmonisering av medlemsstatens regelverk (EØS)
- Forene kravene til privatliv og innovasjon
- Sikre rettsikkerhet for individers personvern gjennom bærekrafttige tiltak ved en teknologinøytral tilnærming

Rettskildene – i dag

- **Personopplysningsloven** (POL)
  - lov 14. april 2000 nr. 31

  - **Personopplysningsforskriften** – (POF)
  - forskrift 15. desember 2000 nr. 1265

Loven og forskriften gjennomfører EU-direktiv 95/46/EF

- Helseforskningsloven
- Helseregisterloven
- Forskningsetikkloven

Hvem har rettigheter og plikter

- Plikter:
  - Behandlingsansvarlig (BA)
  - Databehandler (DB)
  - Underleverandør
- Rettigheter:
  - De registrerte; ansatte, studenter, forskningsdeltakere, andre

Sentrale bestemmelser

- **Krav om et rettslig grunnlag** §§ 8 og 9.
- Samtykke, el lov, el nødvendighetskrav (a-f)
- § 9: Strengere krav ved sensitive opplysninger, tilleggskrav

- Krav om **informasjonssikkerhet** og **internkontroll**
- Krav om konfidensialitet, integritet og tilgjengelighet
- Dokumentasjonskrav

GDPR

Nytt regelverk 2018

- **GDPR – ny EU forordning blir norsk lov mai 2018**
- 99 artikler samt nasjonale lovbestemmelser, mulighet for unntak i forskning, se art. 89

- En del sentrale fortalepunkt
- Forskning vidt definert
- Viderebruk av personopplysninger ved forskningsformål (se fortalepkt 156)

Nytt regelverk 2018 - endringer

- Konsistensmekanisme
- Forordningen gjelder også leverandører utenfor EØS som vil tilby tjenester innen EØS-området

- Meldeplikt og konsesjonsplikt bortfaller
- Erstattes med plikt til internkontroll og vurdering av personvernkonsekvenser (DPIA) (art 35)
- Krav om forhåndsdrøftelser med Datatilsynet
- Dokumentasjonskrav, strengere
- Personvernombud (DPO) off + stor skala, sensitiv po

Endringer forts.

- Styrkede og nye rettigheter for de registrerte
  - Retten til å bli glemt, retten til dataportabilitet)

- Personvern som standardinnstilling og krav til innebygd personvern
- 72 timers krav ved melding til Datatilsynet (art 33)
  - ny avviksløyfe

- Detaljerte krav om innhold til varsel – også krav om varsling til de registrerte (art 34)

- Krav om personvernerklæring(er)

Nytt regelverk 2018 forts

- Et økt kontrollregime som bygger på et grenseoverskridende myndighetsamarbeid av tilsynsmyndighetene

- Høyere bøtenivå/sanksjoner- inntil 4 % av omsetning

Krav til informasjonssikkerhet

- Krav om tekniske og organisatoriske tiltak, må ses i forbindelse med personvernprinsippene i artikkel 5.
- Krav til informasjonssikkerhet – KIT – konfidensialitet – integritet – tilgjengelighet
- Åpen forskning – men så «lukket som nødvendig»
- Personvern en kritisk verdi – styringssystem for informasjonssikkerhet

Sentrale prinsipper art. 5

Behandlingsansvarlig (BA) skal påse og dokumentere at personvernprinsippene etterleves:

- Lovmessighet
- Rettferdighet og gjennomsiktighet
- Dataminimering
- Korrekthet/nøyaktighet/riktighet
- Lagringsbegrensning
- Intergritet og konfidensialitet
- Ansvarlighet
- Iverksette tekniske og organisatoriske tiltak, jf art. 24

Databehandleravtale

- <u>Krav om inngåelse av databehandleravtale</u>
  - Også i dag

- Nytt er at forordningen regulerer *minimumskrav* til innholdet, jf art. 28
- Flere forpliktelser for DB
- De registrerte kan kreve erstatning både fra BA og DB
- Ingen overgangsordninger

Behandlingsansvarlig el databehandler

- Controller (BA) – “means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data”

- Processor (DB) – “means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”

- Joint controllers – artikkel 26 - felles behandlingsansvar

Tiltak artikkel 24

- "*Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the* ***controller*** *shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation..*"

Krav til skriftlige protokoller art 30

- Krav til dokumentasjon over behandlingsaktiviteter

- Sammenheng med krav til «datahåndteringsplaner»
- Krav om protokoller både for BA og DB

Krav om innebygd personvern

- «Privacy by design»
- Forebygging – personvernvennlige løsninger
- Standardinnstillingene settes opp slik at
  - ikke flere personopplysninger enn nødvendig samles inn,
  - det finnes et lovlig formål med innsamlingen, system for samtykke
  - sikker tilgangsstyring, logging
  - det er satt tekniske begrensninger for bruken av opplysningene,
  - unngå fritekstfelter
  - opplysningene slettes når formålet er oppnådd
  - løsninger for innsyn om egne opplysninger, informasjon
  - https://www.datatilsynet.no/globalassets/global/skjema-maler/sjekkliste-for-innebygd-personvern.pdf

Overføring til tredjeland

- Land/organisasjoner utenfor EØS-området
- Forordningen kapittel V – se fortalepkt 101 flg.
- Behov for særskilt grunnlag - tilstrekkelig beskyttelse (i dag se pol § 30)
- Hvordan overføring kan skje:
  - Kommisjonens beslutning om trygg overføring jf art 45 (3)
    - (https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en)
  - Standardkontrakter (model clauses) om overføring, egen mal for BA og DB
  - certification mekanisme (art 42, jf art 43, f.eks. privacy shield)
  - codes of conduct/atferdsnormer (art 40 j)

Spørsmål

- Hvem er behandlingsansvarlig?
- Hva er grunnlaget for behandlingen av personopplysninger?
- Kan data overføres på en tilfredsstillende sikker måte i tråd med regelverket?
- Brukes underleverandører dersom bruk av databehandler?

Håndtering

- Avklar roller
- Dokumenter vurderinger, grunnlag og risiko/ros-analyse
- Være tydelig på hvilke personopplysninger som behandles – sensitive, helseopplysninger, biometriske osv.
- Dersom bruk av databehandler – sjekk hvor de har serverne sine
  - Tredjelandsproblematikk…Forsvarlig overføring - overføringsmaler
  - Reguler bruk av underleverandører
  - Sørg for at prinsippene i artikkel 5 ivaretas
- Dersom delt behandleransvar, reguler dette i avtale mellom partene.

Nyttige lenker

- Datatilsynet:
  - https://www.datatilsynet.no/regelverk-og-skjema/nye-personvernregler/
  - https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/overfore/
- Data protection authority uk (ICO):
  - https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf
- Eus nettsider:
  - https://www.eugdpr.org/eugdpr.org.html
- Personvernforordningen på norsk:
  - https://www.datatilsynet.no/globalassets/global/regelverk-skjema/forordningen/uoffisiell-norsk-oversettelse-av-personvernforordningen.pdf