Databehandleravtaler

Tommy Tranvik

Unit

Spørsmål

- Hva er databehandlere?
- Når er det lovlig å bruke databehandlere?
- Hva må til for at fortsatt bruk skal være lovlig?

Databehandlere i GDPR

- Leverandører av bestemte typer IT-tjenester (gratis eller mot betaling)
  - hvor personopplysninger håndteres på vegne av «kunden»
  - håndtering av personopplysninger er hoved-leveransen
- «Kunden» er behandlingsansvarlig
  - velger hvilke IT-tjenester som skal leveres og hvilke leverandører som skal benyttes
  - står ansvarlig for sine valg – at leverandørene håndterer opplysningene på riktig (lovlig) måte
- Leverandørene har et selvstendig ansvar for riktig (lovlig) håndtering av opplysningene

Plikter – behandlingsansvarlig

- Må selv ha lov til å håndtere personopplysningene før de kan «overleveres» til leverandører (databehandlere)

- Må velge en lempelig leverandør – en seriøs aktør med kapasitet til å gjøre det som kreves av ham

- Dette innebærer tre typer plikter

  - utredningsplikt (før bruk)
  - avtaleplikt (før bruk)
  - oppfølgingsplikt (under bruk)

Utredningsplikten

- Sjekke leverandørens tjeneste før den tas i bruk
- Innholdet i utredningsplikten
  - sjekke at leverandøren kan håndtere personopplysningene på riktig måte
  - vurdere om informasjonssikkerheten i tjenesten er tilfredsstillende
    - ✓ konfidensialitet
    - ✓ integritet
    - ✓ tilgjengelighet
    - ✓ motstandsdyktighet

Avtaleplikten

- Inngå avtale med leverandøren (databehandleravtale) før tjenesten tas i bruk

- Avtalen skal beskrive hva leverandøren kan gjøre med opplysningene og hvordan de skal sikres

- GDPR regulerer derfor

  - at det skal inngås avtale
  - når avtalen skal inngås
  - hva avtalen skal inneholde

Avtaleinnhold # 1

- Forplikter leverandøren seg til å behandle opplysningene etter instruks fra virksomheten?
    - formålsbegrensning: hva leverandøren (og eventuelle underleverandører) vil bruke opplysningene til?
- Gir leverandøren informasjon om hvor i verden opplysningene havner?
    - spesielle vilkår ved overføring av opplysninger til tredjeland (land utenfor EØS-området)
- Gir leverandøren informasjon om eventuelle underleverandører, blant annet
    - hvem underleverandørene er og hva de gjør?
    - i hvilke land underleverandørene er etablert?
    - hvordan leverandøren kontrollerer sine underleverandører («speilavtaler»)?

Avtaleinnhold # 2

- Hvordan sørger leverandøren for at vesentlige endringer blir varslet til og (eventuelt) godkjent av virksomheten?
- *Forklarer leverandøren hvordan krav om utlevering av opplysninger til politi eller andre myndigheter vil bli håndtert?*
- Forplikter leverandøren seg til å varsle om sikkerhetsbrudd og forklares hvordan slik varsling vil skje?
- Hvordan bidrar leverandøren til at personvernrettighetene ivaretas?
    - den enkeltes rett til informasjon, innsyn, retting, sletting, innsigelse, begrensning, osv.

Avtaleinnhold # 3

- Hvordan ivaretas informasjonssikkerheten hos leverandører (og eventuelle underleverandører), for eksempel:
    - tilgangsstyring
    - datasegmentering
    - kryptering
    - sikkerhetskopiering
    - fysisk sikring
    - taushetsplikt
- Gis det tilgang til rapporter fra sikkerhetsrevisjoner hos leverandøren (og eventuelle underleverandører)?
- Forplikter leverandøren seg til å bistå ved gjennomføring av personvernkonsekvensvurderinger (DPIA)?
- Hva skjer med opplysningene når bruken av tjenesten opphører?

Oppfølgingsplikten

- Sjekke tjenesteleveransen mens tjenesten er i bruk
- Virksomheten skal jevnlig forsikre seg om at
  - leverandøren ivaretar sine plikter etter avtalen
  - opplysningene forblir tilfredsstillende sikret mot sikkerhetsbrudd
  - varsle Datatilsynet, eventuelt også de berørte (studenter, ansatte, forskningsdeltakere, osv.), om sikkerhetsbrudd
- Motta og gjennomgå rapporter fra sikkerhetsrevisjoner hos leverandøren
- Revidere risikovurderingen ved vesentlige endringer i tjenesten