WIKBORG | REIN

GDPR og PSD2

- særlig om håndtering av samtykke

Rolf Riisnæs

Advokat dr. juris

rri@wr.no

BITS seminar PSD2

11. oktober 2017

Bakgrunn

- PSD2 fastlegger at
  - *Behandling av personopplysninger skal skje i henhold til kravene i personverndirektivet (vil bli avløst av GDPR)*

- Samvirket mellom regelverkene er ikke nærmere avklart i PSD2

- Gjelder bl.a. kravet til samtykke
  - *PSD2: Behandling av personopplysninger knyttet til betalingstjenester skal bare skje med uttrykkelig samtykke fra kunden*
  - *Begrepet samtykke er nærmere definert i personopplysningsregelverket*

Formål

- PSD2
  - *Sikre forbrukerrettigheter*
  - *Legge til rette for konkurranse om betalingstjenester*

- Personvernforordningen
  - *Sikre den enkeltes rett til personvern som grunnleggende rettighet*
  - *Sikre fri utveksling av personopplysninger*

- => Stor grad av sammenfall, men prioriteringene kan være ulike

Personvernforordningen – iverksetting

- General Data Protection Regulation (GDPR)
  - *Avløser personverndirektivet og dagens personopplysningslov*
  - *Får virkning i EUs medlemsland fra 25. mai 2018*
- Innføres i Norge gjennom egen lov
  - *Iverksetting planlagt på samme tid som i EU*

Personvernforordningen – nytt og endret

- Grunnleggende begreper, roller og prinsipper består
- Justeringer (i norsk rett)
  - *Samtykke (beste praksis)*
  - *Internkontroll – protokoll*
  - *Risikovurdering – dybdeanalyse*
- Nytt
  - *Styrkede rettigheter for de registrerte*
  - *Plikt til å oppnevne personvernombud*
  - *Meldeplikt (og konsesjonsplikt) bortfaller*
  - *Databehandlere i større grad direkte regulert*
  - *Innebygget personvern og personvern som standard*
  - *Strengere sanksjoner (i hvert fall vesentlig høyere maksimalsatser)*

Personvernforordningen – virkeområde og begreper

- Virkeområde
  - *Gjelder all elektronisk behandling av personopplysninger*
- Begreper
  - *Personopplysninger*
    - Enhver opplysning som direkte eller indirekte kan knyttes til en enkeltperson
  - *Behandling*
    - Enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter

=> Alle elektroniske disposisjoner knyttet til en enkeltpersons konto berøres av personopplysningsrettens regler

Personvernforordningens roller

- Den registrerte
- Behandlingsansvarlig
- Databehandler

PSD2 – roller og rammer

- Relevante roller
  - *Kontotilbyder (ASPSP)*
  - *Betalingsfullmektig (PISP)*
  - *Opplysningsfullmektig (AISP)*

⇒ alle er selvstendig behandlingsansvarlige

⇒ alle disposisjoner utløser behandling av personopplysninger

Grunnkrav for behandling av personopplysninger

- Spesifisert behandlingsformål
- Lovlig behandlingsgrunnlag
- Tilstrekkelige og relevante opplysninger
- Datakvalitet og begrenset lagring
- Dataminimalitet

Vilkår for å behandle personopplysninger

- Krav til lovlig behandlingsgrunnlag (pol § 8)
- Personopplysninger kan bare behandles i henhold til:
  - Samtykke
  - Lovhjemmel
  - Eller behandling er nødvendig for:
    - a) å oppfylle en avtale med den registrerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås,
    - …
    - f) at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen.
- Tilleggskrav for behandling av *sensitive* personopplysninger (pol § 9)

Alternativet "samtykke"

- PSD2
  - *Uttrykkelig samtykke*
- Personvernregelverket
  - *Personopplysningsloven*
    - Frivillig, uttrykkelig og informert erklæring
  - *GDPR*
    - Frivillig, spesifikk, informert og utvetydig viljesytring

- Hvem innhenter samtykket og hvordan?
  - *Samtykke til å utføre en betalingstransaksjon kan gis via betalingsfullmektig, jf PSD2 Art. 64(2)*
- Hva med behandlingen av personopplysninger?
  - *Ikke utelukket å benytte tredjepart, MEN*
  - *Kontroll med oppfyllelse av grunnkravene til samtykke*
  - *Mangler ved samtykket vil innebære at behandlingen er ulovlig*

Alternativet "avtale"

- Kan kontotilbyder inngå avtale med kontoinnehaver om å akseptere forespørsler fra PISP/AISP?
- Er det praktisk?

Alternativet "lovhjemmel"

- Forslag til ny finansavtalelov § 71
  - *Gjennomføring av avtaler om betalingsfullmakt og opplysningsfullmakt krever uttrykkelig samtykke fra kunden.*
  - *Med mindre det foreligger objektivt begrunnede og dokumenterte forhold som gir grunn til å tro at nødvendig samtykke mangler, skal kontotilbyderen gi nødvendig tilgang til kontoen.*

- Kan lovhjemmelen presiseres?
- Presisering gjennom henvisning til omforente standarder (RTS) kan sikre forutberegnelighet og fleksibilitet

Sikker brukerautentisering

- Tilgang til kontotilbyders autentiseringstjenester
- Avtalte løsninger
- Hva med eIDAS?
  - *Forordning (910/2014) om eID og andre elektroniske tillitstjenester*

Foto: *Wikborg Rein, Erik Burås/STUDIO B13, Ilja Hendel, istockphoto.com*