Personvern og bransjeutfordringer

Nye «økosystemer» for bruk og utveksling av persondata

Advokat Arve Føyen

FØYEN TORKILDSEN

Forordning – i kraft i mai 2018

Bindende tekst for landene uten rom for endringer, verken strengere eller mildere

- *nesten…*

PSD2 – i kraft 1.1.2018 – forholdet til GDPR

Artikkel 94 Personvern

1. **Medlemsstatene skal tillate behandling av personopplysninger i betalingssystemer og av betalings tjenesteleverandører når det er nødvendig for å sikre forebyggelse, etterforskning og avdekking av betalingssvindel.**

   Informasjon til enkeltpersoner om behandling av personopplysninger og om behandling av slike personopplysninger og om enhver annen behandling av personopplysninger for de formål som er angitt i dette direktivet, skal gjøres i samsvar med Personverndirektivet (95/46 EC) (og etter 24.5.2018 GDPR)

2. **Betalingstjenesteleverandører skal bare ha tilgang til, behandle og lagre persondata som er nødvendig for deres ytelse av betalingstjenester, med et uttrykkelig samtykke fra den enkelte bruker av betalingstjenestene**

Nye regler - noe er som før

- Definisjon av personopplysning (nesten)
- Behandlingsansvarlig - databehandler
- Behandlingsgrunnlag: samtykke – avtaler – lov
- Informasjonsplikt
- Innsynsrett
- Sletteplikt
- Oppbevaringstid – «nødvendig»
- Internkontrolldokumentasjon

Men:

mye mer detaljert og mye blir svært annerledes

FØYEN TORKILDSEN

Each supervisory authority may impose administrative fines up to 20 000 000 EUR, or in case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, **whichever is higher**, for infringements of

- the basic principles for processing, including conditions for consent, the data subjects' rights
- the transfers of personal data to a recipient in a third country or an international organisation

Internkontroll

- **Norge har hatt slike regler siden 2000 – i varierende grad respektert**

- **Pol §§ 13 og 14**

Risk assessment and information security (DPA)

- **The controller shall carry out a risk assessment for its handling of personal information. The risk assessment must be seen in connection with established risk acceptance criteria, and the controller shall implement appropriate measures to achieve a satisfactory information security.**
- **To achieve satisfactory information security the controller shall ensure that the service in use, meets the requirements laid down during the work with the acceptance criteria and risk assessment.**
- **The assessment must be given greater weight when going from its own operations to cloud solutions, since the personal information will be outside the data controller's direct control.**

Hva må på plass i Norge pre-GDPR?

- **Tilstrekkelig lovkunnskap demonstreres via internkontrolldokumentasjon**
- **Rutine for å sjekke at hjemmel foreligger – avtale/samtykke/grunnlag i lov**
- **Vurdering av «formål» – nødvendig og adekvat behandling?**
- **Vurdering av personopplysningenes kvalitet i forhold til formålet med behandlingen**
- **Rutine for oppfyllelse av krav om innsyn og informasjon**
- **Rutine for oppfyllelse av personopplysningslovens regler om melde- og konsesjonsplikt**
- **Rutine for avviksbehandling, dokumentasjon av inntrufne avvik og håndtering av disse**
- **Rutine for opplæring**
- **Sikkerhetstiltak - oppnå tilfredsstillende konfidensialitet, integritet og tilgjengelighet**
- **Databehandleravtaler (!) - Det er flere underleverandører enn man tror**

Hva må på plass i Norge pre-GDPR (forts)?

- **Oversikt over hvilke data man forvalter – hvordan - Dokumentasjon av informasjonssystemet (opplysninger, prosesser, formål, applikasjoner, etc)**
- **Sikkerhetspolicy - beskriver mål og strategier for tilfredsstillende informasjonssikkerhet**
- **Sikkerhetsorganiseringen med roller og ansvar**
- **Rutiner for risikovurderinger (for alle systemer), dokumentasjon av utførte risikovurderinger**
- **Rutiner for sikkerhetsrevisjoner og personverngjennomganger/-revisjon,**
- **Dokumentasjon av utførte revisjoner**

Avvik i GDPR – mye strengere enn i dag

- **In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent, unless the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals.**
- **The processor shall notify the controller without undue delay after becoming aware of a personal data breach.**
- **When the personal data breach is likely to result in a high risk for the rights and freedoms of individuals, the controller shall communicate the personal data breach to the data subject without undue delay.**

Personopplysning - definisjon

Hva er en personopplysning? Når er regelverket relevant?

- **'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;**

- **Mye det samme som etter dagens lovgivning, men flere eksempler gjør at enkelte tvilstilfeller (f.eks. dynamiske IP-addresser som relaterer seg til en bruker) nå er klart innenfor.**

Teknisk mer detaljert PO-definisjon enn nå - metadata

- **Utdypes i fortalen - metadata:**

- **Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tag**

Når er noe identifiserbart?

- **To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by any other person to identify the individual directly or indirectly**

- **To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development (26)**

Konsekvens

- **Rom for å forstå mange typer data og metadata som personopplysning**
- **Gir regelverket stor anvendelse**
- **Feiloppfatning av hva som er «personopplysning» kan bli dyrt**
- **Sørg for å ha god dokumentasjon om vurderinger som er gjort**

FØYEN TORKILDSEN

GDPR – generelle endringer

Forsvinner all Datatilsynets forhåndskontroll?

Ja og nei.

I hovedsak blir det etterfølgende kontroll. *Det betyr..*

…at brukerne av lovverket overtar en del av datatilsynets nåværende oppgaver

FØYEN TORKILDSEN

Sentrale endringer

- Den registrerte kan «restrict» behandlingsansvarliges rett til å behandle data når dataenes korrekthet bestrides i en periode inntil korrektheten verifiseres (ny art 17a)

- Plikt til å informere mottakere av informasjon når den registrerte krever data rettet/slettet og krever at mottakere av opplysningene får vite dette (ny art 17b)

Portabilitet – viktig å regulere for databehandlere

- Datasubjektet har rett å få overført dataene fra den behandlingsansvarlige slik at vedkommende kan overføre dataene til en annen behandlingsansvarlig.
- Vilkår
  - Data som er levert av datasubjektet
  - Basert
  - på samtykke fra eller
  - avtale med datasubjektet
  - Elektronisk behandling
- Unntak i forhold til myndighetsutøvelse fra offentlig myndighet osv,

FØYEN TORKILDSEN

GDPR – internkontroll

Iverksetting av tiltak

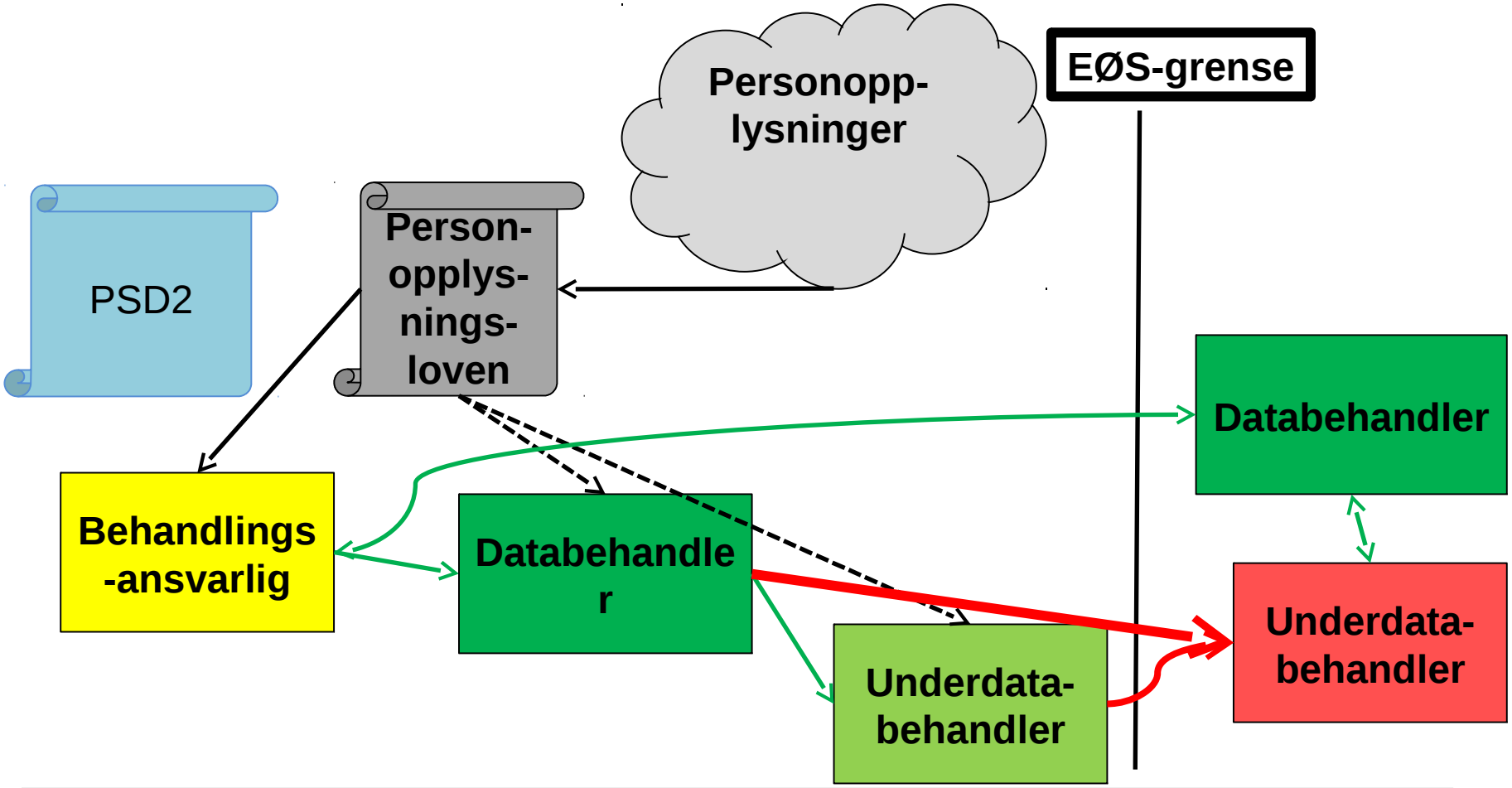
- Risikovurdering et must – sikringstiltak skal stå i forhold til eksisterende risiki
  - Risikovurderingen må dokumenteres
- Kryptering et vesentlig virkemiddel for å sikre informasjonssikkerhet, i mange tilfeller påkrevet
  - **Krypterte personopplysninger er likevel personopplysninger!**
  - Lovens øvrige krav gjelder derfor fortsatt
- Sikkerhetslogging av brukeres aktivitet etc. kun så langt som «strictly neccesary and proportionate».
  - Loggene kan typisk ikke brukes til andre formål, f.eks. kontroll med ansatte.

I praksis – følgende skal være på plass allerede nå

- Beskrivelse av informasjonssystemet og dataene som lagres der
- Oversikt over i hvilke land data lagres
- Oversikt over fra hvilke land servicepersonell kan aksessere data
- Definerte sikkerhetsmål
- Sikkerhetsstrategi
- Gjennomført risikovurdering
- Organisasjonskart over ansvar og myndighet om informasjonssikkerhet og drift

Personopplysningsloven - Roller og modellavtaler

-når virker avtalene og når virker de ikke.



FØYEN TORKILDSEN

Store endringer i finansbransjen

Bruk av skytjenester – En viktig del av fremtiden

- **Finansbransjen er vant til store IT-prosjekter med høye investeringer, lang levetid, lav fleksibilitet og tungt vedlikehold.**
- **Utvikling innen betalingsformidling og disruptive teknologier, samt mobilteknologi og sosiale medier endrer adferd hos bankkundene.**
- **Danner grunnlaget for store endringer i finansbransjen med økende behov for større dynamikk i IT-plattformene.**
- **Skytjenester utvikles i ekspressfart på basis av spesielt sosiale medier, netthandel og spill.**

- Arve Føyen

- Mobil: +47 918 199 62
- E-post: af@foyentorkildsen.no