INFORMASJONSSIKKERHET & GDPR

Kundeforum 18.oktober

Direktoratet for økonomistyring

Den nye personvernforordningen
GDPR (General Data Protection Regulation)


Official Journal
of the European Union
L 119
Legislation
Volume 59
4 May 2016
English edition
Contents
1 Legislative acts
REGULATIONS
• Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (1) 1
DIRECTIVES
• Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA 89
• Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime 132
(1) Text with EEA relevance
Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.
The titles of all other acts are printed in bold type and preceded by an asterisk.
EN

Hvem gjelder den for?

Lovverket gjelder for alle EU- og EØS-land og alle bransjer samt alle aktører som behandler persondata som tilhører innbyggere i EU- og EØS-land

Hvilke data gjelder den for?

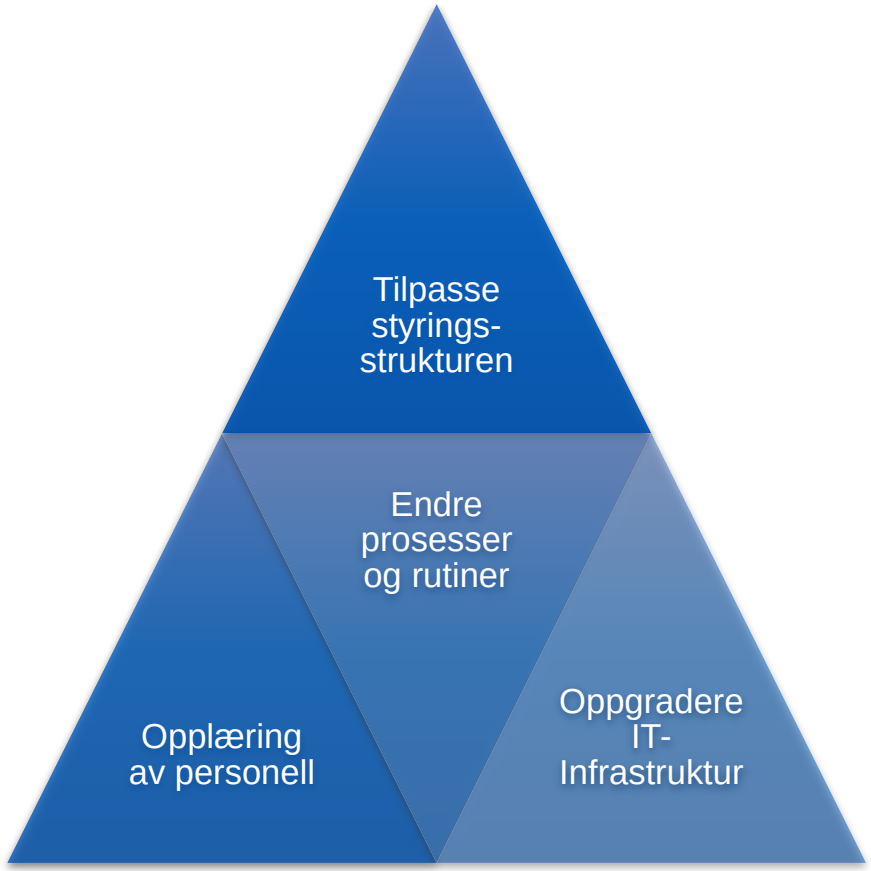
- Personopplysninger
- Atferdsmønstre
- Sensitive data

Eksempler på områder som blir påvirket

- Teknologi
- Prosesser
- Rutiner
- Styringsstruktur

Direktoratet for økonomistyring

GDPR Fokusområder



Fokusområder – eksempler:

- **Tilpasse styringsstrukturen**

  Klargjøre ansvarsfordelingen mellom kundene og DFØ i forvaltningen av personopplysninger

- **Opplæring av personell**

  Utføre tilpasset opplæring og kompetanseheving for å forvalte og prosessere persondata

- **Endre prosesser og rutiner**

  Utføre nødvendige endringer i innsamling, bruk, lagring og sletting av samtykker og persondata

- **Oppgradere IT-infrastruktur**

  Avdekke nødvendige tiltak for å oppgradere IT-infrastrukturen. Understøtte nødvendige endringer i prosesser og rutiner for å imøtekomme nye og skjerpende krav

Om Informasjonssikkerhet i GDPR-forordningen

Prinsipper for behandling av personopplysninger

«Personopplysninger skal behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak»

*- **GDPR** - Artikkel 5, bokstav f.*

Personopplysningssikkerhet

«.. den behandlingsansvarlige og databehandleren (skal) gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen»

*- **GDPR** - Artikkel 32*

Direktoratet for økonomistyring

Behandlingsansvarlig & Databehandler

«Personvernforordningen skiller mellom begrepene behandlingsansvarlig og databehandler. Den behandlingsansvarlige bestemmer over personopplysningene, mens databehandleren opptrer på vegne av den behandlingsansvarlige. Databehandleren kan derfor bare behandle personopplysninger etter instruks fra den behandlingsansvarlige.»

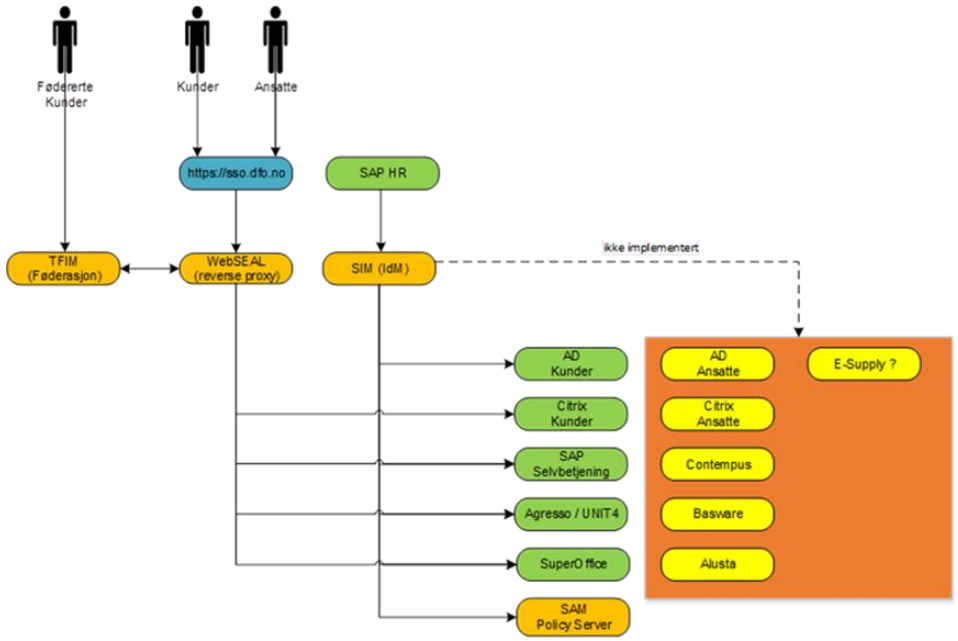
- Datatilsynet

Direktoratet for økonomistyring

Utvalgte tiltak for å sikre personopplysningene

- Begrense tilgang til personopplysninger til tjenstlige behov
- Begrense overføring, behandling og innsyn av personopplysninger (dataminimalisering)
- Benytte kunstige personopplysninger (syntetiske data) i test
- Rutiner for å slette personopplysninger vi ikke har hjemmel for å oppbevare
- Vurdere personvernkonsekvenser ved større endringer av prosesser eller innføring av nye IT-systemer
- Oppdatert personvernerklæring og mulighet til å reservere seg mot tilbud om kurs og seminarer

Tilgangsstyring



- Det er et behov for å begrense innsyn i personopplysninger
- Vi jobber derfor med å begrense / tilpasse tilganger for DFØ sine ansatte i henhold til tjenstlige behov
- Omfanget inkluderer hele systemporteføljen til DFØ
- Det er et særskilt fokus på SuperOffice

Direktoratet for økonomistyring

Hva som er utført i GDPR-prosjektet så langt

- **Databehandleravtale**
  - ny databehandleravtale med kundene
  - oppdaterte databehandleravtaler med leverandører
- **Besluttet**
  - opprettelse av personvernombud
  - innføre syntetiske testdata for utvikling og test
  - tilpasse tilganger til tjenstlige behov

- **Kommunikasjon**
  - kundenotater om GDPR
  - intern kommunikasjon og opplæring
- **Dokumentasjon**
  - vurderinger av behandlingsformål og behandlingsgrunnlag som grunnlag for databehandleravtaler
  - forvaltning av personopplysninger i tjenesteproduksjonen
  - oppdatert personvernerklæring
  - avklaringer med Finansdepartementet, Datatilsynet, kunder og Arkivverket
  - vurdering av personvernkonsekvenser (DPIA) ved endringer i tjenesteproduksjonen

Direktoratet for økonomistyring

Personvernombudet sine oppgaver

Informere og gi råd

Kontrollere og sikre etterlevelse av personvernregelverket

Gi råd om vurdering av personvernkonsekvenser (DPIA) og kontrollere gjennomføringen

Samarbeide med Datatilsynet og være et kontaktpunkt

Oversikt over behandling av personopplysninger

Direktoratet for økonomistyring