Skatteetaten

Skatteetatens prosjekt personvernforordningen
Personvern i samarbeid med våre leverandører, hvem gjør hva?

DFØ kundeforum 2018

Kristin Lyng

18. Oktober 2018

Agenda

1. Om Skatteetaten og vårt GDPR-prosjekt
2. Om databehandler og behandlingsansvarlig
3. Om databehandleravtaler

Stort omfang av personopplysninger

Registrerte

- 6500 medarbeidere
- 7 millioner registrerte i Folkeregisteret
- 3,8 millioner registrerte skattepliktige

Datamengde (eksempler)

- 4,4 millioner skattemeldinger
- 3,8 millioner skattetrekksmeldinger (skattekort)
- 44 millioner innrapporteringer av grunnlagsdata
- Ca. 300 IT-system, både på modernisert og ikke-modernisert plattform

Innhenting og utlevering av data

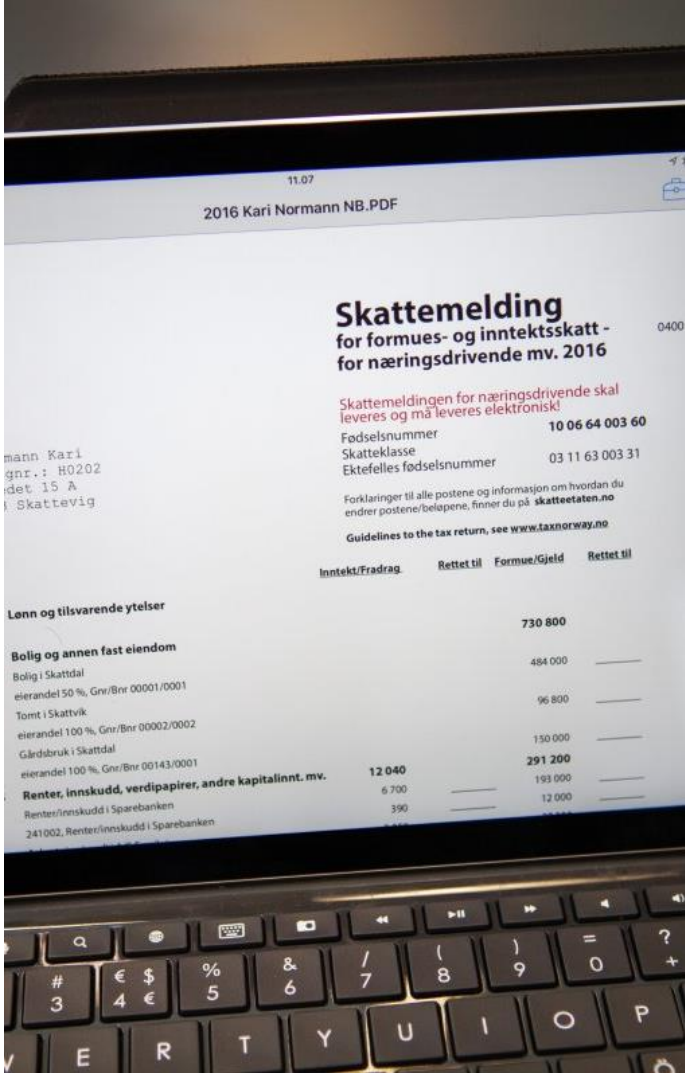
- Nye teknologiske muligheter gjør at stadig flere avgir data til Skatteetaten eller mottar data fra Skatteetaten

Samtykkeløsning

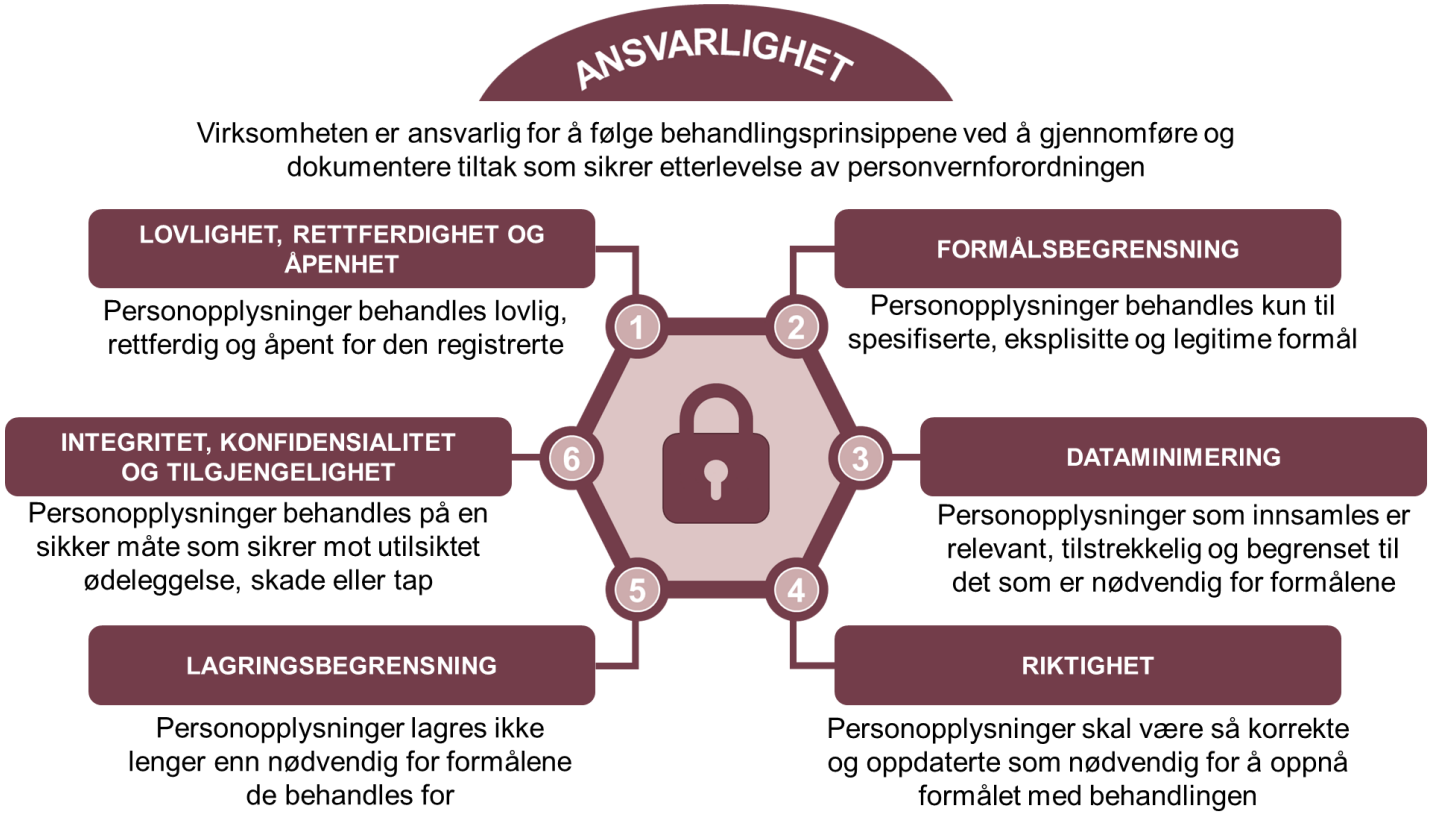
- 125.000 samtykker er gitt via samtykkeløsningen med bankene

Utvikling

- 900.000 timer utvikling årlig



Prinsipper for behandling av personopplysninger art. 5



Personvernkrav (PVK)

- Skatteetaten har valgt å tolke regelverket om til konkrete personvernkrav
- Etaten vil fremover ha fokus på ivaretagelse av innebygd personvern i løsninger som anskaffes

Krav nr	Beskrivelse
PVK-01	Behandlingsgrunnlag og formålsbegrensning
PVK-02	Innsyn for de registrerte
PVK-04	Opplysningsplikt og Personvernerklæring
PVK-06	Sporbarhet (auditlogging)
PVK-07-01	Behandlingsprotokoll
PVK-08	Dataminimering
PVK-10	Riktighet – identifisering og retting av feil
PVK-11	Varsling av eksterne mottakere av personopplysninger ved feil
PVK-12	Lagringsbegrensning - sletting
PVK-13-01	Personvernretningslinjer
PVK-15-01	Personvernkonsekvensvurdering (DPIA)
PVK-15-02	Forhåndsdrøftelser – Datatilsynet
PVK-17	Sikkerhet - Integritet, konfidensialitet, tilgjengelighet
PVK-18	Automatiske individuelle beslutninger
PVK-19	Rutiner for håndtering av personvernavvik
PVK-20	Geografiske begrensninger
PVK-21-01	Innebygget personvern og personvern som standard innstilling

Faseinndeling prosjekt personvernforordningen

01.07.2017 — 30.11.2017 — 30.06.2018 — 30.04.2019

Fase 0

- Tolkning av regelverket
- **Kartlegge behov for databehandleravtaler**
- Kartlegge manglende etterlevelse (gap-analyse)
- Interessentanalyse
- Plan og estimat fase 1
- Etablert tverretatlig samarbeid Personvernforum

Fase 1

- **Inngå og revidere databehandleravtaler**
- Opplæringstiltak
- Kommunikasjonstiltak (personvernerklæring mv)
- Vurdering og dokumentasjon av personvernrisiko
- Endring av metodikk og retningslinjer
- Personvernombud på plass
- Plan og estimat for fase 2

Fase 2

- Utarbeide retningslinjer for å ivareta personvern i prosesser, systemer **og i anskaffelser**
- Utarbeide protokoller over behandling av personopplysninger
- Utarbeide vurderinger av personvernkonsekvenser (DPIA)
- **Inngå gjenstående databehandleravtaler**
- Gjennomføre innføringstiltak
- Utrede behov for systemendringer

Databehandler og behandlingsansvarlig i GDPR art. 4

Behandlingsansvarlig, art. 4 nr. 7

En fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes […]

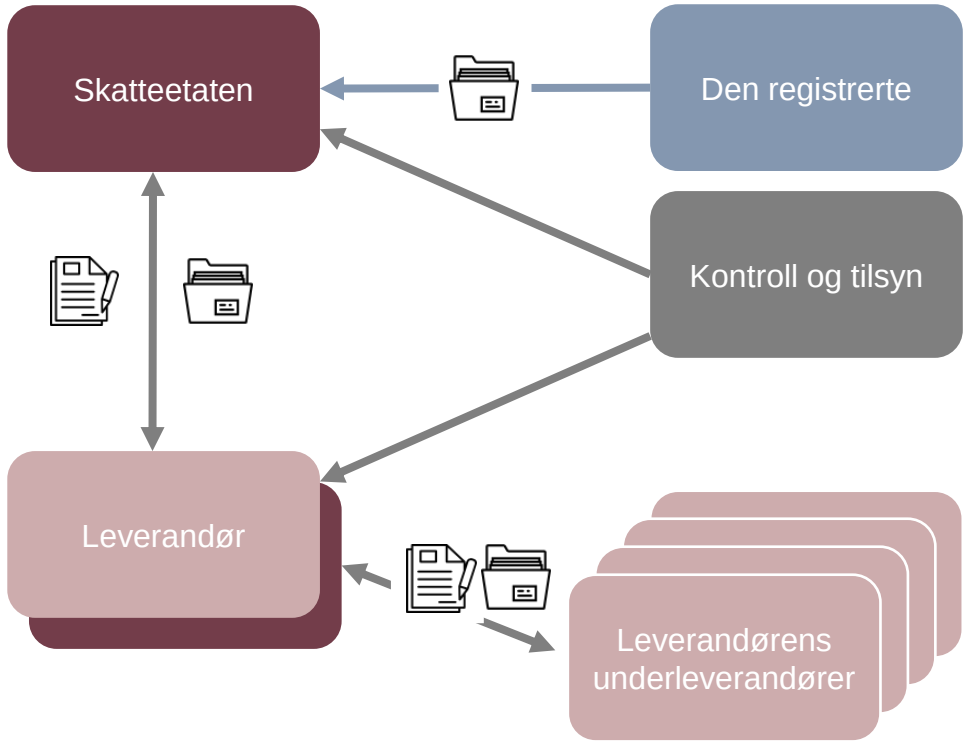
Databehandler, art. 4 nr. 8

En fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert organ som behandler personopplysninger på vegne av den behandlingsansvarlige.

- Hvis vilkårene i definisjonene oppfylles, forutsettes det i art. 28 at behandlingsansvarlig og databehandler avtaleregulerer forholdet
- Behandlingsansvarlig kan bare velge en databehandler som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer etterlevelse av forordningen

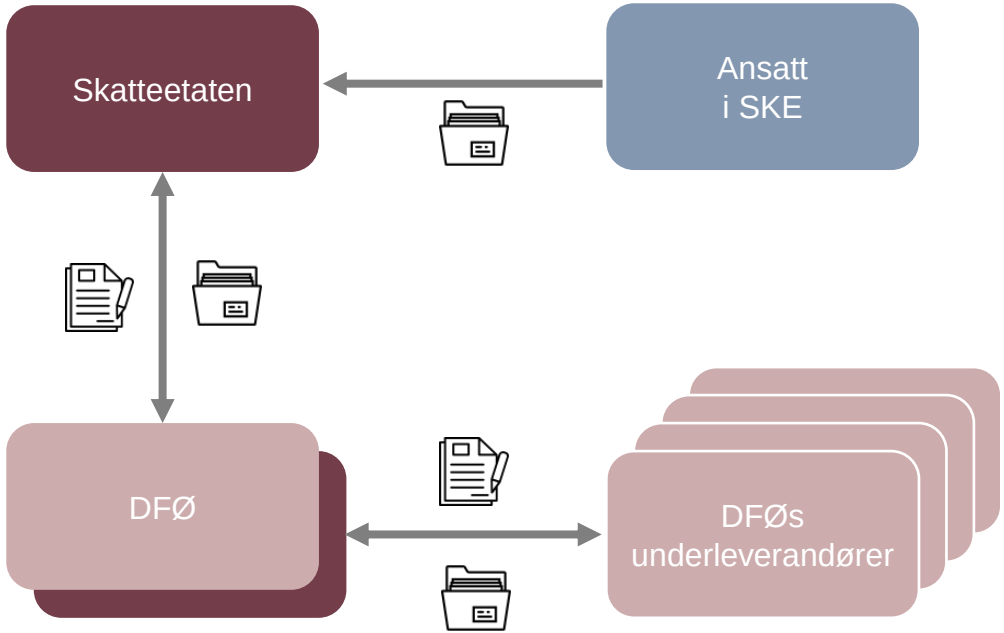
Fra leverandørstyring til samarbeid

- Behandlingsansvarlig
- Databehandler
- Personopplysninger
- Kontraktsforvaltning av kommersiell leveranse, herunder databehandleravtale



Enkelt: DFØ som databehandler

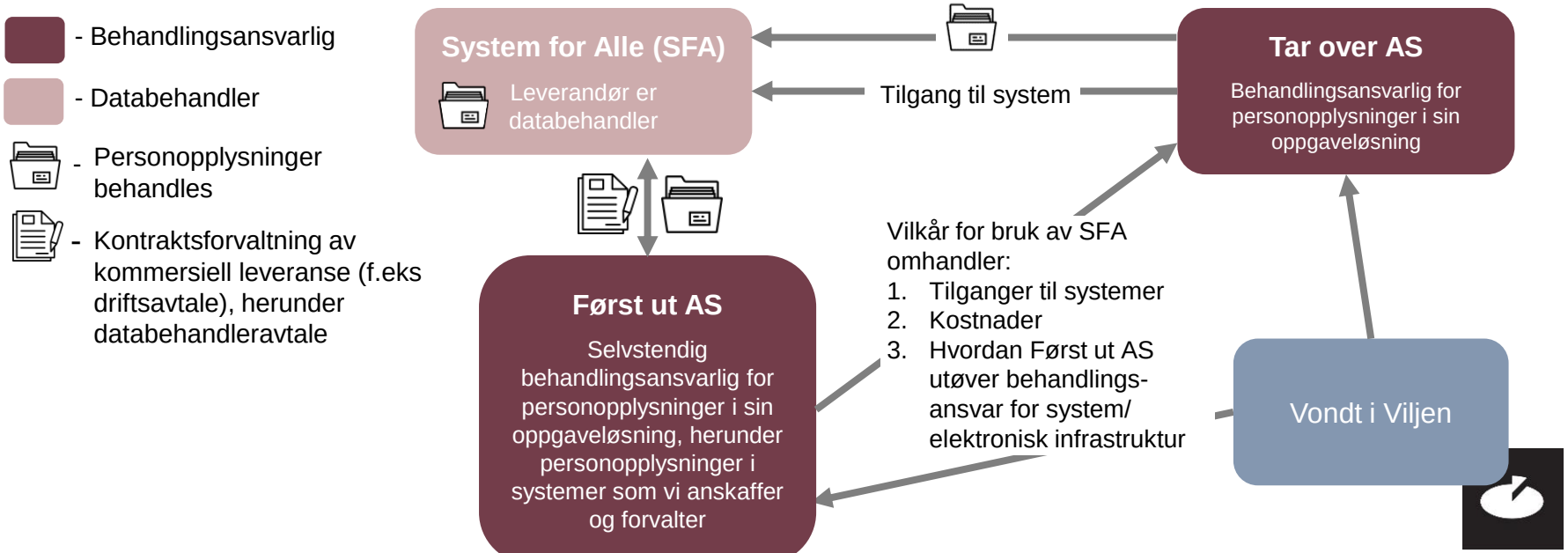
- Behandlingsansvarlig
- Databehandler
- Kontraktsforvaltning av leveranse, herunder databehandleravtale



Litt mer komplisert: Selvstendig behandlingsansvar eller felles behandlingsansvar?

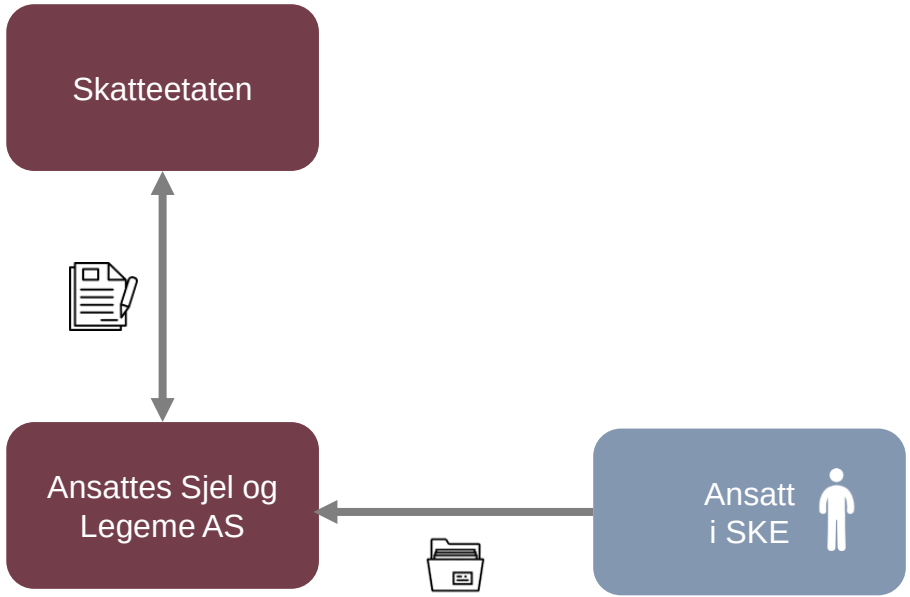
Tar over AS har spesifikke lovpålagte oppgaver som etter sin art er forskjellig fra Først ut AS sine oppgaver. Tar over AS har dermed et selvstendig behandlingsansvar for de personopplysninger de behandler for sin oppgaveløsning. Tar over AS sørger for å utøve sitt ansvar på ulike måter, f.eks å sørge for å følge opp arbeidsgiveransvaret overfor sine medarbeidere når de behandler personopplysninger.

Her har man ikke et felles behandlingsansvar for personopplysninger.



Enkelt, men komplisert: leverandøren har selvstendig behandlingsansvar

- Behandlingsansvarlig
- Registrert
- Personopplysninger
- Kommersiell leveranse utkontraktert tjeneste



Krav til databehandleravtalen art. 28

- Behandlingsansvarlig kan bare velge en databehandler som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer etterlevelse av forordningen
- Art. 28 (3) a-h angir minstekrav for hva som skal stå i avtalen, det er ikke godt nok å basere seg på Datatilsynets gamle malverk

a) behandler personopplysningene bare på dokumenterte instrukser fra den behandlingsansvarlige, herunder med hensyn til overføring av personopplysninger til en tredjestat eller en internasjonal organisasjon, med mindre det kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt; i så fall skal databehandleren underrette den behandlingsansvarlige om nevnte rettslige krav før behandlingen, men mindre denne rett av hensyn til viktige samfunnsinteresser forbyr en slik underretning,

b) sikrer at personer som er autorisert til å behandle personopplysningene, har forpliktet seg til å behandle opplysningene fortrolig eller er underlagt en egnet lovfestet taushetsplikt,

c) treffer alle tiltak som er nødvendig i henhold til artikkel 32,

d) overholder vilkårene nevnt i nr. 2 og 4 når det gjelder å engasjere en annen databehandler,

e) idet det tas hensyn til behandlingens art og i den grad det er mulig, bistår, ved hjelp av egnede tekniske og organisatoriske tiltak, den behandlingsansvarlige med å oppfylle vedkommendes plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i kapittel III,

f) bistår den behandlingsansvarlige med å sikre overholdelse av forpliktelsene i henhold til artikkel 32–36, idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for databehandleren

g) etter den behandlingsansvarliges valg, sletter eller tilbakeleverer alle personopplysninger til den behandlingsansvarlige etter at tjenestene knyttet til behandlingen er levert, og sletter eksisterende kopier, med mindre unionsretten eller medlemsstatenes nasjonale rett krever at personopplysningene lagres

h) gjør tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i denne artikkel er oppfylt, samt muliggjør og bidrar til revisjoner, herunder inspeksjoner, som gjennomføres av den behandlingsansvarlige eller en annen inspektør på fullmakt fra den behandlingsansvarlige.

Punktene a-h i forordningen betyr

a) Behandlingsansvarliges instruks om behandlingen

b) Taushetsplikt

c) Krav om å treffe tiltak for «sikkerhet ved behandlingen» (art. 32)

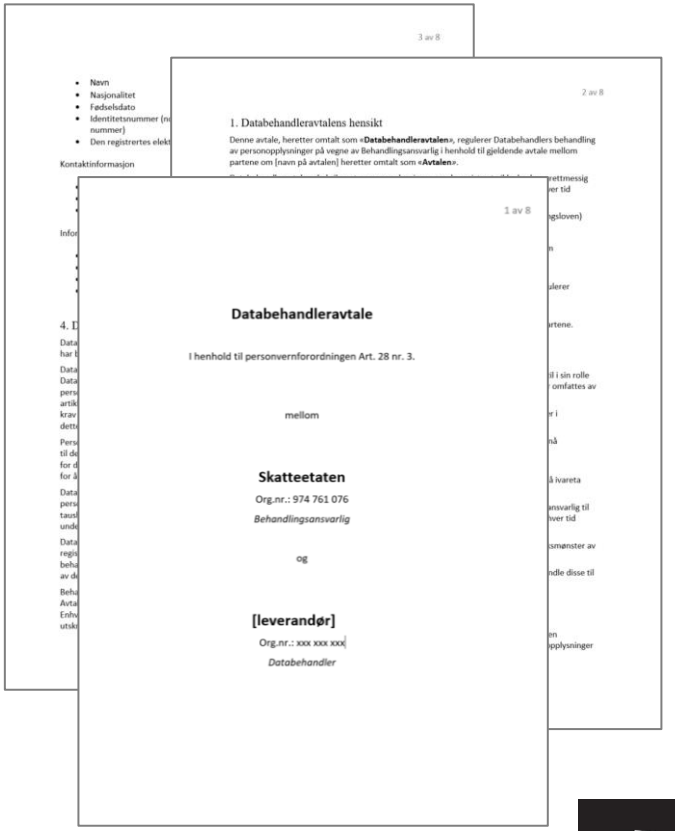
d) Vilkår for bruk av underdatabehandler

e) Bistand til behandlingsansvarlig (når rettighetene til den registrerte blir utøvd)

f) Bistand til behandlingsansvarlig (med å overholde egne forpliktelser)

g) Sletting og tilbakelevering av personopplysninger

h) Fasilitere for revisjon og inspeksjon



Vår angrepsmetode – brukes konkret for hver avtale

Tre spørsmål vi har stilt oss selv:

1	Hvem er behandlingsansvarlig?	Kartlegge ansvarsforhold i lys av oppgaveløsningen
2	Hva er rammene for behandlingen av opplysningene?	Avtalen skal sette en klar ramme, da må vi vite hva databehandler skal levere
3	Hvor omfangsrik, inngripende eller risikofylt er behandlingen av personopplysninger i mitt avtaleforhold?	Svaret du får gir deg holdepunkter for hvor detaljert databehandleravtalen må være

Noen eksempler på leverandører som er databehandlere…

IT-drift

Flyttebyrå

Kølappsystem

Kameraovervåkning

Print

Kantinen

Spørreverktøy

Kundesenter

Rekruttering

Coach

Og mange flere..

…og nå skal vi klare å finne ut av spørsmålet: *hvem gjør hva*?

1. Behandlingsansvarlig

- ..har ansvaret for å velge en databehandler (leverandør) som etterlever forordningen, behandlingsansvarlig må vurdere konkret hvilke tiltak leverandøren har for etterlevelse av personvernforordningen.
- Utarbeider instrukser for behandlingen
- Gir tillatelse til bruk av underdatabehandler
- Varsler tilsynsmyndigheter, etter avtalte rutiner

….følger opp at forpliktelsene overholdes i samarbeid med databehandler

2. Databehandler

Databehandler har **plikt til å bistå behandlingsansvarlig i spørsmål om behandlingssikkerhet** (art. 32 – 34)

Databehandleravtalen skal beskrive hvilke ***tiltak*** databehandler skal ha som er nødvendige i henhold til art 32 om **behandlingssikkerhet**

Videre skal databehandler sørge for at **underdatabehandler** etterlever regelverket og sikre at sitt eget **personell** er autorisert

Databehandleravtalen bør beskrive hvordan databehandler skal bistå behandlingsansvarllg med å oppfylle pliktene til å svare den registrerte som ønsker å utøve rettigheter som er fastsatt i forordningens kap. III:

- innsynsrett (art. 15)
- rett til korrigering (art. 16)
- sletting (art. 17)
- begrensning av behandling (art. 18)
- dataportabilitet (art. 20)
- innsigelsesrett (art.21)
- rett til ikke å være gjenstand for helt automatiserte avgjørelser (art. 22)

Databehandler skal slette eller tilbakelevere alle personopplysninger til behandlingsansvarlig etter at tjenestene knyttet til behandlingen er levert, og slette eksisterende kopier

Databehandler skal gjøre tilgjengelig for behandlingsansvarlig all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i artikkel 28 er oppfylt (jf. krav til protokoll i art. 30(2))

Hva stilles det spørsmål om?

Takk for henvendelsen, men vi er ikke databehandler!

Kan vi avtale delt behandlingsansvar?

Hvem eier dataene?

Hva er bransjestandarden?

Vi tilbyr ønsket sikkerhetsnivå, men dere må betale ekstra

Vi tar ansvaret, men dere må bære risikoen for at vi er databehandler

Hvordan operasjonalisere kravene i en anskaffelse?

- Dekode og tilpasse personverkravene i nytt regelverk til din virksomhet. Standardiser så langt det går.
- Hvilke krav dekkes av databehandleravtalen du utarbeider og hvilke skal du stille eksplisitt i kravspesifikasjonen?
- Hvordan skal forpliktelsene følges opp i samarbeid med *dine* leverandører?

Skatteetaten

SPØRSMÅL

TAKK FOR MEG

Ta kontakt dersom du ønsker å få tilsendt Skatteetatens mal for databehandleravtale

Kristin Lyng
Kategorileder IT / Delprosjektleder avtaler GDPR
kristin.lyng@skatteetaten.no