



# REFERAT FRA MØTE I COMPLIANCEFORUM

---

Dato: 17.9.2019  
Sted: Ruter, Dronningens gate 40, Oslo  
Tid: Kl. 10.00 - 15.00

## TILSTEDE:

Terje Øen, Gunn Sissel Brasetvik og Beate Borrevik (Kolumbus), Svend Erik Wandaas (Ruter), Bjørn Erik Lunde (Skyss), Kristin Løining Kjeldsen (AKT), Kristin Fredriksen (VKT) og Line Holmesland (AtB)

Sekretariat: Reidun Kvitberg Eckhoff

## PROGRAM:

### VELKOMMEN V/ TERJE ØEN

### DILEMMATRENING

Terje presenterte to dilemmaer som ble diskutert i grupper, deretter diskutert i plenum.

Tilbakemeldinger på det første dilemmaet:

- En ren IT-sak
- Ikke greit å gi fra seg passordet, selv om sjefen sier det

Dilemma 2:

- Tydelige grenser på at dette ikke er greit



## OPPFØLGING AV LEVERANDØRER PÅ ETISKE RETNINGSLINJER I HELE LEVERANDØRKJEDEN

- **Handlingsregler for Ruters leverandører v/ Svend Erik Wandaas**

Temaet tatt opp i presentasjon Complianceforum 17 september SW

- **System for kontroll av leverandørene v/ Factlines v/ daglig leder Siri Engesæth**

Presentasjon 2019\_Kollektivtrafikkforeningen\_SiE sammen med et produktark og en eksempelrapport

## DATABEHANDLERAVTALER OG OPPFØLGING AV (UNDER)LEVERANDØRER PÅ GDPR

Presentasjon v/ Svend Erik Wandaas supplert av Line Holmesland fra AtB.

Temaet tatt opp i presentasjon Complianceforum 17 september SW

I GDPR er det flere steder henvist til den registrertes grunnleggende rettigheter og friheter. Dette omfatter ikke bare personvern hensyn (selv om det er det mest sentrale), men skal også sikre at Forbrukerrettigheter blir ivaretatt på en god måte

Dersom en leverandør får en underleverandør utenfor EU kan dette ikke aksepteres. Hvordan kan dette løses? Ruter anbefaler å bruke innkjøpsmakt ved å nekte å underskrive kontrakten og bruke egne databehandleravtaler. Man bør utfordre leverandøren på hva de er uenige i, ikke akseptere leverandørens unnskyldninger og heller stoppe avtalen selv om det er upopulært

Skoleskyss problematikken ble tatt opp og hvordan man bør forholde seg til GDPR og håndtering av dataopplysninger. Her finnes det ikke et klart svar. Det bør tas opp med Datatilsynet.

Sekretariatet opplyser om at Skoleskyssforum utarbeider et eget dokument. Complianceforum vil gjerne bidra til dette arbeidet.



## STATUS BRUDD PÅ GDPR

Presentasjon v/ Svend

Temaet tatt opp i presentasjon Complianceforum 17 september SW

Brudd på GDPR gjelder ofte økonomiske saker og straffes med bøter.

Ansvar for lukkede grupper på Facebook - AtB v/ Line Holmesland

Hvilket ansvar har AtB for ytringer på Facebook? Felles behandlingsansvar ble konklusjonen. Dermed har AtB et ansvar for personopplysninger som blir lagt ut av andre på AtBs Facebook sider for eksempel kommentarer om sjåførere og krenkede ytringer. AtB har vurdert å stenge kommentarfeltet når det ikke kan redigeres, på tider kundesenteret er stengt. Bør man stenge kommentarfeltet utenom åpningstidene?

Andre eksempler: Bilde av sjåfør som snakket i telefonen ble lagt ut på nettsiden til Kolumbus. Kolumbus slettet informasjonen på egne sider, men bilde var allerede delt videre.

AtB sletter bilder så fort noen oppdager overtramp, men dersom noen legger ut på natta, blir det umulig å følge opp med en gang. Da må kommentarfeltet stenges utenom åpningstider til kundesenteret. VG og Dagbladet gjør det. Ruter har det åpent, men stenger en periode dersom de har fjernet mange innlegg.

Det kommer en ny lov om redaktøransvar. Denne omhandler mest kommentarfelt i aviser, men er også relevant for kollektivtrafikk og fylkesadministrative selskaper.

En mulig løsning kan være å utvikle egne tjenester enn å bruke Facebook og andre tilsvarende steder.



## RUNDE RUNDT BORDET

### Spørsmål til runden:

- Status GDPR og relevante problemstillinger
- Databehandleravtaler, hvordan følge opp disse avtalene
- Status varslingsrutiner for underleverandører

### **AKT:**

Arbeid med Protokollen er viktig. Skoleskyss har vært mye arbeid med et gammelt system. Nye DPIAer og mange hindringer, særlig tilgang til Folkeregisteret. Databehandleravtaler blir neste gjennomgang.

### **Kolumbus:**

Flere nye Personvernombud hos Kolumbus. Databehandleravtaler gjennomgått og ordnet det som manglet. Det gjennomført en kartlegging og pågår et kontinuerlig arbeid for å avdekke feil og mangler. Arbeidsmetodikken er å tilegne ny kunnskap og deretter gå tilbake å korrigere. Et eksempel er personvernerklæringer, som er vanskelig få oversikt på.

### **Skyss:**

Styringsdokumenter er på plass. Det pågår en omorganisering og ansvaret for personvern skal ligge i en stabsenhet. utfordringen er at når man sender rundt jevnlig forespørsler om personvern er det kun 1/3 som svarer. Det er derfor behov for å få en dedikert person som overtar ansvaret.



### **AtB:**

Startet for et par år siden med å kartlegge behandlinger. Det ble lagd en rapport med anbefalinger til videre arbeid. Ny kvalitetsansvarlig begynte i august og har begynt å se på styrende dokumenter. Å lage databehandleravtaler er viktig, men oppfølging må også ivaretas. Den øverste ledelsen tar ansvar for behandlingsansvarlig. Personvernombudet skal ikke ta dette ansvaret. Kluge overtok ansvaret for å følge opp inntil kvalitetsrådgiver startet.

### **VKT:**

Skoleskyss er ikke helt i mål med GDPR. Rutinene er der, men er ikke skrevet ned. Kommer hele tiden nye ting å tenke på og man må passe på å følge opp. Et eksempel er et krav om innsyn. En far ønsket å vite om bruk av skolekortet for å måle avstand fra fars bosted til skolen.

Hvordan kan man samle erfaringer og dele disse slik at man kan samarbeide om løsninger som kan brukes over hele landet? Skyss har hatt inne et konsulentselskap. Der det finnes ulike rutiner på ulike områder som man kan dele. Et dokumentdelingssystem - ala Teams til Microsoft eller One Note er etterspurt. Teams er bedre egnet som et bibliotek og fildelingssystem. Workplace og Facebook er ikke til å stole på.

### **Ruter:**

Ruter har blitt meldt til Datatilsynet om et billettsystem, men ble avvist. Å drive framtiden mobilitets tjenesteår er krevende. Opplæring er viktig og det behov for en opprydding. Ruter utvider stadig og blir større. Målsetningen er at Ruter skal gå framover, men innenfor regelverket og med fokus på informasjonssikkerhet. Det skal ansettes en Sisu - informasjonssikkerhetsansvarlig.

Man bør vurdere å erstatte Workplace med Teams.



## AVSLUTNING OG VEIEN VIDERE V/TERJE ØEN

- **Tidspunkt for vårmøtet**  
Foreløpig ikke bestemt et tidspunkt
- **Frekvens på møtene framover**  
Dersom man kunne få på plass et nytt system blir arbeidet mellom møtene vel så viktig. Da holder det med møte en gang i året
- **Forslag til temaer for neste møte fra forumets medlemmer?**
  - Et felles sted å diskutere og dele informasjon. Et juridisk forum, men ikke bare for jurister. En type forslagskasse. Sekretariatet foreslår Workplace, men Complianceforum ønsker ikke å bruke det. Tilliten til Facebook er ganske lav
  - Eksterne varslingsrutiner. Dersom en sjåfør ønsker å si fra - hvordan håndteres det?
  - Universell utforming i IT-løsninger. Det er krav om nye strenge løsninger, også i interne løsninger. Ved innføring av nytt intranett er man omfattet av nytt regelverk eller ved vesentlige oppgraderinger. Mange Compliance-utfordringer i regelverket, eksempelvis WCAG-kravet
  - Ny arkivlov, spesielt endringer som omfatter personvern. Flere blir omfattet av arkivloven og får ikke dokumentert virksomheten fordi man ikke har gode lagringsalternativer