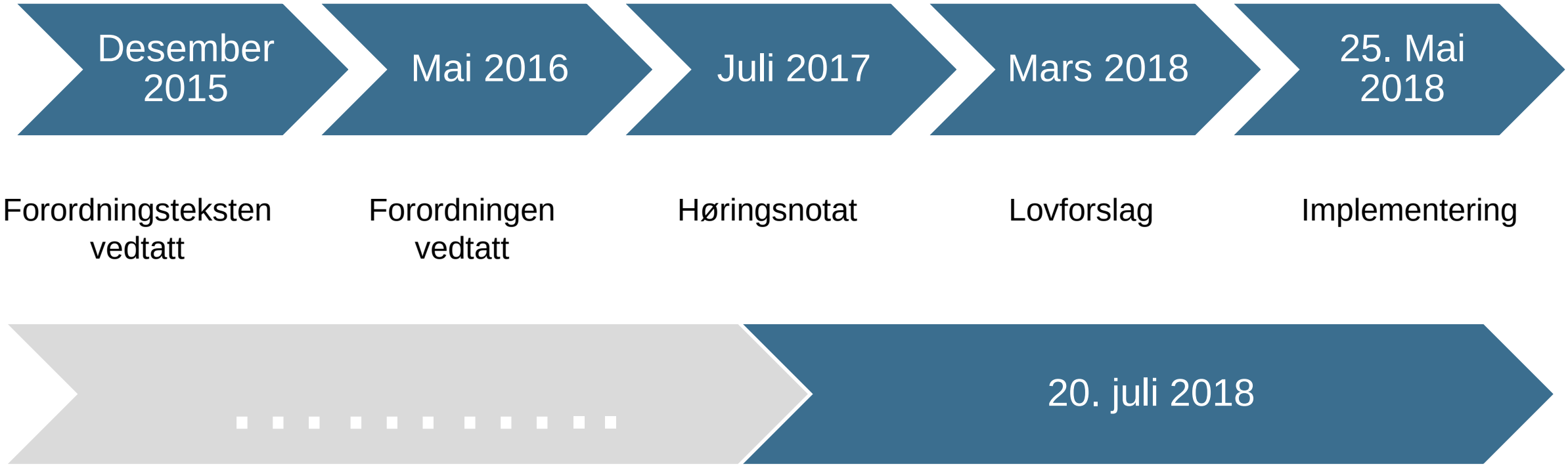
Personvernforordningen

Complianceseminaret

Advokat Nils Henrik Heen

Finans Norge

Personvernforordningen



Grunnleggende begreper

- Personopplysning
  - «normal»
  - «spesielle kategorier av…»
- Den registrerte
- Behandling
- Behandlingsansvarlig
- Databehandler
- Tredjeland

Personvernforordningen

- Teknologisk utvikling
- Internasjonalisering
- Godt personvern

Problemene

- Rot med begreper
- Tvetydige begrep
- Uklare intensjoner
- Manglende harmonisering
- Rettskilder

Oppfyllelse er ikke bare compliance

- God kontroll
- God kundetilfredshet
- God vekst

Avvikshåndtering – dagens regelverk

- Når det har skjedd en uautorisert utlevering av personopplysninger som krever konfidensialitet.
- «Så snart som mulig etter at avviket er oppdaget»
- Ingen uttrykkelig krav om varsling av berørte.

Avvikshåndtering – personvernforordningen

- Varslingsrett når det har skjedd sletting, endring og tap av personopplysninger med mindre det er usannsynlig at bruddet innebærer en risiko.
- Utvidet undersøkelsesplikt

- Uten unødig forsinkelse og senest innen 72 timer fra man blir oppmerksom på avviket.
- Varslingsplikt selv om man ikke er ferdig med intern granskning.
- Krav til avviksrapporten.
- Krav til dokumentasjon.

Avvikshåndtering - personvernforordningen

- Varslingsplikt til de registrerte dersom det er sannsynlig at bruddet innebærer en høy risiko for fysiske personers rettigheter og friheter (uten unødig forsinkelse)
- Manglende etterlevelse kan utløse sanksjoner og de registrerte kan kreve erstatning.

Avvikshåndtering – betydning for dere

- Rutiner for å avdekke avvik.
- Rutiner for varsling av avvik.
- Konsekvenser?

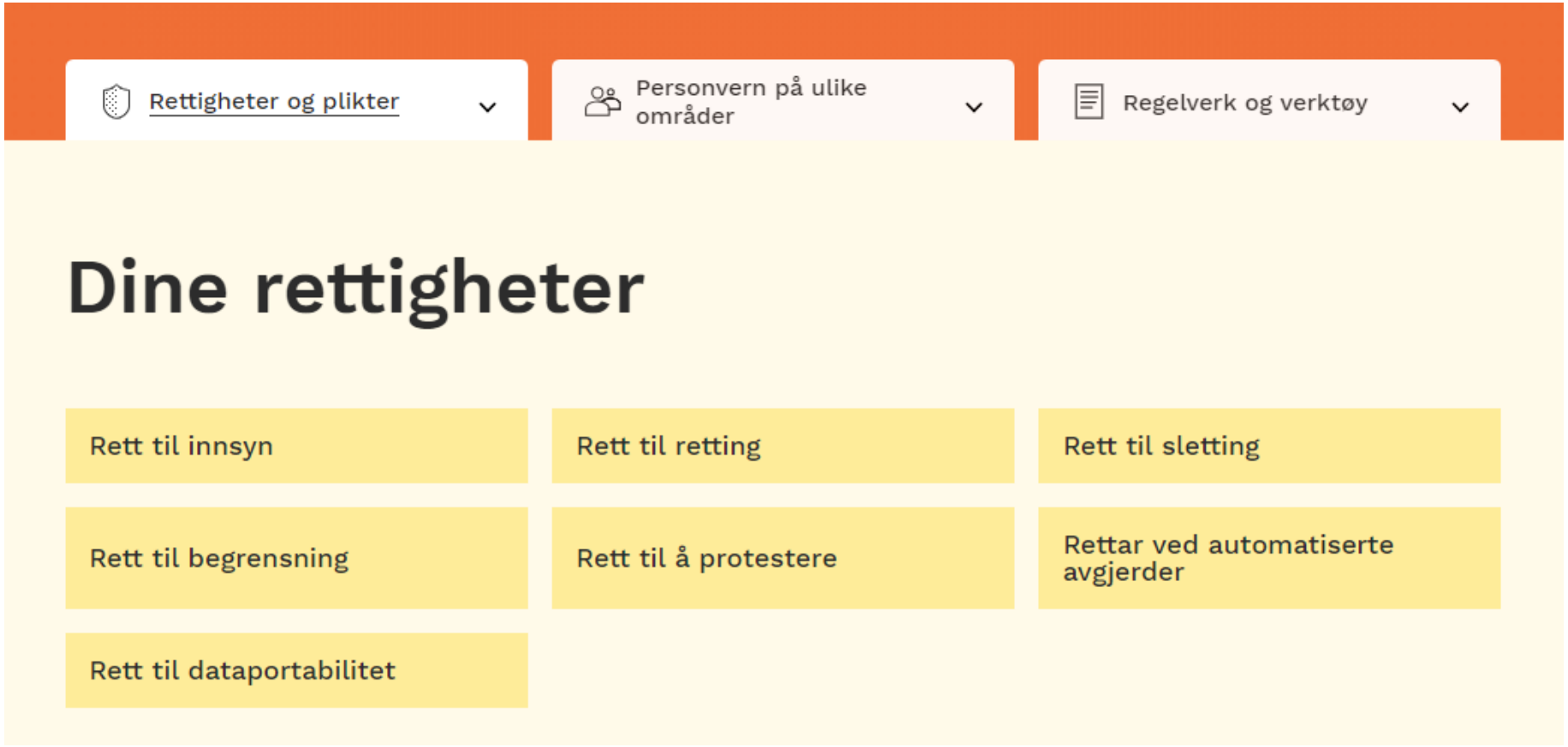
Personvernombud

Skal:

- Involveres tidlig nok i prosessen
- Skal få tilstrekkelig støtte i utførelsen av oppgaver
- Skal ikke instrueres mv. i utførelsen
- Skal rapportere direkte til øverste ledelsesnivå
- Taushetsplikt

- Flytende kompetansekrav:
  - Mengden av personopplysninger
  - Behovet for beskyttelse
  - Kompleksitet i behandlingene
  - Systematisk behandling utenfor EU

De registrertes rettigheter



Etterlevelse

Artikkel 5.2:

«Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at nr. 1 overholdes («ansvar»)»

Artikkel 30.1:

«…skal føre en protokoll over behandlingsaktiviteter som utføres under deres [behandlingsansvarliges] ansvar.»

Bransjenormer

Formålet med bransjenorm for bank og kredittforetak er dels å skape forutsigbarhet for bransjen i tolkningen av lov om behandling av personopplysninger og GDPR, slik at regelverket etterleves på en tilfredsstillende måte, og dels å skape et tillitsvekkende og godt personvern for de registrerte.

Bransjenormer – forutsigbarhet

Formål

- Kundeadministrasjon, fakturering og gjennomføring av bank- og finansieringstjenester
- Markedsføring
- Risikoklassifisering av kunder og kredittporteføljer
- Forebygging og avdekking av straffbare forhold

…

Behandlingsgrunnlag

- Avtale
- Samtykke
- Rettslig forpliktelse
- Berettiget interesse

Særlig relevante formål for bank og kredittforetak vil være:

- Kundeadministrasjon og gjennomføring av bank- og finansieringstjenester
  - Den daglige behandlingen av personopplysninger for å oppfylle avtale med kunden, for eksempel inngåelse, fornyelse og administrasjon av låneavtale, kredittvurdering, utførelse av betalingsoppdrag og rådgivning med hensyn til hvilke typer produkter og/eller tjenester som kan være hensiktsmessig for kunden,samt dokumentasjon av kundens forespørsler og kundeengasjement.
  - Behandlingsgrunnlag: Personvernforordningen artikkel 6 nr. 1 bokstav b) og f)
- Markedsføring
  - Aktivitet, herunder for eksempel profilering og segmentering, der formålet er å inngå avtaler om nye tjenester eller produkter med nye eller eksisterende kunder
  - Behandlingsgrunnlag: Personvernforordningen artikkel 6 nr. 1 bokstav a) og f)
- Utvikling av nye og eksisterende tjenester
  - Behandling av personopplysninger for å identifisere potensiell etterspørsel etter nye produkter og tjenester eller forbedring av funksjonalitet i allerede eksisterende produkter og tjenester, herunder analyse og testing i forbindelse med utviklingen av disse.
  - Behandlingsgrunnlag: Personvernforordningen artikkel 6 nr. 1 bokstav a), b) og f)
- Konsernkunderegister/deling av informasjon innad i konsern/samarbeidende gruppe[9]
  - Føring av felles kunderegister med andre finansforetak i samme konsern. Formålet med konsernkunderegisteret er å administrere kundeforholdet og samordne tilbudet av tjenester og rådgivning fra de forskjellige selskapene i konsernet, herunder markedsføring
  - Utveksling av fødselsnummer samt enkel kundeinformasjon, (navn, kontaktopplysninger og hvilke tjenester og produkter en kunde har avtale om), knyttet til den delen av virksomheten som samarbeidet gjelder.
  - Utveksling av informasjon om utdypende kundeinformasjon, slik som ytterligere informasjon om produktene og bruken av disse, herunder transaksjoner etc.
  - Behandlingsgrunnlag: Personvernforordningen artikkel 6 nr. 1 bokstav a) og f)

Bransjenorm – etterlevelse

Informasjon

- Hvem skal informeres
- Hva skal det informeres om?
- Hvordan kan informasjon gis?
- Når skal det informeres?

5.1.1 Hvem skal informeres?

Det er den registrerte som har krav på informasjon i tråd med bestemmelsene, det vil si de personer banken har registrert personopplysninger om – dette kan være alt fra kunder, potensielle kunder, medarbeider hos kunder eller andre relevante parter, som reelle rettighetshavere, autoriserte representanter, bedriftskortinnehavere og tilknyttede parter. Selv om informasjonsplikten er rettet mot de registrerte, kan det være hensiktsmessig også å informere via bankens åpne kanaler, eksempelvis bankens nettsider. Da sikres det at informasjonen er tilgjengelig på enkel måte.

- For privatkunder kan informasjon gis som et vedlegg til en inngåelse av en tjenesteavtale, via nettbank eller andre digitale kanaler som bankens nettside (evt. med en henvisning i tjenesteavtalen til hvor informasjonen finnes)
- For kontaktpersoner hos virksomhetskunder kan det være hensiktsmessig å informere via nettsidene, men da gjerne med en henvisning i tjenesteavtale eller lignende om hvor informasjonen forefinnes
- For kontaktpersoner hos leverandører og samarbeidspartnere er det også naturlig å informere via nettsider, men også her gjerne med en henvisning til hvor informasjonen finnes i avtaler eller lignende
- Øvrige personer må informeres på en mest hensiktsmessig måte avhengig av hvilken tilknytning den registrerte har til banken. Kreditorer, kausjonister ol som banken har en naturlig relasjon til, bør informeres tilsvarende som privatkunder.
- Personvernforordningen artikkel 14 gjør unntak fra informasjonsplikten der det er umulig eller vil innebære uforholdsmessig stor innsats å gi informasjon. Informasjon via bankens nettsider bør imidlertid ta høyde for å informere disse gruppene av personer

Bransjenorm – etterlevelse

Sletting

- Avtale
- Rettslig forpliktelse
- Samtykke
- Berettiget interesse

Bransjen er underlagt omfattende regulering, som nødvendiggjør å kunne dokumentere sin virksomhet, eksempelvis inngåtte avtaler, transaksjoner som er gjennomført mellom foretaket og kunden og de beslutninger som foretaket har tatt i kundeforholdet - både overfor relevante tilsyns- og kontrollmyndigheter og tidligere kunder. Dette innebærer i realiteten et dokumentasjonsbehov så lenge en kunde potensielt kan rette et erstatningskrav mot foretaket, frem til foreldelsesfristen er utløpt. Den alminnelige foreldelsesfrist er 3 år, men denne kan utvides med inntil 10 år på bakgrunn av "uvitenhet og andre hindringer".[32] For gjeldsbrev, pengekrav og kausjon er det 10 års foreldelsesfrist.[33] Utgangspunktet vil dermed være at personopplysningene slettes når det er gått 13 år. For avtaler og annen dokumentasjon knyttet til rammene for kundeforholdet regnes fristen fra det aktuelle avtaleforholdet er avsluttet.

Bokføringsloven § 13

- 5 års lagring av primærdokumentasjon (faktura knyttet til annet enn kontoforhold, herunder leasingavtaler, kredittkortavtaler o.l.) etter regnskapsårets slutt.
- 3,5 års lagring av sekundærdokumentasjon (kundeavtaler, korrespondanse knyttet til tap/nedskrivinger o.l.) etter regnskapsårets slutt.

Bokføringsforskriften § 8-13-4

- 10 års lagring av kontoutskrifter, eller informasjon som danner grunnlag for å utarbeide kontoutskrifter.

Hvitvaskingsloven § 30

- 5 års lagring av opplysninger innhentet i forbindelse med kundekontrollen eller mistenkelige transaksjoner etter at kundeforholdet er avsluttet eller transaksjonen gjennomført.[31]

Regler om BankID pkt. 15.2

- Minst 10 års lagring av sertifikatopplysninger etter at gyldighetsperioden for et BankID er utløpt eller etter at det er tilbakekalt.

Bransjenorm – godt personvern

- Personvernombud
- Gjenbruk
- Informasjonsplikt og innsynsrett
- Dataportabilitet

Harmonisering

Noen eksempler

Hvitvaskingsloven § 27:

«rapporteringspliktig kan behandle personopplysninger, herunder sensitive personopplysninger, for å oppfylle sine plikter etter loven her»

Noen eksempler

PSD2:

- Uttrykkelig samtykke?
- Gjenbruk?

Hva nå?

Er GDPR over?

GDPR er ikke over

www.finansnorge.no/personvern