Etterlevelse av GDPR i finansbransjen

Oslo, 6. mars 2019

Building a better working world

Introduksjon

Ingvild O. Kågen
Advokat/Associate Partner

E-post:
Ingvild.O.Kaagen@no.ey.com

Mobil: 93 44 12 16

Financial Services Organization:
400 i Norden og ca 12 500 i Europa
62 500 globalt

1 integrert team med en felles visjon som arbeider på tvers av **19** ulike land og fire forretningsområder

Bransjespesialisering
- Bank og kapitalmarked
- Forsikring
- Kapitalforvaltning

Databehandleravtaler

Begrepsavklaring

Behandlingsansvarlig

Fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes. Den behandlingsansvarlige er det primære rettssubjektet etter forordningen, og er overordnet ansvarlig for å overholde regelverket

Databehandler

Fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige

Databehandleravtale

En avtale som regulerer forholdet mellom en behandlingsansvarlig virksomhet og databehandleren. Avtalen skal sikre at personopplysningene blir behandlet i samsvar med regelverket og setter en klar ramme for hvordan databehandleren kan behandle opplysninger

Databehandleravtaler

Når må databehandleravtale foreligge?

Dersom en virksomhet som er behandlingsansvarlig, setter ut hele eller deler av behandlingen av personopplysninger til andre virksomheter, er den eller de som behandler opplysningene på vegne av den behandlingsansvarlige definert som databehandlere

Kontrollspørsmål tilknyttet etterlevelse:

- Behandler andre rettssubjekter personopplysninger på vegne av foretaket?
- Har vi rett fokus i databehandleravtalen?
- Har vi inngått unødvendige databehandleravtaler – og derved økt egen risiko?
- Hvordan sikrer vi i avtaleperioden at databehandler faktisk ivaretar personopplysninger på våre vegne på en forsvarlig måte?

Behandles personopplysninger på vegne av foretaket?

- Ikke nok at du finner en databehandleravtale i systemet
- Sjekk at avtalen er nødvendig og tilstrekkelig
  - Hva med leverandør av elektronisk utstyr?
  - Hva med konsulenter som bruker eget utstyr?
  - Hva med konsulenter som bruker foretakets utstyr?
  - Hva med namsfogden?
- Konsern
  - Nødvendig med avtaler mellom selskapene i konsern?
  - Er foretaket databehandler?
- Felles behandlingsansvarlig?
  - Hver enkelt behandlingsansvarlig har lovlig adgang på egenhånd til å behandle konkrete personopplysninger – fastsetter mål og midler i fellesskap

KONTROLLSPØRSMÅL

- Behandles personopplysningene kun til foretakets formål?
- Har den andre part bestemmelsesrett over personopplysningene?
- Er den annen part et selvstendig rettssubjekt?
- Har du instruksjonsmyndighet ovenfor den annen part?
- Kan du kontrollere at den andre part behandler personopplysninger som avtalt?
- Kan du kreve at den andre part sletter eller tilbakeleverer opplysninger?

Har vi rett fokus i databehandleravtalen?

- Beskriver databehandleravtalen konkret hva databehandler faktisk skal gjøre?
  - Lagring på server
  - Plattform for tjenester
  - Systemer som skal brukes
  - Markedsføring
  - Kameraovervåkning
- Er det tydelig hvordan de skal behandle personopplysningene?
- Er det tydelig hva som er formålet med behandlingen?
  - Hindre at personopplysningene brukes på annen måte enn avtalt
- Hvor lenge skal avtalen løpe?
- Hva slags personopplysninger er registrert?
- Hvilke kategorier personopplysninger gjelder dette?
  - Ansatte?
  - Kunder?
  - Leverandører?

Oppfølging av databehandlers sikkerhetstiltak - risikostyring

- Tips
  - Har foretaket kontroll på hele livsløpet?
  - Har foretaket kvalitetssikret at de som bestiller tjenester faktisk har nødvendig kompetanse?
    - Tverrfaglig kompetanse ofte nødvendig
      - Juridisk kompetanse
      - IT kompetanse
      - Personvern kompetanse – personvernombud
  - Selve internkontrollen bør ofte gjennomføres med et tverrfaglig team
    - Oppfølging at databehandler fortsatt har nødvendig kompetanse
    - Sikkerhetskrav både fysisk, personell og informasjons-sikkerhet
  - Hva med avtaler som er underlagt andre jurisdiksjoner?
  - Hva med selskaper som henviser til BCR?
  - Oppfølging av planer for at data tilhørende foretaket blir forsvarlig slettet av leverandør
  - Stikkprøver på at tekniske og organisatoriske tiltak for å beskytte personopplysninger mot uautorisert tilgang, skade eller misbruk er gode nok
    - Maskinvare
    - Programvare
    - Tilknyttet infrastruktur
  - Teste at evt. krav til kryptering eller anonymisering er gode nok
  - Gjennomføres krav til logging i tråd med hva som er avtalt?
  - Internkontroll

Håndtering av avvik

Håndtering av avvik

- Hva er et avvik?
- Hvem har ansvar for hva?
- Hvem må varsles internt og eksternt?

Hva er et avvik?

- Brudd på behandling av personopplysninger som fører til
  - Utilsiktet eller
  - Ulovlig tilintetgjøring
  - Tap
  - Endring
  - Ulovlig spredning av eller
  - Tilgang til personopplysninger

- Eksempler på dette
  - E-post med personopplysninger som krever særlig beskyttelse sendt på åpen og ukryptert e-post
  - Feil ved utsendelse av dokumenter – elektronisk eller per post
  - Feil i kundeuttrekk – markedsføring til noen som ikke har gitt samtykke
  - Personopplysninger som burde vært slettet er ikke slettet
  - Tilgangskontroll ikke tilstrekkelig

Hvem har ansvar for hva og kan vi dokumentere det og at systemet fungerer?

- Er det tydelig hvem som har hvilke oppgaver ved et avvik?
- Vet alle hvor en hendelse skal rapporteres?
- Hvem har ansvar for å følge opp innrapporterte hendelser?

Hvem skal det rapporteres til internt og eksternt?

- Personvernombud eller intern personvernansvarlig?

- Varsling til Datatilsynet
  - Må alt varsles?
  - Lite trolig at bruddet medfører en risiko for de registrertes rettigheter?
  - Personvernombudet vurderer og rapporterer til Datatilsynet

- Varsling til den registrerte
  - Hvem skal varsle den registrerte?
  - Når må den registrerte varsles?
  - Hvilken informasjon er gitt den registrerte?
    - Hva har skjedd
    - Hvilke personopplysninger gjelder det
    - Kontaktinformasjon til rett person i foretaket
    - Beskrivelse av mulige konsekvenser
    - Beskrivelse tiltak

Håndtering av avvik

Avvikshåndtering

- Alle virksomheter skal melde fra til **Datatilsynet** ved brudd på personopplysningssikkerheten
- Avviksmeldingen skal uten ugrunnet opphold leveres så snart det er kjennskap til bruddet, senest innen **72 timer**
- **Formålet** med avvikshåndtering er å begrense skadeomfanget for selskapet og for den enkelte registrerte. Vi må også registrere avvik for å kunne lære av våre feil og forbedre sikkerhetskrav og -rutiner.

Når vi oppdager at det har skjedd et avvik skal det meldes fra til nærmeste leder umiddelbart

Eksempler på avvik

- Personopplysninger blir sendt til feil mottaker
- Uautorisert innsyn i saksbehandlings-systemer
- Innsamling av informasjon som ikke er nødvendig for formålet
- Sammenstilling og gjenbruk av informasjon som ikke er forenelig med det opprinnelige formålet
- Mangelfull sletting av informasjon når lovlig oppbevaringstid er passert
- Hacking

Se gjerne Datatilsynets veileder

Personvernforordningen art. 32 til 34

Opplæring og modenhet i foretaket

Opplæring og modenhet i foretaket

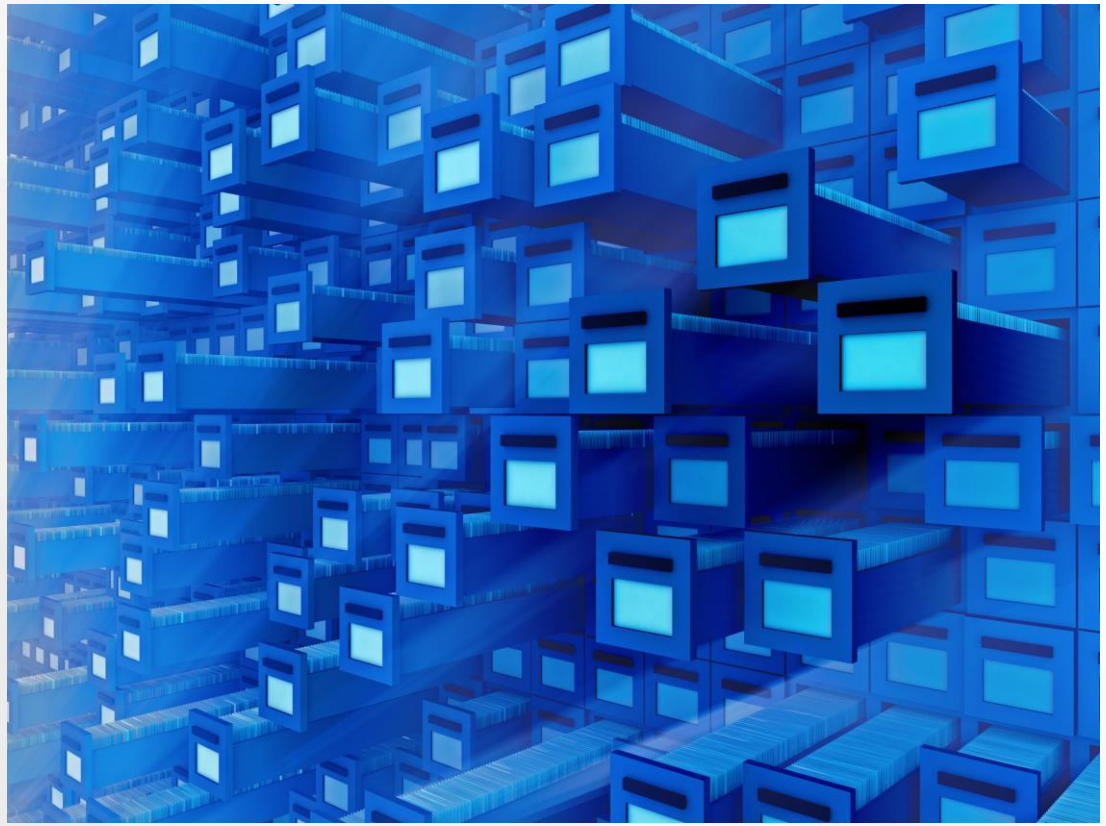
- Er det nok å ha rutiner og å kjøpe e-læringsprogram fra eksterne parter?
- Hvordan sikrer vi at de ansatte faktisk har nødvendig GDPR kunnskap til å håndtere personopplysninger korrekt i sin rolle?
- Når må opplæring og modenhet følges opp ovenfor de ansatte?
- Har det konsekvens dersom vi har ansatte som ikke har nødvendig kunnskap?

Strukturert og ustrukturert data

Strukturert og ustrukturert data

- Strukturert data = data organisert på en predefinert måte i en database
- Ustrukturert data = Alt mulig annet
  - E-post
  - Dokumenter
  - Regneark
  - Bilder
  - Lydfilmer
  - Kameraopptak
  - Annen data ikke organisert i en database

- Vet egentlig de ansatte forskjellen på strukturert og ustrukturert data og hvorfor vil uvitenhet øke selskapets risiko for ikke å ha kontroll?



Kartlegging og dataminimering – hva bør internrevisjonen etterprøve?

Informasjon er lagret i relevante og sentraliserte IT-systemer	**Bruk av e-post brukes ikke som medium ved deling av personopplysninger**	**E-post brukes ikke som lagringsmedium**	**Foretaket bruker ikke felles lagring på disk eller lokalt område som lagringsmedium for andres personopplysninger**