Personvernforordningen - for regnskapsførere

Agenda

- Kort om personvernforordningen (GDPR)
- Bransjenorm for regnskapsførere
- Regnskapsførervirksomhetens behandling av personopplysninger
- Databehandlerens plikter
- Databehandleravtaler
- Internkontroll og risikovurderinger
- Den registrertes rettigheter
- Ansvar
- Oppsummering

Personvernforordningen

Personvernforordningen (GDPR)

- Forordning inkorporert i norsk lov
- I kraft fra mai 2018 i EU og fra juli 2018 i Norge
- Viderefører i stor grad gjeldende rett
- Enkelte nye rettigheter og plikter
- Personvernregelverket:
  - Personopplysningsloven, inkludert personvernforordningen
  - Andre lov- og forskriftsbestemmelser som regulerer personvern og personoppplysninger

  = «Personvernregelverket»

Personvernforordningen (GDPR)

- Nøkkelbegreper:
  - «Personopplysninger»
  - «Den registrerte»
  - «Sensitive personopplysninger»
  - «Behandling»
  - «Behandlingsansvarlig»
  - «Databehandler»
  - «Underdatabehandler»

Bransjenorm for regnskapsbransjen

Bransjenorm for regnskapsbransjen

- Bransjestandardutvalget: Atferdsnorm for behandling av personopplysninger i regnskapsbransjen
- NB: utkast, ikke godkjent av Datatilsynet (enda)
- Gjelder regnskapsførervirksomheten som databehandler
- Etterlevelse og kontroll
- Status
- Veileder fra European Data Protection Board (EDPB)

Regnskapsførerbransjens behandling av personopplysninger

Regnskapsførerbransjens behandling av personopplysninger

- Både behandlingsansvarlig og databehandler
- Personopplysninger som behandles i regnskapsførerbransjen
  - Ordinære personopplysninger
  - Sensitive personopplysninger, særlig;
    - Fagforeningsmedlemskap
    - Tilknytning til trossamfunn og politisk tilhørighet
    - Helseopplysninger
- Formålet med behandlingen
  - Hovedformål: Assistere oppdragsgiver med sine plikter i forbindelse med regnskap, lønn, skatt og avgift.
  - Endring av formål

Regnskapsførerbransjens behandling av personopplysninger

- Behandling av personopplysninger må ha et rettslig grunnlag – «behandlingsgrunnlag»
  - Lovpålagte plikter og andre lovhjemler
  - Samtykke
- Personvernombud
  - I de fleste tilfeller ikke pålagt
  - Kan opprettes frivillig
- Personvernkontakt
  - Pålagt i hht. bransjenormen

Databehandlerens plikter

Databehandlerens plikter

- Behandlingsansvarlig har det primære ansvaret
- Databehandleren er pålagt en rekke plikter:
  - Behandling i hht. databehandleravtale og instruks fra behandlingsansvarlig
  - Protokoll
  - Varslingsplikt
  - Tilgang til informasjon
  - Samarbeidsplikt med Datatilsynet
  - Sørge for tilstrekkelig informasjonssikkerhet
  - Personvernombud
  - Grenseoverskridende overføring

Databehandleravtaler

Databehandleravtaler

- Legaldefinisjonen:

Personvernforordningen art. 28 nr. 3:

«*Behandling utført av en databehandler skal være* ***underlagt en avtale*** *eller* ***et annet rettslig dokument*** *i henhold til unionsretten eller medlemsstatenes nasjonale rett* ***som er bindende for databehandleren*** *med hensyn til den behandlingsansvarlige* […].»

Databehandleravtaler

- En del av oppdragsavtalen eller separat avtale
- Minimumskrav til innhold
  - Gjenstanden for og varigheten av behandlingen
  - Behandlingens art og formål
  - Typen personopplysninger
  - Kategorier av registrerte
  - Den behandlingsansvarliges rettigheter og plikter
- Underdatabehandleravtaler

Internkontroll og risikovurderinger

Internkontroll

- Regnskapsførerloven § 2: autoriserte regnskapsførere skal utføre sine oppdrag i samsvar med bestemmelser i og i medhold av lov og i samsvar med god regnskapsføringsskikk
- Standard for god regnskapsføringsskikk (GRFS)
- Personvernforordningen:
  - Tekniske og organisatoriske tiltak
  - Digitalt og analogt
  - Konfidensialitet, integritet og tilgjengelighet
  - Dokumentasjonskrav

Internkontroll

- Bransjenormen
  - Tilgangskontroll
  - Krav om innebygget personvern
  - Logiske og fysiske sikkerhetstiltak
  - Behandling av ustrukterte opplysninger
- Vurdering av personvernkonsekvenser – DPIA
  - Ansvaret ligger hos oppdragsgiver
  - Regnskapsførervirksomheten kan bistå i arbeidet etter behov og etter avtale med oppdragsgiver

Risikovurdering

- Helhetlig tilnærming i samhold med annen risikovurdering
- Vurdering av intern og ekstern eksponering, samt eksponering utenfor behandlingsmiljøet
- Skriftlig, oppdatert og tilgjengelig

Den registrertes rettigheter

Den registrertes rettigheter

- Den registrerte har rett til:
  - Informasjon
  - Innsyn
  - Sletting (retten til å bli glemt)
  - Retting
  - Overføring (dataportabilitet)
- Den registrerte skal forholde seg til behandlingsansvarlig
- Oppdragsgiver kan instruere regnskapsførervirksomheten

Særlig om sletting

- Personopplysninger skal ikke oppbevares lengere enn nødvendig
- Oppdragsgiver har ansvaret
- Regnskapsførervirksomheten skal kun slette opplysninger etter avtale eller instruks
- En fordel å utarbeide faste sletterutiner med oppdragsgiver
- Sletting kan ikke utføres hvis opplysningene er nødvendig for å ivareta oppbevaringskrav i regnskapsførerloven, bokføringsloven, hvitvaskingsloven eller annen relevant lovgivning.

Ansvar

Ansvar

- Erstatning til de registrerte iht. forordningen
- Overtredelsesgebyr iht. forordningen
- Avtalerettslig erstatningsansvar

Oppsummering

Oppsummering

- Behandlingsansvarlig vs. Databehandler
- Databehandlerens plikter, særlig;
  - Databehandleravtale
  - Varslingsplikt
- Tips og råd
  - Kunnskap
  - God dokumentasjon
  - Solid avtaleverk
  - Klare rutiner
  - Jevnlig gjennomgang og oppdateringer
  - Overholdelse

Takk for oppmerksomheten!

Kontaktdetaljer:

Navn: Lisa Urke Hennum

Web: www.braekhus.no

Epost: urke@braekhus.no

Mobil: 98 86 04 75