Kjappe fakta om GDPR

Hva er det?

Hvis du behandler personopplysninger i virksomheten din, må du kjenne til at EU har vedtatt en ny personvernforordning (GDPR) som inneholder regler for hvordan man kan behandle personopplysninger. Det har tatt EUs største tungvektere fire år å bli enige om en ny lovtekst, og denne forordningen kommer til å erstatte den nåværende personvernlovgivningen i Norge.

Når?

Forordningen trer i kraft 25. mai 2018.

Hvorfor?

Den nye personvernforordningen innføres for å gi en økt grad av beskyttelse for alle registrerte personer, og er tilpasset dagens teknologi. En annen grunn til at den nye loven er utarbeidet, er for å kunne ensrette behandlingen av personopplysninger i alle EU-land samt land som velger å følge den, slik som Norge.

Hva er en personopplysning?

Personopplysninger er all informasjon som kan knyttes til en enkeltperson. Typiske personopplysninger er personnummer, navn og e-postadresse. Bilder av personer regnes også som personopplysninger. Et organisasjonsnummer regnes som regel ikke som en personopplysning, men hvis det dreier seg om organisasjonsnummeret til et enkeltpersonforetak, er det en personopplysning. Registrerings-nummeret på en bil kan være en personopplysning, hvis bilen er registrert på en fysisk person. Registreringsnummeret på en firmabil som kanskje brukes av flere, er neppe en personopplysning.

Hvordan?

Det er mye i GDPR som ligner på de reglene som finnes i personopplysningslovgivningen i dag. En viktig forskjell er at det her uttrykkelig fastslås at de som behandler personopplysninger, skal være ansvarlig for, og kunne *bevise*, at man følger reglene i den nye personvernforordningen (ansvarlighet). Virksomheter som behandler personopplysninger, må dermed aktivt ta ansvar for å sikre at reglene i forskriften følges, og kunne *bevise* dette. Alt som har med behandling av personopplysninger å gjøre, skal dokumenteres.

Når og for hvem gjelder personvernforordningen?

Personvernforordningen gjelder for alle virksomheter som behandler personopplysninger, både når virksomheten selv bestemmer over behandlingen (behandlingsansvarlig) og når virksomheten utfører behandlingen på vegne av noen annen (databehandler). Det er alltid den behandlingsansvarlige som står ansvarlig overfor de registrerte personene.

Kan man fortsatt innhente og behandle personopplysninger?

Det vil også i fremtiden være tillatt å innhente, behandle og oppbevare personopplysninger. Det avgjørende er formålet med innhentingen og det rettslige grunnlaget for å håndtere personopplysninger. All behandling av personopplysninger må oppfylle kravene i personvernforordningen, og man skal kunne vise til at loven gir støtte for behandlingen av personopplysningene. Et slikt juridisk grunnlag kan eksempelvis være samtykke,

eller at behandlingen av personopplysninger er nødvendig for å kunne oppfylle en tjeneste som avtalt med den registrerte. Følgende er fire «juridiske grunnlag» som virksomheter kan bruke som grunnlag for behandling av personopplysninger (se også artikkel 6 i personvernforordningen):

- ✓ **Juridisk forpliktelse** – I enkelte tilfeller plikter virksomheter å registrere personopplysninger, f.eks. for å overholde regnskapsmessige forpliktelser etter bokføringsloven.
- ✓ **Avtaler** – Arbeidskontrakter, kundeavtaler og leverandøravtaler er eksempler på kontrakter som krever at selskaper registrerer og administrerer personopplysninger (kun nødvendige opplysninger).
- ✓ **Interesseavveining** – Hvis selskapet kan vise at dennes behov for å håndtere personopplysningene veier tyngre enn den enkeltes rett til personvern.
- ✓ **Samtykke** – Man kan alternativt be personen om lov til å registrere informasjon om vedkommende.

I tillegg til det ovenstående finnes det to andre grunner som ikke er like vanlige:

- ✓ **Behandling for å utføre en oppgave av allmenn interesse**
- ✓ **Offentlig interesse og utøvelse av offentlig myndighet**

Hva gjelder for innsamling av personopplysninger?

Personopplysninger kan kun innhentes for bestemte, eksplisitte og legitime formål. Dette innebærer at hvis du som kunde skal lagre personopplysninger, må du definert et klart formål for dette før innhentingen av personopplysninger begynner. Dette formålet skal også dokumenteres skriftlig.

Mengden opplysninger skal også begrenses til det som er nødvendig for å kunne oppfylle det definerte formålet. Opplysningene kan ikke behandles på et senere tidspunkt på en måte som ikke er i samsvar med dette formålet, og kan heller ikke oppbevares lenger enn det som er nødvendig. Virksomheten som behandler personopplysninger, må kunne dokumentere samsvar med reglene.

Hvem sjekker at den nye loven blir overholdt?

Datatilsynet kontrollerer om GDPR overholdes i Norge, og kan ilegge dem som ikke overholder reglene i forordningen, bøter på opptil 20 millioner euro. Beløpets størrelse avhenger av regelbruddets art, for eksempel om det er forsettlig eller ikke, hvordan og om virksomheten har rettet opp det som bryter med reglene, og om virksomheten har tjent penger på overtredelsene.

I dag kan personer varsle Datatilsynet hvis man mener at personvernet har blitt krenket. Da kan tilsynssak opprettes. Det er imidlertid uklart hvorvidt den nye EU-loven kommer til å innebære f.eks. stikkprøvekontroller. Et nytt moment er at man skal kunne henvende seg til «sin egen» tilsynsmyndighet hvis man har innsigelser til behandling av personopplysninger i et annet land.

Hva er et personvernombud, og hvilke virksomheter er pålagt å ha et slikt ombud?

Alle selskaper der kjernevirksomheten innebærer håndtering av sensitiv informasjon eller informasjon som krever regelmessig og systematisk overvåking i et betydelig omfang, små ansette et personvernombud (Data Protection Officer, DPO). Vedkommende skal ha ansvar for å sørge for at virksomheten følger retningslinjene i personvernforordningen og andre lover om personvern. Konsernselskaper og også uavhengige selskaper kan ha et felles personvernombud. Myndigheter og offentlige organer skal alltid ha et personvernombud.