Ny veiledning for behandling av personopplysninger i revisjonsbransjen

I artikkelen redegjøres det nærmere for utvalgte punkter som tas opp i revisjonsbransjens veiledning for behandling av personopplysninger. I tillegg gis noen praktiske råd for hvordan man kan ivareta personvernet i det daglige.

Advokatfullmektig
Marthe Femanger Pettersen
Wiersholm

Advokat
Line Haukalid
Wiersholm

I revisjonsbransjen finnes det flere lover som revisjonsforetak må forholde seg til ved behandling av personopplysninger. I tillegg har revisorloven egne taushetspliktsregler.

Revisorforeningen har utarbeidet en veiledning som skal gjelde for behandling av personopplysninger i revisjonsbransjen. Denne oppsummerer de viktigste personvernforpliktelsene som gjelder for et revisjonsforetak ved levering av revisjons- og andre tjenester. Formålet med veiledningen er å klargjøre hvordan personvernreglene skal praktiseres i bransjen, samt bidra til forsvarlig behandling av personopplysninger.

Datatilsynet kan godkjenne bransjenormer som kan håndheves og sanksjoneres av bransjeorganisasjoner. Revisorforeningen har ikke ønsket å ha slike mekanismer og har derfor utarbeidet en veiledning for behandling av personopplysninger i revisjonsbransjen.

Når behandler revisjonsforetaket personopplysninger?

Et revisjonsforetak behandler normalt først og fremst bedriftsrelaterte opplysninger i sine oppdrag for klienter. I en viss grad er det imidlertid også nødvendig å behandle personopplysninger, for eksempel i utførelsen av revisjonsoppdrag, utarbeidelse av regnskap og skattemeldinger, og for å overholde forpliktelsene etter hvitvaskingsregelverket.

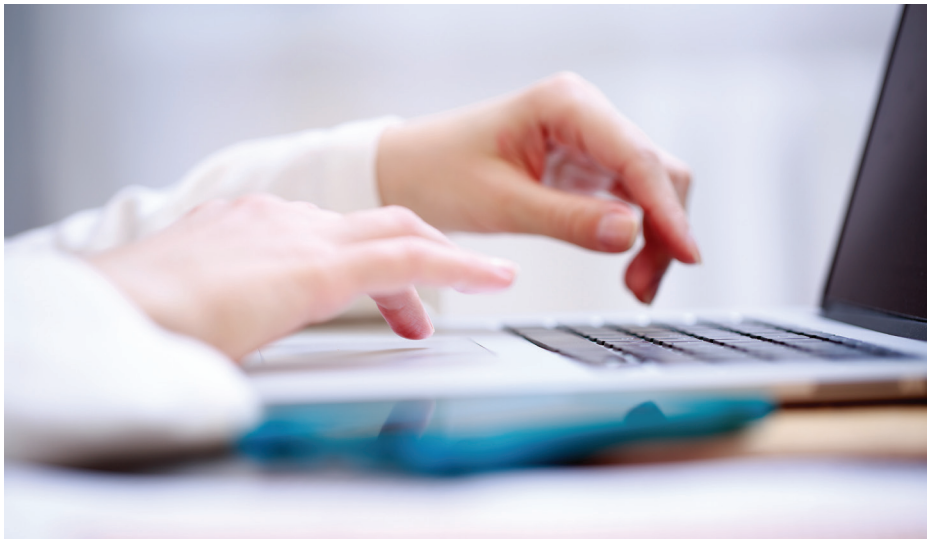
Revisjonsforetaket vil også behandle personopplysninger i forbindelse med administrering av personalmessige forhold, markedsføring, oppfølging av leverandører og annet som gjelder drift av revisjonsforetaket. Denne type behandlingsaktiviteter må håndteres i revisjonsforetak på samme måte som i andre foretak, og omtales derfor ikke i veiledningen eller i denne artikkelen.

Behandlingsansvarlig og databehandler

En behandlingsansvarlig er i personvernrettslig forstand den som bestemmer formål og midler med behandlingen av personopplysningene. Dette vil være tilfellet for en rekke av revisjonsforetakets behandling av personopplysninger, ettersom revisjonsforetaket avgjør hvilke kontrollhandlinger som må utføres og hvilke opplysninger som må innhentes som grunnlag for sin uttalelse eller rapport. Revisorforetaket vil typisk bestemme *at* personopplysninger samles inn, hvilke personopplysninger som trengs for å utføre revisjonsoppdraget, samt i *hvilket system eller verktøy* personopplysningene skal behandles.

Den behandlingsansvarlige må ha et rettslig grunnlag for behandlingen av personopplysninger. Dette kalles behandlingsgrunnlag, og kan for eksempel være lovhjemmel, samtykke, avtale eller en dokumentert interesseavveining, hvor interessen i å behandle personopplysninger for et gitt formål veies opp mot hensynet til den enkeltes personvern.

I noen tilfeller er det klienten som bestemmer at personopplysninger samles inn og hvilke personopplysninger som behandles, mens revisjonsforetaket behandler personopplysningene på klientens vegne. Da er revisjons-



Et revisjonsforetak behandler normalt først og fremst bedriftsrelaterte opplysninger i sine oppdrag for klienter.

foretaket en databehandler, og må behandle personopplysningene i tråd med klientens instrukser. Slike instrukser gis i en databehandleravtale, som partene må inngå samtidig med oppdragsavtalen. Når revisjonsforetaket er databehandler, er det databehandleravtalen som gir rettslig grunnlag for behandling av personopplysninger.

Revisjonsforetaket som behandlingsansvarlig

Veiledningen slår fast at revisjonsforetaket opptrer som behandlingsansvarlig når foretaket samler inn og bruker personopplysninger i forbindelse med revisjon, forenklet revisorkontroll av regnskaper, attestasjonsoppdrag og avtalte kontrollhandlinger hvor revisor bekrefter opplysninger overfor offentlige myndigheter eller utfører forenklet revisorkontroll etter aksjeloven §§ 7–7 til 7–9. Revisorloven er behandlingsgrunnlag for slik behandling av personopplysninger.

Videre er revisjonsforetaket behandlingsansvarlig for personopplysninger som samles inn i forbindelse med utførelse av kundetiltak. Dette inkluderer registrering av opplysninger om reelle rettighetshavere og den som handler på vegne av kunden. Behandlingsgrunnlaget følger her av hvitvaskingsloven.

Revisjonsforetaket er videre behandlingsansvarlig for årsoppgjørsoppdrag og utarbeidelse av aksjonærregisteroppgaver for egne revisjonsklienter. Dette gjelder imidlertid kun hvis personopplysningene brukt i forbindelse med disse tjenestene også har betydning for revisjonen. Hvis revisor for aksjonærregisteroppgave- og årsoppgjørsformål behandler personopplysninger som *ikke* har betydning for revisjonen, vil revisorforetaket behandle disse personopplysningene som en databehandler. Veiledningen oppfordrer revisjonsforetaket til å anvende skjønn for å avgjøre om personopplysningene har betydning for revisjonen eller ikke.

Andre eksempler på tjenester som revisjonsforetaket utfører som en behandlingsansvarlig er: due diligence, granskningsoppdrag, internrevisjon, samt andre attestasjonsoppdrag eller avtalte kontrollhandlinger enn de som er nevnt ovenfor. I disse tilfellene er det GDPR art. 6 nr. 1 bokstav f interesseavveining, som er behandlingsgrunnlag.

Rollen som behandlingsansvarlig innebærer at revisjonsforetaket har ansvaret for å sikre at personopplysningene behandles i tråd med personvernregelverket, herunder at de behandles sikkert, at revisjonsforetaket har behandlingsgrunnlag og at individene som personopplysningene gjelder («de registrerte») er informert om behandlingen.

At revisjonsforetaket opptrer som behandlingsansvarlig for personopplysninger mottatt fra klienten, betyr at revisor ikke trenger å inngå en databehandleravtale med klienten. Noen foretak velger likevel å ta inn en egen personvernklausul i oppdragsavtalen, som slår fast at revisjonsforetaket mottar personopplysningene som behandlingsansvarlig, og har ansvar for å behandle personopplysningene i samsvar med personvernregelverket.

Revisjonsforetaket som databehandler

Som nevnt over, er revisjonsforetaket databehandler for personopplysninger som behandles for aksjonærregisteroppgave- og årsoppgjørsformål, dersom opplysningene ikke har betydning for revisjonen. Tilsvarende vil revisjonsforetaket være databehandler når det yter slike tjenester til andre enn revisjonsklienter. Et annet eksempel på en databehandlersituasjon er regnskapsføreroppdrag.

I de nevnte tilfellene vil revisjonsforetaket behandle personopplysninger *på vegne av* klienten, for å bistå klienten med å utføre sine plikter etter regnskaps- og bokføringslovgivningen, skattebetalingsloven, skatteforvaltningsloven mv. Da må partene inngå en databehandleravtale.

Plikt til å informere de registrerte om behandlingen av personopplysninger

Når det behandles personopplysninger, skal den registrerte i utgangspunktet motta informasjon fra den behandlingsansvarlige. Dette følger av GDPR artikkel 13 og 14.

For å oppfylle informasjonsplikten skal revisjonsforetaket utarbeide en personvernerklæring. Denne bør publiseres på revisjonsforetakets hjemmeside. Personvernerklæringen skal blant annet beskrive kategoriene av personopplysninger som vil eller

kan bli brukt i forbindelse med revisors oppdrag og formålet med bruken. Personvernerklæringen skal også angi kontaktinformasjon til personvernansvarlig i revisjonsforetaket, eller personvernombud hvis revisjonsforetaket har det.

Veiledningen anbefaler at personvernerklæringen gjøres kjent for klienten.

Lagring av personopplysninger

Revisjonsforetaket må sørge for at personopplysningene ikke lagres lenger enn nødvendig for å oppfylle formålet de er innhentet for. I noen tilfeller er det fastsatt i lov hvor lenge det er nødvendig å lagre personopplysningene. Når lagringstidene ikke følger av lov, må revisjonsforetaket selv ta stilling til hvor lenge det er nødvendig å lagre personopplysningene, og dokumentere disse vurderingene i egne interne sletteregler og/eller i protokollen over behandlingsaktiviteter etter GDPR artikkel 30.

Etter revisorloven § 5–5 skal oppdragsdokumentasjon lagres i minst ti år. Når lagringstiden er utløpt, må revisjonsforetaket eventuelt ha et annet behandlingsgrunnlag for fortsatt å lagre oppdragsdokumentasjon som inneholder personopplysninger.

Etter hvitvaskingsloven § 30 første ledd skal revisjonsforetaket lagre opplysninger og dokumenter som er innhentet og utarbeidet i forbindelse med kundetiltak i fem år etter at kundeforholdet ble avsluttet eller transaksjonen ble gjennomført. Når femårsfristen er utløpt, skal personopplysningene slettes.

Når oppdraget ikke er regulert av revisorloven, kan de registrerte i utgangspunktet kreve personopplysninger slettet når opplysningene ikke lenger er nødvendige for å følge opp oppdraget forsvarlig. Hvis opplysningene er nødvendige for å forsvare seg mot erstatningskrav eller anklager, kan det gi revisor rettslig grunnlag for å beholde opplysningene lenger.

Hvordan sikre tilstrekkelig personopplysningssikkerhet?

GDPR har generelle bestemmelser om personopplysningssikkerhet. Revisjonsforetaket må blant annet gjennomføre risikovurderinger, og deretter etablere egnede tekniske og organisatoriske tiltak for å sikre og dokumentere at behandlingen av personopplysninger er i samsvar med personopplysningsregelverket. Med så overordnede regler, er det opp til revisjonsforetaket selv å vurdere hva som er et egnet sikkerhetsnivå. Denne vurderingen må baseres på momenter som personopplysningens art, omfang, den tekniske utviklingen og gjennomføringskostnadene.

Veiledningen angir at et tilfredsstillende personopplysningssikkerhetsnivå skal ivaretas som en del av kvalitetsstyringen etter revisorloven § 5b-1 om intern kvalitetskontroll og den internasjonale standarden for kvalitetsstyring i revisjonsforetak (ISQC 1). Informasjonssikkerheten må ivareta både revisjonsforetakets taushetsplikt etter revisorloven og personopplysningssikkerheten etter personvernregelverket.

Tilgangskontroll er et viktig tiltak for å ivareta personopplysningssikkerheten. Revisjonsforetaket må sørge for at brukere av fagsystemer, kundesystemer og regnskapssystemer kun har tilgang til områder eller personopplysninger som er nødvendig for å utføre oppdraget. Personer som ikke har et saklig behov for opplysningene, skal ikke ha tilgang.

Videre gir veiledningen andre eksempler på egnede tekniske og organisatoriske tiltak:

- Ekstern tilkobling til arbeidsplassen skjer gjennom kryptert VPN-tunnel eller lignende sikkerhetstiltak.
- Mobilt utstyr med jobb-e-post har automatisk tastelås etter kort tid.
- Det skal brukes tilgangskontroller for å sikre at tilgang til personopplysninger og annen taushetsbelagt informasjon begrenses til det som er nødvendig for forsvarlig og effektiv gjennomføring av revisors oppdrag.
- Rutiner som sikrer at mellomlagrede personopplysninger blir slettet fra mellomlageret innen rimelig tid. Personopplysningene skal flyttes til revisjonsverktøyet når det er nødvendig å oppbevare dem.

Hvis revisjonsforetaket benytter en databehandler til å lagre eller på annen måte behandle personopplysninger, for eksempel leverandør av revisjonsverktøy eller regnskapssystem, skal det inngås en databehandleravtale. Gjennom avtalen skal databehandleren gi tilstrekkelige garantier for at personopplysnings- og informasjonssikkerhet ivaretas.

Hvordan håndtere personopplysninger på e-post?

Et praktisk spørsmål som oppstår i forbindelse med personopplysningssikkerhet, er hvordan man skal håndtere sending og mottak av personopplysninger på e-post. Veiledningen angir generelt at revisjonsforetaket må implementere tiltak som bidrar til at sending og mottak av taushetsbelagt informasjon skjer på en forsvarlig måte, og videre at kryptering og lignende tiltak skal anvendes når det må anses som alminnelig praksis i bransjen.

Datatilsynet har gitt uttrykk for at e-postkommunikasjon av sensitive personopplysninger må være kryptert. Et revisjonsforetak som behandler taushetsbelagte opplysninger, herunder personopplysninger, bør sørge for at e-poster er kryptert, for eksempel ved «tvungen» eller «foretrukket» Transport Layer Security (TLS). «Tvungen» TLS innebærer at ingen e-post slipper ut dersom krypteringsløsningen hos avsender eller mottaker feiler, og at kun krypterte mail flyter mellom serverne. «Foretrukket» TLS betyr at ved sending av e-post sjekkes serveren hos mottaker, og e-posten sendes kryptert kun dersom mottaker har implementert tilsvarende løsning. Ulike varianter av slike krypteringsverktøy er tatt i bruk hos de fleste foretak.

Videre bør ikke personopplysninger lagres ustrukturert i ansattes e-postinnbokser i større grad enn nødvendig. E-poster som inneholder personopplysninger, bør derfor flyttes til revisjonsverktøyet så snart som mulig.