revisorforeningen

Bransjenorm for behandling av personopplysninger i revisjonsbransjen

Utkast oversendt Datatilsynet for vurdering og godkjenning etter GDPR artikkel 40 nr. 5

Versjon:	1.0
Versjonsdato:	28.06.2018
Godkjent av Datatilsynet	xx.xx.2018

Den norske Revisorforening
Postboks 2914 Solli • 0230 OSLO • Henrik Ibsens gate 100 • Telefon: 23 36 52 00
post@revisorforeningen.no • revisorforeningen.no • NO 980 374 092 MVA

Innhold

Del I - Innledning

1 Anvendelsesområde

Bransjenormen gjelder overholdelse av personvernreglene ved aksept og utførelse av revisjon og forenklet revisorkontroll av regnskaper, samt andre attestasjonsoppdrag og avtalte kontrollhandlinger.

I tillegg omhandler bransjenormen kapittel 9 og 10 overholdelse av personvernreglene ved levering av andre tjenester enn de som er nevnt ovenfor.

Anvendelse av denne bransjenormen forutsetter kjennskap til de sentrale elementene i personvernreglene.

Bransjenormen omhandler ikke behandling av personopplysninger i forbindelse med håndtering av personalmessige forhold, markedsføring, leverandører og annet som gjelder drift av revisjonsforetaket. Dette må håndteres i revisjonsforetak på samme måte som i andre foretak.

1.1 Personopplysninger og bedriftsrelaterte opplysninger

Personvernreglene gjelder når revisor behandler personopplysninger. Når revisor behandler bedriftsrelaterte opplysninger, gjelder de ikke. Revisor vil i noen grad måtte innhente personopplysninger for å utføre sine oppdrag. Revisors taushetsplikt innebærer krav om forsvarlig informasjonssikkerhet både for personopplysninger og bedriftsrelaterte opplysninger. Den registrertes rettigheter etter personvernreglene gjelder egne personopplysninger, og ikke bedriftsopplysninger revisor har innhentet fra den registrerte.

2 Definisjoner

Behandling: Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

Personvernreglene gjelder ikke for manuell behandling av personopplysninger som ikke inngår eller skal inngå i et register.

Som behandling regnes ikke situasjoner der revisor ser informasjon som inneholder personopplysninger (eksempelvis et vedtak), forutsatt at personopplysningene ikke registreres i oppdragsdokumentasjonen.

Behandlingsansvarlig: Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal benyttes. Det er revisjonsforetaket, representert ved øverste administrative leder, som eventuelt er behandlingsansvarlig.

Databehandler: En som behandler personopplysninger på vegne av den behandlingsansvarlige.

Databehandleravtale: En avtale hvor gjenstand for og varighet i behandlingen, behandlingens art og formål, typen personopplysninger og kategorier av registrerte samt den behandlingsansvarliges rettigheter og plikter er fastsatt. Databehandleravtalen kan være en integrert del av oppdragsavtalen som inngås eller være en selvstendig avtale.
Den registrerte(s): Den fysiske personen personopplysningen kan knyttes til.
Personopplysninger: Enhver opplysning om en identifisert eller identifiserbar fysisk person (den registrerte). Se også GDPR artikkel 4 nr. 1 og punkt 1.1 ovenfor.**Personvernansvarlig:** En person som er utpekt som revisjonsforetakets ansvarlige for etterlevelse av personvernreglene og denne bransjenormen, og til å være kontaktperson for eksterne parter i den forbindelsen. Dette kan være daglig leder eller en annen denne har utpekt.

Personvernansvarlig etter denne bransjenormen er ikke det samme som personvernombud etter GDPR artikkel 37. Et revisjonsforetak som frivillig har utpekt et personvernombud etter GDPR artikkel 37, trenger ikke utpeke en personvernansvarlig.

Personvernreglene: Personopplysningsloven (lov 15. juni 2018 nr. 38) og forordning (EU) 2016/679 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (personvernforordningen – GDPR). Personopplysningsloven § 1 fastsetter at GDPR gjelder som lov i Norge (inkorporasjon).

Revisjonsforetak: Et revisjonsselskap eller en revisor som driver revisjonsvirksomhet gjennom et enkeltpersonforetak.

Revisors oppdrag: Avtale om utførelse av revisjon eller forenklet revisorkontroll av regnskaper, andre attestasjonsoppdrag og avtalte kontrollhandlinger.

Revisjonsoppdrag: Revisjon av årsregnskap (selskapsregnskap og konsernregnskap).

Sikkerhetsbrudd: Brudd på informasjonssikkerheten (personopplysningssikkerheten) som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

Særlige kategorier personopplysninger: Opplysninger om:

- rasemessig eller etnisk opprinnelse,
- politisk oppfatning,
- religiøs eller filosofisk overbevisning,
- fagforeningsmedlemskap,
- genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person,
- helseopplysninger og
- opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Del II – Revisors oppdrag

3 Forholdet mellom personvernreglene og revisorloven mv.

Personvernreglene fastsetter regler for vern av fysiske personer i forbindelse med behandling av personopplysninger. Revisorloven regulerer revisors oppgaver og plikter ved

revisjon av årsregnskap og utførelse av de fleste attestasjonsoppdrag og avtalte kontrollhandlinger, se punkt 5.1.

Revisorloven § 5b-1 om etablering av forsvarlige systemer for intern kvalitetskontroll og den internasjonale standarden om kvalitetsstyring i revisjonsforetak (ISQC 1), vil også gjelde for revisjonsforetakenes overholdelse av personvernreglene, se kapittel 6.

3.1 Personopplysningssikkerhet

Bestemmelsene i revisorloven om taushetsplikt og betryggende oppbevaring av oppdragsdokumentasjon sikrer etterlevelse av kravene til personopplysningssikkerhet i personvernreglene.

Revisor og revisors medarbeidere har lovbestemt taushetsplikt om alt de under sin virksomhet får kjennskap til med mindre annet følger av lov. Taushetsplikten innebærer både et forbud mot å viderebringe opplysninger og en plikt til å hindre uautorisert tilgang til opplysningene.

Revisorloven krever at oppdragsdokumentasjonen skal oppbevares ordnet og på en betryggende måte, og sikret mot ødeleggelse, tap og endring, jf. revisorloven § 5-5 og revisorforskriften § 5-1.

Sikring av oppdragsdokumentasjonen skal ivareta tre formål:

- Tilgjengelighet - sikre tilgjengelighet for autoriserte personer ved behov.
- Integritet - sikre nøyaktighet og fullstendighet, sikkerhet mot uautorisert endring og sporbarhet av endringer.
- Konfidensialitet - sikre at kun autoriserte brukere har tilgang.

3.2 Dataminimering

Ved utførelse av revisors oppdrag skal revisor foreta de kontrollhandlingene og innhente den informasjonen som er nødvendig for å kunne avgi sin uttalelse (revisjonsbevis). Revisor plikter å dokumentere innhentede revisjonsbevis. Dette følger av revisorloven § 5-2 om god revisjonsskikk og blant annet ISA 230 pkt. 5 som krever at revisor utarbeider dokumentasjon som gir et tilstrekkelig og hensiktsmessig grunnlag for revisors uttalelse. I tråd med dette skal den revisjonspliktige gi revisor adgang til å foreta de undersøkelser revisor finner nødvendig, og gi revisor adgang til de opplysninger denne krever for utførelsen av sitt oppdrag, jf. revisorloven § 5-2 tredje ledd.

Når revisor utarbeider oppdragsdokumentasjon skal personvernprinsippet om dataminimering følges. Prinsippet krever at personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålet de behandles for. Det innebærer at revisor ikke skal innhente og oppbevare personopplysninger i større utstrekning enn det som er nødvendig for at revisor skal kunne avgi sin uttalelse. Blant annet skal det ikke tas unødvendige kopier av materiale som er oppbevaringspliktig hos klienten.

3.3 Den registrertes rettigheter

Revisorlovens bestemmelser om taushetsplikt er ikke til hinder for at den registrerte får innsyn i egne personopplysninger. Dette følger av at den som opplysningene gjelder kan samtykke til at taushetsplikten ikke skal gjelde, jf. revisorloven § 6-1.

Den registrertes rett til informasjon, sletting og innsyn og forholdet til revisorloven, er omtalt i kapittel 7.

4 Behandlingsansvarlig og databehandler

Revisjonsforetaket er behandlingsansvarlig etter personvernreglene ved behandling av personopplysninger i forbindelse med utførelse av revisors oppdrag – revisjon og forenklet revisorkontroll av regnskaper samt andre attestasjonsoppdrag og avtalte kontrollhandlinger.

Formålet med slike oppdrag er at revisors uttalelse eller rapport skal gi økt tillit til de kontrollerte opplysningene. Revisor avgjør hvilke kontrollhandlinger som må utføres og hvilken informasjon som må innhentes som grunnlag for sin uttalelse eller rapport. Dette vil være en forutsetning både for oppdrag som reguleres av revisorloven, jf. lovkravet om å følge god revisjonsskikk, og andre av revisors oppdrag. Revisor bestemmer dermed formålet med behandlingen av de personopplysningene som måtte bli innhentet og hvilke hjelpemidler som skal benyttes, jf. GDPR artikkel 6 nr. 1 bokstav c.

Ved utførelse av andre tjenester, vil revisjonsforetaket etter forholdene kunne være behandlingsansvarlig eller databehandler, se kapittel 9 og 10.

4.1 Bruk av databehandler

Hvis revisjonsforetaket benytter en databehandler til å lagre eller på annen måte behandle oppdragsdokumentasjon, skal det inngås en databehandleravtale, se punkt 6.2.

5 Behandlingsgrunnlag

For at det skal være tillatt å behandle personopplysninger må det foreligge et gyldig behandlingsgrunnlag. Når revisor er behandlingsansvarlig, må revisor påse at det foreligger et gyldig behandlingsgrunnlag. Behandlingsgrunnlagene for utførelse av revisors oppdrag er:

- *GDPR artikkel 6 nr. 1 bokstav c – rettslig forpliktelse*: Behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige.
    - Revisorloven, se punkt 5.1
    - Hvitvaskingsloven, se punkt 5.2
- *GDPR artikkel 6 nr. 1 bokstav f – interesseavveining*: Innhenting og oppbevaring av personopplysninger er nødvendig for å ivareta de berettigede interessene til revisjonsforetaket eller en klient, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysningene.

Disse behandlingsgrunnlagene omtales nærmere nedenfor.

5.1 Revisorloven

Revisorloven er behandlingsgrunnlag for behandling av personopplysninger i forbindelse med revisors oppdrag som reguleres av revisorloven, jf. GDPR artikkel 6 nr. 1 bokstav c. Etter revisorloven § 1-1 gjelder loven for alle revisjonsoppdrag, både for revisjonspliktige og frivillig revisjon. Revisorloven gjelder også for attestasjonsoppdrag og avtalte kontrollhandlinger hvor revisor bekrefter opplysninger overfor offentlige myndigheter eller utfører forenklet revisorkontroll etter aksjeloven §§ 7-7 til 7-9. Dette inkluderer revisorbekreftelser etter selskapslovgivningen.

For andre attestasjonsoppdrag og avtalte kontrollhandlinger er behandlingsgrunnlaget interesseavveining etter GDPR art 6 nr. 1 bokstav f, se punkt 5.3 om dette behandlingsgrunnlaget.

5.2 Hvitvaskingsloven

Hvitvaskingsloven er revisors behandlingsgrunnlag for opplysninger som behandles i forbindelse med utførelse av kundekontroll og opplysninger som registreres om reelle rettighetshavere, jf. GDPR artikkel 6 nr. 1 bokstav c.

I Finanstilsynets veiledning om hvitvaskingsregler (rundskriv 24/2016) fremkommer det at: «Rapporteringspliktige kan, uten hinder av personopplysningsloven, registrere personopplysninger som er nødvendige for å overholde forpliktelsene etter hvitvaskingsregelverket». Det vil gjelde på samme måte etter personvernreglene.

5.3 Interesseavveining

For revisors oppdrag som ikke er regulert av revisorloven (punkt 5.1) eller revisors plikter etter hvitvaskingsloven (punkt 5.2), er revisors behandlingsgrunnlag en interesseavveining etter GDPR artikkel 6 nr. 1 bokstav f. Hvis revisor i disse tilfellene vurderer at klienten mangler et berettiget behov for revisors uttalelse, skal revisor ikke påta seg oppdraget. Et berettiget behov kan for eksempel være at klientens bankforbindelse ber om en uttalelse i forbindelse med et lån.

5.4 Særlige kategorier personopplysninger mv.

Behandling av særlige kategorier personopplysninger er i utgangspunktet forbudt. Når det behandles særlige kategorier av personopplysninger er kravene til personvern sterkere enn ellers.

Behandling av særlige kategorier personopplysninger krever at det foreligger et behandlingsgrunnlag (se punkt 5.1 – 5-3), samt at det må finnes et spesifikt unntak i personvernreglene.

GDPR artikkel 9 nr. 2 bokstav g gir revisor rett til å behandle særlige kategorier personopplysninger på revisors oppdrag som reguleres av revisorloven, jf. punkt 5.1. Behandlingen skal etter bestemmelsen sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser. Dette forutsetter at revisor utviser særlig forsiktighet ved behandling av særlige kategorier personopplysninger.

Straffbare forhold og lovovertredelser
Revisor innhenter og dokumenterer i enkelte tilfeller informasjon om straffbare forhold eller lovovertredelser som kan knyttes til bestemte personer og som ikke er alminnelig kjent. GDPR artikkel 10 gir revisor rett til å behandle slike personopplysninger på revisors oppdrag som reguleres av revisorloven.[1] Det forutsettes at revisor behandler slike personopplysninger med samme forsiktighet som særlige kategorier personopplysninger, se punkt 5.4.

6 Sikring av personvernet

6.1 Kvalitetsstyring – ISQC 1

Revisjonsforetaket skal gjennomføre tiltak for å sikre og påvise at revisjonsforetakets behandling av personopplysninger utføres i samsvar med personvernreglene, jf. GDPR artikkel 24.

Dette kravet skal ivaretas som en del av kvalitetsstyringen etter revisorloven § 5b-1 om intern kvalitetskontroll og den internasjonale standarden for kvalitetsstyring i revisjonsforetak (ISQC 1). Kravene i denne bransjenormen er derfor knyttet til de aktuelle punktene i ISQC 1.

Revisorloven § 5b-1 krever at et revisjonsforetak skal etablere forsvarlige systemer for intern kvalitetskontroll av revisjonsvirksomheten. Den internasjonale standarden for kvalitetsstyring i revisjonsforetak (ISQC 1) angir at revisjonsforetak skal etablere og vedlikeholde et kvalitetskontrollsystem som gir rimelig sikkerhet for at revisjonsforetaket og personalet etterlever relevante lovmessige og regulatoriske krav.[2] Dette inkluderer personvernreglene (ISQC 1.11).

ISQC 1 gjelder, i likhet med denne bransjenormen, ved utførelse av revisjon og forenklet revisorkontroll av regnskaper, samt andre attestasjonsoppdrag og avtalte kontrollhandlinger (ISQC 1.1 og 4).

6.2 Kravene

Denne bransjenormen krever at følgende ivaretas gjennom revisjonsforetakets ISQC 1-prosess. Kravene er angitt under overskriftene som er hentet fra den internasjonale standarden for kvalitetsstyring i revisjonsforetak (ISQC 1). Referanser til ISQC 1 er angitt i parentes.

[1] Revisorloven dekker kravet i artikkel 10 om at reguleringen skal sikre egnet vern av de registrertes rettigheter og friheter.

[2] Revisorloven § 5b-1 og ISQC 1 bruker begrepet «kvalitetskontroll». «Kvalitetsstyring» er mer dekkende for det som reguleres her, og denne bransjenormen bruker derfor dette begrepet.

- Lederansvar for kvalitetssikring i revisjonsforetaket (ISQC 1.18–19)
    - Daglig leder eller innehaver i revisjonsforetaket skal etablere retningslinjer og rutiner for å sikre at personopplysninger behandles i samsvar med denne bransjenormen. (ISQC 1.18)
    - Styret i revisjonsforetaket har det overordnede ansvaret for at det etableres slike retningslinjer og rutiner. (ISQC 1.18)
    - Revisjonsforetaket skal ha en personvernansvarlig. Den personvernansvarlige skal ha gjennomført opplæring innen personvernreglene, og skal oppdatere kompetansen ved behov, eksempelvis ved endringer i rettigheter og plikter i personvernreglene. Dersom revisjonsforetaket frivillig her utpekt personvernombud i samsvar GDPR artikkel 37 gjelder ikke kravet om å utpeke en personvernansvarlig. (ISQC 1.19)
- Aksept og fortsettelse av klientforhold og enkeltoppdrag (ISQC 1.26–28)
    - Før revisors oppdrag aksepteres må det foreligge et gyldig behandlingsgrunnlag. Er revisors oppdrag regulert av revisorloven, er det denne loven som utgjør behandlingsgrunnlaget, og det er ikke behov for nærmere vurdering av behandlingsgrunnlaget (punkt 5.1). Tilsvarende gjelder for kundekontroll etter hvitvaskingsloven (punkt 5.2).
    - En interesseavveining er behandlingsgrunnlag når revisors oppdrag ikke er regulert av revisorloven, jf. punkt 5.1 og 5.3. Revisor skal i disse tilfellene avstå fra å påta seg oppdraget hvis revisor vurderer at klienten mangler et berettiget behov for revisors uttalelse.
    - Revisor skal ha en personvernerklæring som beskriver revisors behandling av personopplysninger i forbindelse med revisors oppdrag. Se punkt 7.1.
    - Personvernerklæringen skal angi kontaktinformasjon til personvernansvarlig i revisjonsforetaket. Se punkt 7.1.
    - Personvernerklæringen skal gjøres kjent for klienten. Se punkt 7.1.
- Menneskelige ressurser (ISQC 1.29–31)
    - Revisjonsforetaket skal sikre seg at oppdragsansvarlige revisorer er kjent med sin plikt til å sørge for at personopplysninger behandles i samsvar med denne bransjenormen, samt revisjonsforetakets retningslinjer og rutiner for behandling av personopplysninger. (ISQC 1.30.c)
    - Revisjonsforetaket skal sørge for at medarbeidere på oppdrag er kjent med kravene i denne bransjenormen samt revisjonsforetakets retningslinjer og rutiner for behandling av personopplysninger. (ISQC 1.31)
- Gjennomføring av oppdrag (ISQC 1.32–47)
    - Det skal ikke innhentes og oppbevares personopplysninger i større utstrekning enn det som er nødvendig for å utføre revisors oppdrag. Se punkt 3.2.

- Revisjonsforetaket skal kartlegge systemene som benyttes for å behandle personopplysninger i forbindelse med utførelsen av revisors oppdrag (ISQC 1.46 og GDPR artikkel 30). Dette vil typisk være det elektroniske revisjonsverktøyet revisjonsforetaket benytter, mellomlagring på lokal eller ekstern server og mellomlagring på e-postserver.
- Personopplysninger skal behandles i samsvar med revisjonsforetakets retningslinjer og rutiner for å sikre konfidensialitet, trygg oppbevaring, integritet, tilgjengelighet og gjenfinnbarhet av oppdragsdokumentasjon. (ISQC 1.46).
- Revisjonsforetaket skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå informasjonssikkerhet som ivaretar taushetsplikten etter revisorloven og personopplysningssikkerhet etter personvernreglene. (ISQC 1.46 og GDPR artikkel 32). Eksempler på slike tiltak kan være:
  - Tiltak som bidrar til at sending og mottak av taushetsbelagt informasjon skjer på en forsvarlig måte. Kryptering og lignende tiltak skal anvendes når det må anses som alminnelig praksis i bransjen.
  - Ekstern tilkobling til arbeidsplassen skjer gjennom kryptert VPN-tunnel eller lignende sikkerhetstiltak.
  - Mobilt utstyr med jobb-epost 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.
- Etter utløpet av oppbevaringstiden i revisorloven, må revisor ha et annet behandlingsgrunnlag for fortsatt å kunne oppbevare oppdragsdokumentasjon som inneholder personopplysninger. (ISQC 1.47 og 32)
- Hvis noen ber om innsyn i egne personopplysninger, skal revisor gjøre rimelige undersøkelser for å finne ut om revisjonsforetaket har personopplysninger om den registrerte og i tilfelle informere om personopplysningene som er behandlet. Visse unntak fra dette er angitt i punkt 7.3.

- Overvåking (ISQC 1.48–56)
  - Revisjonsforetaket skal vurdere risikoen for uautorisert tilgang til personopplysninger, på samme måte som for annen informasjon som revisor har taushetsplikt om. (ISQC 1.48 og GDPR artikkel 32)
  - Hvis revisjonsforetaket benytter en databehandler til å lagre eller på annen måte behandle oppdragsdokumentasjon, skal det inngås en

databehandleravtale. Gjennom avtalen skal databehandleren gi tilstrekkelige garantier for at de vil gjennomføre egnede tiltak som sikrer at personopplysnings- og informasjonssikkerhet ivaretas i samsvar med revisors taushetsplikt og kravene i personvernreglene og denne bransjenormen.

- Personvernansvarlig i revisjonsforetaket skal se til at denne bransjenormen følges opp i foretaket. (ISQC 1.48.b). Daglig leder eller innehaver i revisjonsforetaket er personvernansvarlig hvis ikke noen andre er utpekt.

- Dokumentasjon av systemet for kvalitetsstyring (ISQC 1.57–59)
  - Revisjonsforetaket skal skriftlig dokumentere (ISQC 1.57):
    - Kartlegging av behandlingen av personopplysninger. Se vedlegg 2 – kartleggingsprotokoll
    - Gjennomførte risikovurderinger.[3]
    - Tekniske og organisatoriske tiltak som er gjennomført for å ivareta personopplysningssikkerhet (systemsikkerhet).
    - Rutiner for avvikshåndtering.
    - Eventuelle sikkerhetsbrudd.
      - Dokumentasjonen skal minst inneholde de faktiske forholdene rundt bruddet, virkningen av det og hvilke tiltak som er satt i verk for å utbedre det.
      - Krav om melding til Datatilsynet er omtalt i punkt 8.1
      - Krav om melding til de registrerte er omtalt i punkt 8.2.
    - Avtaler med databehandlere
    - Personvernerklæring

7 Den registrertes rettigheter

Personvernreglene gir den registrerte en rekke rettigheter. De rettighetene som er mest relevant for revisor er følgende:

- Informasjonsretten, GDPR artikkel 13 og 14
- Rett til sletting, GDPR artikkel 17

[3] Dette omfatter risikovurderinger etter GDPR artikkel 24 og 32. Artikkel 35 om vurdering av personvernkonsekvenser anses ikke aktuell for **revisors oppdrag**. Slik **behandling** av **personopplysninger** medfører ikke høy risiko for fysiske personers rettigheter og friheter.

- Innsynsretten, GDPR artikkel 15

Ivaretakelse av andre rettigheter som den registrerte har etter GDPR kapittel III ved utførelse av revisors oppdrag:

- Uriktige personopplysninger korrigeres i den grad det er tillatt etter revisorloven. Den registrerte vil ikke kunne kreve korrigering eller begrensning i strid med revisorlovens krav til utførelse og dokumentasjon av oppdraget.
- Den registrertes rett til å protestere mot behandling av personopplysninger (innsigelsesrett) gjelder ikke for revisors oppdrag som omfattes av revisorloven og kundeopplysninger som registreres etter hvitvaskingsloven. Innsigelsesretten på revisors oppdrag som ikke er omfattet av revisorloven, ivaretas i samsvar med retten til sletting etter punkt 7.2.
- Revisors taushetsplikt er til hinder for å viderebringe personopplysninger. Plikten til å underrette andre som har mottatt personopplysninger er derfor ikke aktuell.
- Rett til dataportabilitet er ikke aktuell fordi dette bare gjelder når behandlingsgrunnlaget er samtykke eller avtale.
- Revisor treffer ikke avgjørelser om personer ved utførelsen av revisors oppdrag. Rettigheter i forbindelse med automatiserte avgjørelser er derfor ikke aktuelle.

7.1 Informasjonsretten

Når det behandles personopplysninger, skal den registrerte i utgangspunktet motta informasjon fra den behandlingsansvarlige (GDPR artikkel 13 og 14). I den grad det samles inn personopplysninger i forbindelse med revisors oppdrag, hentes disse inn fra klienten og enkelte andre kilder, og kun unntaksvis direkte fra den registrerte. Når personopplysningene ikke innhentes fra den registrerte direkte er det upraktisk og det vil ikke stå i forhold til behovet for personvern, om revisor skulle informere den enkelte registrerte direkte. Revisor kan derfor unnlate å informere på denne måten i henhold til GDPR artikkel 14 nr. 5 bokstav b og c.

Gyldig legitimasjon i forbindelse med kundekontroll etter hvitvaskingsloven, må hentes inn direkte fra den registrerte. Dette gjelder for daglig leder eller ev. en annen som handler på vegne av klienten i forbindelse med revisors oppdrag. Disse må nødvendigvis være godt informert om hvem revisor er og hvorfor revisor ber om opplysningene, jf. GDPR artikkel 13.

For å etterleve informasjonsretten skal revisjonsforetaket utarbeide en personvernerklæring. Denne bør publiseres på revisjonsforetakets hjemmeside. Personvernerklæringen skal beskrive de typer personopplysninger som vil eller kan bli innhentet i forbindelse med revisors oppdrag og formålet med innhentingen. Personvernerklæringen skal også angi kontaktinformasjon til personvernansvarlig i revisjonsforetaket, eller personvernombud hvis revisjonsforetaket har det. Informasjon om hvem som er revisor for et foretak, er offentlig tilgjengelig i årsregnskapet og i Enhetsregisteret.

Personvernerklæringen skal gjøres kjent for klienten.

7.2 Rett til sletting

Den registrerte har rett til å få slettet personopplysninger som ikke lenger er nødvendige for formålet som de ble samlet inn eller behandlet for.

Etter revisorloven § 5-5 skal oppdragsdokumentasjon oppbevares i minst ti år. Etter utløpet av oppbevaringstiden, må revisor eventuelt ha et annet behandlingsgrunnlag for fortsatt å oppbevare oppdragsdokumentasjon som inneholder personopplysninger, jf. GDPR artikkel 17.

Etter hvitvaskingsloven § 22 første ledd skal revisor (den rapporteringspliktige) oppbevare kopier av dokumenter benyttet i forbindelse med kundekontroll som nevnt i hvitvaskingsloven § 7, samt registrerte opplysninger som nevnt i hvitvaskingsloven § 8, i fem år etter at kundeforholdet er avsluttet eller transaksjonen er gjennomført. Opplysningene skal slettes innen ett år etter at oppbevaringsplikten opphører.

Når oppdraget ikke er regulert av revisorloven, kan personopplysninger i utgangspunktet kreves slettet når personopplysningene 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 en berettiget interesse i å beholde opplysningene lenger, jf. GDPR artikkel 6 nr. 1 bokstav f.

7.3 Innsynsretten

Revisorlovens bestemmelser om taushetsplikt hindrer ikke at den registrerte får innsyn i egne personopplysninger (se punkt 3.3).

Hvis noen ber om innsyn i egne personopplysninger, opplyser revisor om de typer personopplysninger som kan bli innhentet i forbindelse med revisors oppdrag og formålet med innhentingen.

Revisor skal gjøre rimelige undersøkelser for å finne ut om revisjonsforetaket har personopplysninger om den registrerte og i tilfelle informere om personopplysningene som er behandlet.

Etter GDPR artikkel 12 nr. 5 kan revisjonsforetaket nekte å etterkomme åpenbart grunnløse eller overdrevne anmodninger. Den behandlingsansvarlige skal bære bevisbyrden for at en anmodning er åpenbart grunnløs eller overdreven. Anmodningen vil være åpenbart grunnløs hvis det ikke er noen reell mulighet for at revisjonsforetaket har personopplysninger om vedkommende. Anmodningen vil være overdreven hvis informasjon etter annet avsnitt ovenfor må anses tilstrekkelig sett i forhold til byrdene med å undersøke om revisjonsforetaket har personopplysninger og vedkommendes interesse i å få innsyn hos revisjonsforetaket.

Revisor kan unnlate å gi innsyn i vurderinger av personers kompetanse og integritet som dokumenteres i forbindelse med revisors oppdrag, jf. personopplysningsloven § 16 første ledd bokstav e. Revisor skal i tilfelle opplyse skriftlig at det kan være nødvendig å vurdere personers kompetanse og integritet for å utføre revisors oppdrag og at innsyn ikke gis fordi revisors vurdering skal være uavhengig av muligheten til innsyn. Revisor skal vise til personopplysningsloven § 16 første ledd bokstav e.

8 Avvikshåndtering

Etter personvernreglene skal revisjonsforetaket ha rutiner og retningslinjer som sikrer håndtering av avvik.

8.1 Melding til Datatilsynet

Sikkerhetsbrudd skal meldes til Datatilsynet uten ugrunnet opphold, og når det er mulig, senest 72 timer etter å ha fått kjennskap til det. Meldeplikten gjelder ikke dersom det er lite trolig at bruddet vil medføre en risiko for fysiske personers rettigheter og friheter. Dersom bruddet ikke meldes til Datatilsynet innen 72 timer, skal årsaken til forsinkelsen oppgis. Meldingen skal minimum beskrive sikkerhetsbruddet, sannsynlige konsekvenser av sikkerhetsbruddet, hvilke tiltak som er eller vil bli iverksatt, og navnet på revisjonsforetakets personvernansvarlig eller personvernombud, jf. GDPR artikkel 33 nr. 3.

Dersom et sikkerhetsbrudd ikke meldes som følge av at det er lite trolig at bruddet vil medføre en risiko for fysiske personers rettigheter og friheter, skal revisjonsforetaket dokumentere begrunnelsen for dette.

8.2 Melding til den registrerte

Et revisjonsforetak behandler i utgangspunktet ikke personopplysninger som kan medføre høy risiko for fysiske personer rettigheter og friheter ved et eventuelt sikkerhetsbrudd. Hvis det likevel er sannsynlig at et sikkerhetsbrudd vil medføre høy risiko for fysiske personers rettigheter og friheter, skal revisjonsforetaket uten ugrunnet opphold underrette den registrerte om bruddet i samsvar med GDPR artikkel 34. Ved usikkerhet bør revisjonsforetaket søke Datatilsynet for råd og bistand.

8.3 Dokumentasjon av sikkerhetsbrudd

Revisjonsforetaket skal dokumentere sikkerhetsbrudd. Dokumentasjonen skal minst inneholde de faktiske forholdene rundt bruddet, virkningen av det og hvilke tiltak som er satt i verk for å utbedre det. Ved sikkerhetsbrudd plikter revisjonsforetaket videre å vurdere og dokumentere konsekvensene for de registrerte.

Del III – Andre tjenester

Revisjonsforetak behandler i noen grad personopplysninger også når de utfører andre tjenester enn revisors oppdrag.

9 Andre tjenester til revisjonsklienter

9.1 Felles for andre tjenester til revisjonsklienter

Revisor er behandlingsansvarlig ved utførelse av revisjonsoppdrag, se kapittel 4. Ved utførelse av andre tjenester for egne revisjonsklienter, er revisor behandlingsansvarlig hvis personopplysningene som innhentes har betydning både for revisjonen og den andre tjenesten.

Rollen som behandlingsansvarlig for revisjonsoppdraget skilles dermed ikke fra den behandlingen som måtte være nødvendig for å utføre den andre tjenester.

Hvis revisor behandler personopplysninger som *ikke* har betydning for revisjonen, gjelder skillet mellom behandlingsansvarlig og databehandler som angitt i punkt 11.1. Revisor må anvende skjønn for å avgjøre om personopplysningene har betydning for revisjonen.

9.2 Årsoppgjørsoppdrag

Revisjonsforetaket er behandlingsansvarlig ved teknisk utarbeidelse av regnskap og skattemelding for egne revisjonsklienter, jf. punkt 10.1.1.

Revisorloven gir behandlingsgrunnlag, jf. GDPR artikkel 6 nr. 1 bokstav c og revisorforskriften § 4-3 nr. 1.

Behandlingsansvaret betyr at pliktene som er nevnt i del I gjelder på samme måte for denne tilleggstjenesten.

9.3 Aksjonærregisteroppgave

Revisjonsforetaket er behandlingsansvarlig ved teknisk utarbeidelse av aksjonærregisteroppgave for egne revisjonsklienter, jf. punkt 10.1.1.

GDPR artikkel. 6 nr. 1 bokstav f om interesseavveining gir behandlingsgrunnlag.

Behandlingsansvaret betyr at pliktene som er nevnt i del I gjelder på samme måte for denne tilleggstjenesten.

10 Tjenester til andre enn revisjonsklienter

10.1 Felles for tjenester til andre enn revisjonsklienter

Ved utførelse av andre tjenester enn revisors oppdrag for *andre* enn egne revisjonsklienter, vil revisjonsforetaket etter forholdene kunne være behandlingsansvarlig eller databehandler.

- Revisor er behandlingsansvarlige når det er revisor som avgjør hvilke opplysninger som er nødvendig å behandle for å utføre tjenesten.
- Revisor er databehandler når det er oppdragsgiver (behandlingsansvarlig) som avgjør hvilke opplysninger som skal behandles. Personopplysningene behandles på vegne av den behandlingsansvarlige.

Behandlingsgrunnlaget er avtale dersom denne inngås direkte med den registrerte. I andre tilfeller gir GDPR artikkel 6 nr. 1 bokstav f om interesseavveining revisor behandlingsgrunnlag.

Når revisjonsforetaket er databehandler er det databehandleravtalen som gir behandlingsgrunnlag.

Nedenfor omtales enkelte tjenester som er praktisk viktige for revisorer.

10.2 Regnskapsføring

Når revisor utfører regnskapsføreroppdrag, herunder årsoppgjørsoppdrag, lønnsoppdrag mv., er revisjonsforetaket databehandler. Eventuelle personopplysninger behandles på vegne av oppdragsgiver for å utføre oppdragsgiverens plikter etter regnskaps- og bokføringslovgivningen, skattebetalingsloven, skatteforvaltningsloven mv.
Regnskap Norge, Økonomiforbudet og Revisorforeningen har sammen utarbeidet en bransjenorm («adferdsnorm») for regnskapsførerbransjen. Denne skal benyttes når revisjonsforetaket utfører regnskapsføreroppdrag.

10.3 Due diligence (selskapsgjennomgang)

Due diligence (selskapsgjennomgang) innebærer innsamling og analyse av informasjon om et selskap for å gi støtte til beslutninger og økt trygghet, ofte i forbindelse med fusjoner, oppkjøp eller andre strategiske endringer.

Revisjonsforetaket er derfor normalt behandlingsansvarlig ved due diligence-oppdrag, jf. punkt 10.1.

GDPR artikkel. 6 nr. 1 bokstav f om interesseavveining gir behandlingsgrunnlag.

Behandlingsansvaret betyr at pliktene som er nevnt i del I gjelder på samme måte.

10.4 Granskingsoppdrag

Granskingsoppdrag går ut på å klarlegge faktiske forhold og sammenhenger innenfor et angitt mandat. En rekke ulike forhold kan være gjenstand for gransking.

Revisjonsforetaket er derfor normalt behandlingsansvarlig ved granskingsoppdrag, jf. punkt 11.1.

GDPR artikkel. 6 nr. 1 bokstav f om interesseavveining gir behandlingsgrunnlag.

Behandlingsansvaret betyr at pliktene som er nevnt i del I gjelder på samme måte.

10.5 Internrevisjon

Internrevisjon er en del av et selskaps internkontroll, og det er styret i selskapet som fastsetter internrevisjonens formål, fullmakter og ansvarsområder. Revisor avgjør hvilke opplysninger som skal innhentes for å utføre oppdraget. Revisjonsforetaket er derfor normalt behandlingsansvarlig ved oppdrag om internrevisjon, jf. punkt 11.1.

GDPR artikkel. 6 nr. 1 bokstav f om interesseavveining gir behandlingsgrunnlag.

Behandlingsansvaret betyr at pliktene som er nevnt i del I gjelder på samme måte.