Bransjenorm for behandling av personopplysninger i revisjonsbransjen

25. mai 2018 skal personvernforordningen (GDPR) etter planen tre i kraft. Revisorforeningen arbeider med en bransjenorm for revisjonsbransjen. Den skal hjelpe revisjonsselskapene med å etterleve personvernreglene og bidra til å dokumentere dette. Her får du en oversikt over hva det er tenkt at bransjenormen skal inneholde.

Statsautorisert revisor
Erik Avlesen-Østli
Rådgiver i Revisorforeningen

Dette handler artikkelen om

Revisorforeningen arbeider med en bransjenorm for revisjonsbransjen hvor formålet er å klargjøre hvordan personvernreglene skal praktiseres i bransjen. Bransjenormen skal bidra til forsvarlig behandling av personopplysninger, samt gjøre det enklere å dokumentere at reglene etterleves. Bransjenormen vil fokusere på revisors behandling av personopplysninger i forbindelse med gjennomføring av revisjonsoppdrag og andre attestasjonsoppdrag. Bransjenormen vil fokusere på de sidene ved GDPR som har særlig betydning for et revisjonsforetak.

Uavhengig av når GDPR blir gjennomført i Norge og når bransjenormen foreligger, er det god grunn til å starte forberedelsene nå. Det er viktig å skaffe seg en oversikt over hvilke personopplysninger som behandles av revisjonsselskapet og vurdere risikoene for personvernet som behandlingen medfører. Risikovurderinger som tidligere er gjort i forbindelse med tiltak for å sikre informasjon, vil kunne være relevante her.

GDPR og revisorloven

Revisjonsoppdrag må utføres i samsvar med reglene i revisorloven og god revisjonsskikk. For å kunne uttale seg om årsregnskapet er det som oftest nødvendig at revisor innhenter og dokumenterer opplysninger om personer (behandler personopplysninger). Personvernforordningen (GDPR) gjelder også i disse tilfellene, men for flere av bestemmelsene i forordningen har det betydning at behandlingen av personopplysninger er nødvendig etter annen lovgivning. Bransjenormen skal klargjøre samspillet mellom GDPR og revisorloven.

Reglene i revisorloven om taushetsplikt og oppbevaring av dokumentasjon skal sikre at informasjon behandles forsvarlig og at opplysninger ikke kommer på avveie. Overholdelse av disse pliktene ivaretar derfor langt på vei formålene i GDPR. I tillegg er ISQC 1, standarden for kvalitetsstyring av en revisjonsvirksomhet, relevant i denne sammenhengen. Dersom disse reglene etterleves, er revisjonsforetakene et godt stykke på vei til å etterleve reglene i GDPR.

Behandling av personopplysninger

Behandling

I praksis omfatter «behandling» all befatning med personopplysninger. Eksempelvis innsamling, registrering, strukturering, lagring og sletting. Manuell behandling av personopplysninger er ikke omfattet av GDPR, med mindre opplysningene inngår eller skal inngå i et register.

Personopplysning

Forordningens definisjon av en personopplysning er vid. En personopplysning er «enhver opplysning om en identifisert eller identifiserbar fysisk person». En identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator. En identifikator er f.eks. personens navn.

En sentral del av definisjonen er at det må være en opplysning om en person. Det er derfor et skille mellom personopplysninger og bedriftsrelaterte opplysninger. Dette skillet er viktig for revisor, og skal tydeliggjøres i bransjenormen. Bedriftsrelaterte opplysninger er ikke omfattet av GDPR. I bransjenormen vil det derfor være sentralt å

En personopplysning er «enhver opplysning om en identifisert eller identifiserbar fysisk person».

Bransjenorm for revisjonsbransjen

En bransjenorm er et regelsett for en spesifikk bransje. Den skal gi konkrete regler og retningslinjer for hvordan virksomhetene skal innrette seg for å etterleve kravene i GDPR.[1]

I fjerde kvartal 2017 startet Revisorforeningen arbeidet med bransjenormen for behandling av personopplysninger i revisjonsbransjen. Det er opprettet en arbeidsgruppe bestående av jurister og revisorer, med representanter fra revisjonsselskapene. Målsettingen er at det skal foreligge et utkast innen utgangen av mai 2018. Bransjenormen skal godkjennes av Datatilsynet.

Formålet med bransjenormen for revisjonsbransjen er å klargjøre hvordan personvernreglene[2] skal praktiseres i bransjen. Bransjenormen skal bidra til at revisjonsselskapene behandler personopplysninger på en forsvarlig måte, og gjøre det enklere for revisjonsselskapene å dokumentere etterlevelse av kravene i GDPR. Bransjenormen vil klargjøre samspillet mellom revisorloven og GDPR.

Bransjenormen vil fokusere på revisors behandling av personopplysninger ved utførelse av revisjonsoppdrag og andre attestasjonsoppdrag. Den skal gi konkrete regler og retningslinjer på en del revisjonsspesifikke problemstillinger, hvor målet er å beskrive praktiske, etterlevbare og gode løsninger for revisjonsbransjen.

I forbindelse med arbeidet med bransjenormen er planen å utarbeide et eksempel på personvernerklæring og databehandleravtale, samt oppdatere engasjementsbrevet.

Det kan også nevnes at Regnskap Norge, Økonomiforbundet og Revisorforeningen arbeider med en bransjenorm for regnskapsførerbransjen.

1 www.datatilsynet.no/regelverk-og-skjema/veiledere/korleis-lage-bransjenorm/?id=8022
2 Personopplysningsloven. GDPR er foreslått gjennomført i norsk rett gjennom inkorporasjon – en henvisning til forordningen.

tydeliggjøre hva som anses som personopplysninger og hva som anses som bedriftsrelaterte opplysninger i typiske situasjoner revisor står overfor. Når revisor utfører revisjonsoppdrag, er det vesentligste av opplysningene som innhentes, opplysninger om revisjonsklienten – ikke om menneskene i eller i tilknytning til revisjonsklienten.

Eksempelvis er det ønskelig å avklare om det er anledning til å regne intervjuer av ansatte hos revisjonsklienten for å kartlegge selskapets rutiner eller for å innhente revisjonsbevis, som bedriftsrelaterte opplysninger. Selv om revisor noterer navn og kanskje vedkommendes stilling i sine arbeidspapirer, er opplysningene som innhentes ikke om personen, men om revisjonsklienten.

Revisor må verne både bedriftsrelaterte opplysninger og personopplysninger, men dersom opplysningen ikke regnes som en personopplysning, har dette betydning for den registrertes rettigheter. Mer om dette nedenfor.

Behandlingsgrunnlag

For at det skal være tillatt å behandle personopplysninger, må det foreligge et gyldig behandlingsgrunnlag. Det er derfor viktig å ha et bevisst forhold til behandlingsgrunnlaget forut for behandlingen. Bransjenormen skal klargjøre revisors behandlingsgrunnlag i ulike situasjoner.

Hva som utgjør et gyldig behandlingsgrunnlag, avhenger av hvilket oppdrag revisor skal utføre. Når revisor utfører revisjonsoppdrag og andre attestasjonsoppdrag, er behandlingsgrunnlaget revisorloven. GDPR tillater behandling av personopplysninger når det er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige (revisjonsselskapet). Når revisor reviderer et årsregnskap, er det nødvendig for revisor å behandle

Personvernforordningen – General Data Protection Regulation (GDPR)

Personvernforordningen, eller General Data Protection Regulation (GDPR), inneholder regler for vern av fysiske personer i forbindelse med behandling av personopplysninger. Regler om personvern er ingen nyhet i norsk rett. Den gjeldende personvernloven trådte i kraft i 2001.

På samme måte som at regler om personvern ikke er nytt i norsk rett, er vern av opplysninger generelt, ikke nytt for revisor. Det ligger i revisors grunnholdning at opplysninger som er innhentet i forbindelse med revisjon og andre oppdrag, skal beskyttes. Dette vil også omfatte personopplysninger. For revisjons- og attestasjonsoppdrag bidrar reglene i revisorloven et godt stykke på vei til å etterleve reglene i GDPR.

De fleste revisjonsforetakene har nok likevel en jobb å gjøre for å bli i samsvar med GDPR. Dette er noe som må prioriteres av alle. Forsvarlig personvern er viktig for tilliten til revisorer og revisjon.

Nylig ble det kjent at gjennomføring av GDPR i norsk rett trolig blir litt forsinket, men dette bør ikke være en hvilepute – for reglene kommer. Tidspunktet for ikrafttredelsen av GDPR i Norge er en viktig dato, men minst like viktig er det at det arbeides med personvern i revisjonsselskapet og at dette gjøres til en kontinuerlig jobb i fremtiden.

Bransjenormen skal klargjøre samspillet mellom GDPR og revisorloven.

personopplysninger for å kunne oppfylle sine plikter etter revisorloven.

Tilsvarende vil hvitvaskingsloven være revisors behandlingsgrunnlag når revisor foretar pliktige undersøkelser etter hvitvaskingsloven. Et annet eksempel på et gyldig behandlingsgrunnlag er forskrift til skatteforvaltningsloven i de tilfellene revisor plikter å attestere Lønns- og pensjonskostnader/kontrolloppstillingen (RF-1022).

Når revisor er databehandler (behandler data på vegne av den behandlingsvarlige), er det databehandleravtalen som gir revisor rett til å behandle personopplysningene.

Behandlingsansvarlig eller databehandler

Bransjenormen skal klargjøre når revisor er behandlingsansvarlig og når revisor er databehandler. Dette avhenger av oppdraget som revisor utfører.

Når revisor utfører revisjonsoppdrag og andre lovbestemte attestasjonsoppdrag, vil revisor alltid være behandlingsansvarlig for de personopplysningene som revisor finner nødvendig å innhente i forbindelse med gjennomføringen av oppdraget. Et revisjonsoppdrag har ikke som formål å behandle personopplysninger, men revisor må av og til behandle personopplysninger som ledd i utførelsen av revisjonen.

Når revisor innhenter og oppbevarer personopplysninger i forbindelse med utførelse av andre oppdrag, vil revisor kunne være databehandler. Eksempler på slike oppdrag er teknisk utarbeidelse av årsregnskap og skattemelding. Når revisor er databehandler, må det inngås skriftlig databehandleravtale med kunden, og revisor må gi tilstrekkelige garantier for at personvernreglene etterleves.

En tommelfingerregel er at revisor er behandlingsansvarlig hvis det er revisor som avgjør hvilken informasjon som det er nødvendig å innhente for å kunne avgi sin uttalelse eller utføre sitt oppdrag. I andre tilfeller er revisor databehandler.

Rutiner og intern kontroll

En rekke bestemmelser i personvernforordningen (GDPR) pålegger den behandlingsansvarlige å gjennomføre det som benevnes «egnede tekniske og organisatoriske tiltak». Blant annet skal det gjennomføres egnede tekniske og organisatoriske tiltak som sikrer og dokumenterer at behandlingen av personopplysningene gjennomføres i samsvar med reglene i GDPR (artikkel 24). Det skal også gjennomføres slike tiltak for å oppnå et nivå på personopplysningssikkerheten som er egnet i forhold til risikoen (artikkel 32). For å oppfylle kravene må det implementeres gode rutiner og en hensiktsmessig intern kontroll hos den som behandler personopplysninger.

For å kunne vurdere hvilke tekniske og organisatoriske tiltak som skal gjennomføres, er det en forutsetning at det i forkant gjennomføres en risikovurdering. I GDPR fremkommer det flere steder at det skal tas hensyn til risikoen for å krenke personers rettigheter og friheter i vurderingen av hvilke tiltak som skal gjennomføres.

For å kunne foreta en fornuftig risikovurdering, er det nødvendig å gjøre en kartlegging av hvilke personopplysninger som revisjonsforetaket behandler. Revisjonsforetaket må ha god oversikt over hvilke typer personopplysninger de behandler, og i hvilken sammenheng de behandles. Kartlegging betyr ikke å etablere nye registre eller systematisere personopplysningene i egne lister mv. Det vil være en ny og unødvendig behandling av personopplysningene.

Kartleggingen bør minimum omfatte:
- Hvilke prosesser som innebærer behandling av personopplysninger
- Hvilke typer personopplysninger som samles inn, herunder kategori (alminnelig eller særlig kategori)
- Formålet med behandlingen
- Behandlingsgrunnlaget
- Hvor behandlingen finner sted (typisk IT-system)
- Hvor personopplysningene oppbevares (fysisk og lokasjon), og eventuell bruk av databehandler

Bransjenormen vil inneholde veiledning om kartlegging av personopplysninger og implementering av rutiner og intern kontroll.

Personopplysningssikkerhet

Bransjenormen skal også omhandle personopplysningssikkerhet (informasjonssikkerhet). Personopplysninger skal ikke komme på avveie eller i gale hender. Personvernforordningen (GDPR) krever at behandlingsansvarlig og databehandler skal gjennomføre egnede tekniske og organisatoriske tiltak som reduserer risikoen for å krenke personvernet til et akseptabelt nivå. I denne vurderingen skal det særlig tas hensyn til risikoen for utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

En revisor må ha generelt god informasjonssikkerhet for å sikre at klientopplysninger behandles fortrolig i samsvar med taushetsplikten og kravene til sikker oppbevaring av dokumentasjon. Revisor må forsikre seg om at revisjonsdokumentasjonen til enhver tid er tilfredsstillende sikret. Det gjelder både for personopplysninger og forretningsopplysninger. Revisjonsklienten skal ha tillit til at informasjonssikkerheten ivaretas på en god måte av revisjonsselskapet. Disse tiltakene vil være relevante også for etterlevelsen av reglene i GDPR.

Den registrertes rettigheter

Personvernforordningen (GDPR) styrker rettighetene til de fysiske personene som opplysningene gjelder (den registrerte). Hvordan revisor skal forholde seg til disse rettighetene, vil bli behandlet i bransjenormen.

Informasjonsretten
Personer har krav på informasjon når det behandles personopplysninger om han eller henne. I forordningen skilles det på situasjoner hvor opplysninger innhentes direkte fra person og hvor opplysningene om personen innhentes fra andre. I begge situasjonene skal personen motta informasjon fra den behandlingsansvarlige. Personen skal ha informasjon om formålet med behandlingen, hvor lenge personopplysningene skal oppbevares og informasjon om sine rettigheter. GDPR gjør imidlertid enkelte unntak fra informasjonsretten. Blant annet i forbindelse med lovbestemt taushetsplikt i tilfeller opplysningene innhentes fra andre. Dette kan være aktuelt for revisorers behandling av personopplysninger, og vil bli behandlet i bransjenormen.

Innsynsretten
GDPR gir en person som henvender seg til en behandlingsansvarlig og anmoder om innsyn, rett til å få bekreftet om personopplysninger om vedkommende behandles, og i tilfelle, rett til innsyn i personopplysningene. Personen har da også rett til å motta informasjon om blant annet formålet med behandlingen, kategoriene av personopplysninger som behandles, oppbevaringstid og om hvor opplysningene stammer fra dersom de ikke er samlet inn direkte fra personen.

Innsynsretten kan virke litt fremmed for revisor. Skal en ansatt hos en revisjonsklient kunne anmode om innsyn i revisors arbeidspapirer? Revisjonsselskapene må imidlertid forholde seg til innsynsretten etter GDPR, også når det gjelder revisjonsoppdrag. Innsynsretten omfatter opplysningene, og gir ikke rett til å få se dokumenter.

GDPR åpner for at den behandlingsansvarlige kan nekte å etterkomme en innsynsanmodning dersom anmodningen er åpenbart grunnløs eller overdreven. Det må vurderes i det enkelte tilfellet. Det er den behandlingsansvarlige (revisjonsselskapet) som har bevisbyrden. Trolig vil innsynsanmodninger forekomme sjelden i revisjonsbransjen, men revisjonsselskapene må håndtere de som måtte komme.

Sletting
Personen som opplysningene gjelder, har i en rekke tilfeller rett til å få opplysninger om seg selv slettet. Den behandlingsansvarlige har plikt til å slette disse opplysningene. Opplysningene skal slettes selv om personen ikke har bedt om sletting. For eksempel skal det slettes når opplysningene ikke lenger er nødvendige for formålet de ble samlet inn for.

GDPR inneholder unntak fra dette. Blant annet er det unntak når det er nødvendig for å oppfylle en rettslig forpliktelse. Revisorloven krever at revisjonsdokumentasjon og nummererte brev oppbevares i ti år (foreslått redusert til fem år i NOU 2017: 15). I oppbevaringsperioden har derfor ikke revisor anledning til å slette personopplysninger som er en del av revisjonsdokumentasjonen. Revisor har heller ikke anledning til å endre revisjonsdokumentasjonen etter at revisjonen er avsluttet (ISA 230).

Revisorloven inneholder ingen krav til sletting av revisjonsdokumentasjonen, kun krav til minimum oppbevaringstid. Bransjenormen skal gi retningslinjer for forholdet mellom oppbevaringsplikten i revisorloven og sletteplikten etter GDPR og hvitvaskingsloven.

Personvernerklæring og engasjementsavtale
Det bør utarbeides en personvernerklæring som gir informasjon om hvordan personopplysninger behandles i revisjonsforetaket og hvordan de registrerte kan ivareta sine rettigheter. Det vil antakelig også være en fordel å avklare enkelte forhold som gjelder personvern i engasjementsavtalen. I forbindelse med arbeidet med bransjenormen er planen å utarbeide en personvernerklæring og oppdatere engasjementsavtalen.

Personvernombud

Under gjeldende personvernregelverk er personvernombud (også kalt personvernrådgiver) en frivillig ordning. Etter GDPR blir enkelte foretak pålagt å ha et personvernombud (artikkel 37–39). Antakelig vil ingen revisjonsforetak ha plikt til å utpeke et personvernombud, men foretakene kan velge å gjøre dette på frivillig basis.

GDPR gir en person som henvender seg til en behandlingsansvarlig og anmoder om innsyn, rett til å få bekreftet om personopplysninger om vedkommende behandles, og i tilfelle, rett til innsyn i personopplysningene.