Atferdsnorm for behandling av personopplysninger i regnskapsbransjen

NB! UTKAST TIL HØRING. IKKE GODKJENT AV DATATILSYNET.

Dato: 7.5.2018

Versjon: 1.5

Utarbeidet av bransjestandardutvalget med medlemmer fra Regnskap Norge, Økonomiforbundet og Revisorforeningen.

Innhold

1. Innledning og formål 3
2. Kort om regnskapsbransjen og forholdet til annet regelverk 3
3. Definisjoner 4
4. Avgrensninger 5
5. Roller 5
6. Kartlegging av personopplysninger 5
7. Formål med behandling av personopplysninger 6
8. Åpenhet i behandlingen 6
9. Om personvernkontakt og personvernombud 6
10. Vurdering av personvernkonsekvenser og risikovurderinger 7
11. Særlige kategorier av personopplysninger 7
12. Rutiner for personopplysningssikkerhet og innebygd personvern 8
13. Dokumentasjon av oppbevaringssted for personopplysninger 9
14. Avtaleverk mellom behandlingsansvarlig og databehandler 9
15. Rutiner for samtykke, motsettelse av behandling, innsyn og retting 9
16. Rutiner for dataportabilitet 10
17. Rutiner for endring av formål med behandling av personopplysninger 10
18. Rutiner for sletting av personopplysninger, forholdet til andre lover 10
19. Rutiner for avvikshåndtering og rapportering 11
20. Dokumentasjon av prosedyrer og intern kontroll 11
21. Kontroll av etterlevelse av atferdsnormen 11
22. Vedlegg 12

1. Innledning og formål

Regnskapsbransjen består av virksomheter som i næring fører regnskapet for andre. I tillegg til å være behandlingsansvarlig for personopplysninger i egen virksomhet, er virksomhetene databehandlere for et stort antall oppdragsgivere gjennom utføring av regnskaps- og lønnsoppdrag. I all vesentlighet er data som behandles regnskapsopplysninger for å utføre oppdragsgivers plikter etter regnskaps- og bokføringslovgivningen og utarbeide oppgaver og opplysninger for oppdragsgiver som denne skal gi i henhold til lov eller forskrift, men dataene kan også inneholde personopplysninger. Behandlingen av personopplysninger i regnskapsførervirksomheter er ganske ensartet, slik at det er nyttig å etablere en atferdsnorm for regnskapsbransjen.

Formålet med denne atferdsnormen er å beskrive rutiner og intern kontroll for å sikre etterlevelse av kravene i personopplysningsloven når regnskapsførervirksomheten utfører et regnskaps-, lønns- eller rådgivningsoppdrag for sin oppdragsgiver. Normen er derfor ikke rettet mot regnskapsførervirksomhetens rolle som behandlingsansvarlig for egne personopplysninger - som eksempelvis opplysninger om egne ansatte og om personer hos sine oppdragsgivere.

Normen dekker ikke de tilfelle hvor regnskapsfører selv er behandlingsansvarlig ved gjennomføring av attestasjonsoppdrag eller rådgivningsoppdrag hvor det er regnskapsførervirksomheten som bestemmer formålet med behandlingen og hvilke hjelpemidler som skal benyttes. I disse tilfelle bærer regnskapsførervirksomheten eksempelvis et større ansvar for formålet og hjemmelsgrunnlaget for behandlingen av personopplysningene.

Atferdsnormen gir grunnlag for at regnskapsfører etterlever personvernreglene i utførelsen av sine oppdrag. Anvendelse av atferdsnormen forutsetter kjennskap til de sentrale elementene i personvernforordningen.

2. Kort om regnskapsbransjen og forholdet til annet regelverk

I henhold til regnskapsførerloven av 18.06.1993 nr. 109 skal alle som fører regnskap for andre i næring inneha autorisasjon fra Finanstilsynet. Ett oppdrag kan innebære å fakturere, føre regnskap, forestå lønnskjøringer, utføre utbetalinger og gjennomføre årsavslutning med årsregnskap og skattemelding, enten som enkeltstående oppgaver eller i en kombinasjon. Regnskapsbransjen behandler derfor personopplysninger på mange oppdrag for mange oppdragsgivere, og det er derfor viktig med god intern kontroll og god etterlevelse av personopplysningsregelverket.

Regnskapsførerloven § 2 krever at autoriserte regnskapsførere skal utføre sine oppdrag i samsvar med bestemmelser i og i medhold av lov og i samsvar med god regnskapsføringsskikk. Etter § 10 har regnskapsfører og regnskapsførers medarbeidere taushetsplikt om alt de under sin virksomhet får kjennskap til med mindre annet følger av eller i medhold av lov, eller den som opplysningene gjelder har samtykket til at taushetsplikten ikke skal gjelde. Regnskapsfører og regnskapsførers medarbeidere kan ikke utnytte slike opplysninger i egen virksomhet eller i tjeneste eller arbeid for andre. Standard for god regnskapsføringsskikk (GRFS) gir føringer for hva som skal anses som god regnskapsføringsskikk etter loven. Standarden skisserer krav til intern kontroll og rutiner. Den er ikke spesifikk på behandlingen av personopplysninger, men inneholder krav om eksempelvis konfidensialitet og sikring av regnskapsopplysninger som har relevans for behandlingen av personopplysninger.

Det foreligger en rekke tilliggende regelverk som regulerer det materielle innhold i den yrkesutøvelse som skjer. Hvilke regelverk som er aktuelle må vurderes konkret, basert på oppdragsgivers virksomhet. God regnskapsføringsskikk utdyper ikke innholdet i slike tilliggende regelverk, men det er i fotnoter gitt henvisninger til sentrale bestemmelser i andre regelverk, hvorav de viktigste antas å være bokførings- og regnskapsreglene. Andre relevante områder er selskaps-, skatte- og avgiftsregler samt personopplysningsregler.

3. Definisjoner

Det vises til personopplysningslovens artikkel 4 for definisjoner av begrepene benyttet i personopplysningsloven. I denne atferdsnormen gjelder følgende definisjoner:

Personopplysning: En personopplysning er enhver opplysning om en identifisert eller identifiserbar fysisk person (den registrerte). For at det skal være en personopplysning er det en forutsetning at det er en kobling mellom opplysningen og personen.

Særlige kategorier personopplysning: Opplysning om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Regnskapsfører: Med regnskapsfører menes enhver person som utfører oppgaver på oppdraget, herunder oppdragsansvarlig regnskapsfører og medarbeidere.

Regnskapsførervirksomhet: Med regnskapsførervirksomhet menes både enkeltpersonforetak og selskap som i næring fører regnskap for andre. Minst en må være autorisert regnskapsfører, og for de fleste regnskapsførervirksomheter vil dette være daglig leder, eventuelt sammen med flere autoriserte regnskapsførere. Regnskapsførervirksomheten vil være databehandler overfor oppdragsgiver.

Behandlingsansvarlig: Behandlingsansvarlig er i denne normen en oppdragsgiver som har utkontraktert eksempelvis regnskaps- og lønnsoppdrag til en regnskapsførervirksomhet. Behandlingsansvarlig er den som bestemmer formålet med behandlingen, og kan instruere regnskapsførervirksomheten hvordan behandling skal skje.

Databehandler: Regnskapsførervirksomheten som gjennomfører behandling av personopplysninger på vegne av, og etter instruks av, sin oppdragsgiver.

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.

Oppdragsavtale: En avtale mellom oppdragsgiver og regnskapsførervirksomheten som angir hvilke av oppdragsgivers plikter etter regnskaps- og/eller bokføringslovgivningen som regnskapsfører har påtatt seg å utføre, samt hvilke oppgaver og opplysninger som skal utarbeides på vegne av oppdragsgiver. Andre oppdrag enn regnskapsføreroppdrag skal også nedfelles i oppdragsavtale. Dette gjelder enhver selvstendig oppgave som regnskapsførervirksomheten forplikter seg til å utføre mot betaling i kombinasjon med regnskapsføreroppdrag.

Lønnsoppdrag: Oppdrag som inkluderer registrering av lønnsgrunnlag, utarbeidelse av lønnsdokumentasjon, utarbeidelse av grunnlag for utbetaling av lønn, feriepenger, trekk og arbeidsgiveravgift, og/eller utarbeidelse og innsending av offentlige oppgaver på vegne av oppdragsgiver.

Den registrerte: Den registrerte er den personen som opplysningene gjelder. Dette kan være ansatte eller andre hos oppdragsgiver hvor personopplysninger blir behandlet av regnskapsførervirksomheten.

4. Avgrensninger

Regnskapsførervirksomheten inngår en skriftlig oppdragsavtale med oppdragsgiver som angir de regnskapsfunksjoner og andre oppdrag som skal utføres av regnskapsførervirksomheten. Dette gjelder eksempelvis regnskaps-, lønns- og rådgivningsoppdrag.

Oppdragsavtalen og databehandleravtalen avgrenser de personopplysninger som er nødvendige for at regnskapsførervirksomheten skal ivareta oppdraget etter avtalen. Andre personopplysninger enn de som er nødvendige skal ikke mottas, behandles eller oppbevares.

5. Roller

Ivaretakelse av plikter: Behandlingsansvarlig, som i denne normen betegnes som oppdragsgiver, har de aller fleste pliktene etter personopplysningsloven. Oppdragsgiver kan benytte regnskapsførervirksomheten til å ivareta noen av disse pliktene gjennom oppdragsavtalen og databehandleravtalen. Databehandler, som i denne normen omtales som regnskapsførervirksomheten, vil også ha selvstendige plikter etter personopplysningsloven, herunder gjennom databehandleravtale å gi tilstrekkelige garantier for at behandlingen vil skje i henhold til personopplysningsloven, og å varsle oppdragsgiver hvis regnskapsførervirksomheten ser at oppdragsgiver ikke følger personopplysningsloven.

Den registrertes utøvelse av rettigheter: Den registrerte skal forholde seg til oppdragsgiver som bestemmer behandlingen av personopplysninger. Den registrerte kan derfor ikke henvende seg direkte til regnskapsførervirksomheten for å få utøvd sine rettigheter, med mindre det foreligger en dokumentert avtale om dette mellom oppdragsgiver og regnskapsførervirksomheten.

6. Kartlegging av personopplysninger

Det skal foreligge en oversikt over alle personopplysninger som regnskapsførervirksomheten behandler på vegne av oppdragsgiver. Se vedlegg for et eksempel på oppbygging av en kartleggingsmal.

Ved lik behandling av personopplysninger for alle oppdragsgivere, kan denne dokumentasjonen utarbeides for alle oppdragsgivere under ett. Den generelle dokumentasjonen skal kompletteres med særskilte forhold for oppdragsgivere med avvikende formål og behandling. Ved ulik behandling av personopplysninger i regnskapsførervirksomheten, eksempelvis ved bruk av to lønnssystemer, må dokumentasjonen tilpasses for å beskrive behandlingen i de to systemene.

7. Formål med behandling av personopplysninger

Formålet med behandlingen av personopplysninger i en regnskapsførervirksomhet er i hovedsak å assistere oppdragsgiver med å ivareta oppdragsgivers plikter innen regnskap, lønn, skatt og avgift. Hjemmel for disse pliktene er blant annet regnskapsloven, bokføringsloven, skatteloven, skatteforvaltningsloven, skattebetalingsloven og merverdiavgiftsloven. I tillegg kan personopplysninger behandles i forbindelse med rådgivningsoppdrag.

Behandling av personopplysninger innhentes hovedsakelig for å sikre

- registrering av lønnsgrunnlag,
- utarbeidelse av lønnsdokumentasjon,
- utarbeidelse av grunnlag for utbetaling av lønn, feriepenger, trekk og arbeidsgiveravgift,
- utarbeidelse og innsending av offentlige oppgaver på vegne av oppdragsgiver
- korrekt bokføring av lønnsrelaterte regnskapsopplysninger.

I tillegg kommer innrapportering til NAV, Statistisk sentralbyrå og andre interessenter, som gjennom lovhjemmel kan kreve personopplysninger. Dette inkluderer eksempelvis forskriftskrav om innsyn i ansattes lønns- og arbeidsvilkår i bygg- og anleggsbransjen.

Dette er de praktisk viktigste tilfellene hvor regnskapsførervirksomheter behandler personopplysninger, men det kan også være behov for det ved utførelse av andre oppdrag.

Regnskapsførervirksomheten kan ikke bruke oppdragsgivers personopplysninger til andre formål enn det som følger av oppdragsavtalen, databehandleravtalen, gjeldende lovkrav og god regnskapsføringsskikk. Regnskapsførervirksomheten kan derfor ikke bruke oppdragsgivers detaljerte personopplysninger til å understøtte egen virksomhet, herunder for markedsførings- og salgsaktiviteter. Likevel kan personopplysninger fra oppdragsgivere anonymiseres og sammenstilles eksempelvis for å beregne gjennomsnittlig lønnsnivå i regionen. Det må ikke være mulig å identifisere den registrertes lønnsvilkår o.l. gjennom bruk av for snevre kategorier.

8. Åpenhet i behandlingen

Personopplysningsloven krever at personopplysninger behandles på en lovlig, rettferdig og åpen måte. Regnskapsførervirksomheten skal derfor ved forespørsel fra oppdragsgiver kunne gjøre rede for hvordan behandlingen av personopplysninger skjer hos seg og underleverandører. Dette kan skje muntlig og ved fremleggelse av dokumentasjon i form av rutinebeskrivelser, prosedyrer, flytskjema mv. Dokumentasjonen og redegjørelsen skal være tilstrekkelig til å danne et bilde av behandlingen. Det er ikke nødvendig å fremlegge detaljer med mindre dette er absolutt nødvendig for å skape forståelse hos oppdragsgiver eller hos den registrerte som krever innsyn.

9. Om personvernkontakt og personvernombud

Regnskapsførervirksomheten skal peke ut en personvernkontakt som har ansvar for ivaretakelse av regelverk rundt personopplysninger, og være kontaktperson for eksterne parter. Personen kan være daglig leder eller en denne har utpekt. Personen utpekt som personvernkontakt skal ha gjennomført opplæring innen personopplysningsregelverket, og skal oppdatere kompetansen ved endringer i rettigheter og plikter i regelverket.

Personopplysningsloven krever utnevnelse av personvernombud der hvor behandlingsansvarlig og databehandler har oppdrag for offentlig myndighet eller organ, hvor behandlingsansvarlig og databehandler regelmessig og systematisk monitorerer registrerte eller behandler særlige kategorier personopplysninger i stor skala. Kontaktopplysninger om personvernombudet må offentliggjøres og meddeles Datatilsynet.

En regnskapsførervirksomhet vil normalt ikke falle inn under personopplysningslovens krav til pliktig personvernombud. Regnskapsførervirksomheten kan etablere denne rollen frivillig. Beslutningen om dette bør styrebehandles. Om rollen opprettes frivillig, må denne følge personopplysningslovens krav til personvernombud.

Hvis oppdragsgiver må ha personvernombud, og regnskapsførervirksomheten gjennom oppdragsavtalen og databehandleravtalen behandler opplysninger som medførte at oppdragsgiver må ha personvernombud, må også regnskapsførervirksomheten utnevne et personvernombud. Likevel trenger ikke regnskapsførervirksomheten å utnevne personvernombud hvis de eksempelvis kun gjør regnskaps- og lønnsoppdrag for et helseforetak, og regnskapsførervirksomheten ikke har befatning med pasienters helseopplysninger.

10. Vurdering av personvernkonsekvenser og risikovurderinger

Utarbeidelse av en vurdering av personvernkonsekvenser (Data Protection Impact Analysis - DPIA) gjøres i de tilfelle det etableres systemer og rutiner med høy risiko for den registrertes rettigheter og friheter. Ansvaret for å identifisere behov for, og utarbeide en DPIA ligger hos oppdragsgiver. Regnskapsførervirksomheten kan bistå i arbeidet etter behov og etter avtale med oppdragsgiver.

Risikovurderingen av behandling av personopplysninger skal gjennomføres sammen med annen risikovurdering i virksomheten for å sikre en helhetlig tilnærming. Risikovurderingen skal inneholde en vurdering av risiko for intern eksponering i regnskapsførervirksomheten (eksempelvis brudd på arbeidsdeling/svake tilgangskontroller), eksponering hos ekstern system- og/eller driftsleverandør, og eksponering overfor uvedkommende utenfor behandlingsmiljøet til regnskapsførervirksomheten.

Risikovurderingen skal være skriftlig, oppdatert og tilgengelig for tilsynsmyndigheter. Se vedlegg for et eksempel på oppbygging av en risikovurderingsmal.

11. Særlige kategorier av personopplysninger

Regnskapsførervirksomheten vil i enkelte tilfelle kunne behandle særlige kategorier av personopplysninger på vegne av oppdragsgiveren. Dette kan eksempelvis være den registrertes tilknytning til fagforening gjennom trekk i lønn for fagforeningskontingent, oppdrag for trossamfunn og politiske organisasjoner og helseopplysninger i forbindelse med innrapportering til NAV.

Behandling av særlige kategorier av personopplysninger er i utgangspunktet forbudt. Hvis formålet med behandlingen av disse opplysningene er å ivareta en rapporteringsplikt/avtale/forpliktelse, er dette et gyldig formål og dermed tillatt. Regnskapsførervirksomheten skal ha egne konsultasjoner med oppdragsgiver om behandlingen av særlige kategorier personopplysninger og nødvendigheten av å behandle disse. Disse konsultasjonene skal være dokumentert og inneholde en risikovurdering og beskrivelse av intern kontroll.

Regnskapsførervirksomheten skal ha høy oppmerksomhet og gode kontroller rundt særlige kategorier av personopplysninger. Risikovurderingen må inneholde beskrivelse av regnskapsførervirksomhetens vurderinger av denne type opplysninger. Tilgang til særlige kategorier personopplysninger skal holdes på et minimum i regnskapsførervirksomheten.

12. Rutiner for personopplysningssikkerhet og innebygd personvern

Tilgang til personopplysninger i regnskapsførervirksomhetens systemer og arkiver skal kun gis til personer med berettiget behov for opplysningene for å ivareta plikter etter oppdragsavtalen, gjeldende lovkrav og god regnskapsføringsskikk. Norsk Bokføringsstandard NBS 1 om sikring av regnskapsmateriale skal brukes som veiledning for sikring av materialet som inneholder personopplysninger.

Regnskapsførervirksomheten skal sikre personopplysninger som mottas fra oppdragsgiver, som sendes til oppdragsgiver og som behandles internt og hos tredjeparter. Regnskapsførervirksomheten skal påse at det er tilstrekkelige logiske og fysiske sikkerhetstiltak i hele behandlingsløpet. Logisk sikring innebærer blant annet kryptert kommunikasjon og tilgangskontroller til krypterte databaser hvor opplysningene er lagret. Fysisk sikring innebærer blant annet kontroll av tilgang til lokaler og låste arkivskap. Risikovurderingen gir grunnlaget for å vurdere tilstrekkelighet av sikkerhetstiltakene.

Sikkerhetstiltakene skal underbygge konfidensialitet (sikre at kun personer med berettiget behov har tilgang), integritet (sikre at personopplysninger er fullstendige og nøyaktige og ikke skal kunne endres uautorisert) og tilgjengelighet (sikre at personopplysninger er tilgjengelig for autoriserte personer etter behov).

Regnskapsførervirksomheter er organisert ulikt avhengig av størrelse, konserntilknytning og geografisk spredning. Behandlingen av personopplysninger kan derfor gjennomføres ulikt hos ulike regnskapsførervirksomheter.

For mindre regnskapsførervirksomheter, hvor det er naturlig for regnskapsførere å dele på å jobbe på samme oppdrag, er det akseptabelt at flere i regnskapsførervirksomheten har tilgang til personopplysninger på oppdraget. Standard for god regnskapsføringsskikk (GRFS) fremsetter krav om konfidensialitet og tilgangskontroller. Risikovurderingen til regnskapsførervirksomheten må inkludere en vurdering av risikoen med denne arbeidsformen.

For større regnskapsførervirksomheter, hvor det er vanlig at særskilte personer eller team jobber på et oppdrag, skal det etableres begrensninger i tilgang til oppdragsgivers personopplysninger gjennom logisk og fysisk sikring av opplysningene slik at kun disse personene eller teamene har tilgang. Dette skal sikre at kun de som har berettiget behov for å behandle opplysningene for å ivareta oppdragsavtalen har tilgang.

I noen regnskapsførervirksomheter er det av kompetanse- og effektivitetshensyn etablert spesialiserte funksjoner og avdelinger, eksempelvis lønnsavdelinger som ivaretar arbeidsoppgaver for flere kontor og oppdragsgivere. Medarbeidere i slike spesialiserte avdelinger har et berettiget behov til innsyn i personopplysninger for å løse oppgaver etter oppdragsavtalen.

Systemene som regnskapsførervirksomheten benytter skal ha tilstrekkelig innebygget personvern som samsvarer med risikovurderingen regnskapsførervirksomheten har gjort rundt behandlingen av personopplysninger. Manglende innebygget personvern i systemene, eksempelvis svake tilgangskontroller, manglende innstillingsmuligheter og fravær av krypterte databaser og kryptert kommunikasjon, må kompenseres av annen intern kontroll inntil personvern blir innebygget i

prosedyrer og systemer. Hvis systemene ikke får tilstrekkelig innebygget personvern etter påpekning av svakheten, må regnskapsførervirksomheten bytte systemer for å kunne verne den registrerte.

Regnskapsførervirksomheten skal ikke behandle og oppbevare personopplysninger ustrukturert og uten muligheter for god intern kontroll. Eksempel på dette er å angi personopplysninger i bilagsteksten ved registrering av regnskapsopplysninger i regnskapssystemet. Kontrollsporet vil sikre kobling mellom registreringen og dokumentasjonen slik at registrering av personopplysninger i bilagsteksten ikke er nødvendig. Et annet eksempel er å benytte eposten til ansatte i regnskapsførervirksomheten til oppbevaring av personopplysninger. Personopplysninger må i disse tilfelle flyttes fra mer ustrukturerte arkiv til strukturerte arkiv med tilfredsstillende sikring. Etter flytting må personopplysninger fjernes fra det ustrukturerte arkivet.

13. Dokumentasjon av oppbevaringssted for personopplysninger

Oppbevaringssted dekker to dimensjoner, land og system. Personopplysninger kan behandles og oppbevares fritt innen EØS-området. Virksomheter som vil overføre personopplysninger utenfor EØS-området, kan bare overføre til stater som sikrer en forsvarlig behandling av opplysningene.

Land: Regnskapsførervirksomheten skal ha dokumentasjon på fysisk oppbevaringssted for alle personopplysninger som behandles. Dette gjelder i alle ledd fra regnskapsførervirksomheten, via leverandør av system- og driftstjenester til deres underleverandører og frem til endelig oppbevaringssted. Det er tilstrekkelig med angivelse av leverandør og land i dokumentasjonen. Om det ikke er mulig å få stadfestet oppbevaringssted på landnivå, må regnskapsførervirksomheten stoppe behandling og oppbevaring hos leverandøren til dette er avklart, alternativt bytte leverandør.

System: Oversikten over oppbevaringssted må også inkludere hvilke systemer personopplysninger er oppbevart i. Dette er nødvendig for å kunne ha et effektivt innsyn og sikre effektiv dataportabilitet.

14. Avtaleverk mellom behandlingsansvarlig og databehandler

Det skal foreligge en databehandleravtale mellom oppdragsgiver og regnskapsførervirksomheten. Databehandleravtalen kan enten være et selvstendig dokument eller være en del av oppdragsavtalen. Avtalen skal være skriftlig og må signeres av partene.
Regnskapsførervirksomhetens bruk av annen databehandler, eksempelvis en system- og/eller driftsleverandør, kan kun skje etter avtale med oppdragsgiver, normalt gjennom databehandleravtalen. I den grad regnskapsførervirksomheten har utkontraktert behandlingen av personopplysninger til en ekstern system- og/eller driftsleverandør, skal det også foreligge en databehandleravtale mellom regnskapsførervirksomheten og leverandøren(e). Hvis leverandøren igjen har videreutkontraktert til underleverandør, skal disse ha databehandleravtale seg imellom, eventuelt direkte med regnskapsførervirksomheten eller med oppdragsgiver.
Regnskapsførervirksomheten og oppdragsgiver skal ha dokumentasjon av alle databehandlere involvert i utførelsen av oppdraget og hvor personopplysninger behandles.

15. Rutiner for samtykke, motsettelse av behandling, innsyn og retting

Det er oppdragsgiver som skal innhente samtykke til behandling av personopplysningene hvor samtykke kreves. Blir regnskapsførervirksomheten klar over manglende innhenting av samtykke, skal regnskapsførervirksomheten varsle oppdragsgiver umiddelbart om regelbruddet.

Det er kun oppdragsgiver, i rollen som behandlingsansvarlig, som kan instruere regnskapsførervirksomheten om at behandling av personopplysninger ikke skal skje, forvalte krav om innsyn eller be om retting. Den registrerte kan ikke henvende seg direkte til regnskapsførervirksomheten for å motsette seg behandling, kreve innsyn eller kreve retting, med mindre det foreligger en avtale om dette mellom oppdragsgiver og regnskapsførervirksomheten. Blir regnskapsførervirksomheten klar over at oppdragsgiver ikke imøtekommer den registrertes rettigheter, skal oppdragsgiver varsles umiddelbart.

Regnskapsførervirksomheten skal ikke gi innsyn i personopplysninger til den registrerte uten at oppdragsgiver godkjenner innsynet. Dette gjelder likevel ikke hvor noen har juridisk rett til innsyn uavhengig av oppdragsgivers aksept.

16. Rutiner for dataportabilitet

Den registrerte kan kreve elektronisk oppbevarte personopplysninger overført fra en behandlingsansvarlig til en annen hvis mottaker kan lese dataene elektronisk. Dette kalles dataportabilitet. Ansvaret for å ivareta den registrertes rett til dette ligger hos oppdragsgiver.

Regnskapsførervirksomheten kan etter avtale med oppdragsgiver tilrettelegge for dataportabilitet gjennom sin kunnskap om hvor de enkelte personopplysninger oppbevares, og hvordan systemer kan eksportere opplysningene.

Dataportabilitet kan ivaretas som en samlet programmert aktivitet, eller at personopplysninger om den registrerte sammenstilles manuelt fra kildene hvor personopplysninger oppbevares. Metoden for å sikre dataportabilitet må avtales med oppdragsgiver og er avhengig av hva systemene kan håndtere.

Regnskapsførervirksomheten kan ikke på eget initiativ oversende personopplysninger til den registrerte eller ny behandlingsansvarlig uten at oppdragsgiver har gitt sitt samtykke til dette.

Oppdragsgiver kan instruere regnskapsførervirksomheten om at personopplysninger flyttes til ny regnskapsførervirksomhet ved opphør av oppdragsavtalen etter de samme prinsipper som gjelder for dataportabilitet.

17. Rutiner for endring av formål med behandling av personopplysninger

Oppdragsgiver bestemmer formålet med behandlingen av personopplysninger. Formålet for regnskapsførervirksomhetens behandling av personopplysninger er å utføre sine oppdrag i samsvar med oppdragsavtalen, databehandleravtalen, gjeldende lovkrav og god regnskapsføringsskikk. Endring i, eller utvidelse av, formålet med behandlingen må derfor reflekteres i endret oppdragsavtale, databehandleravtale, eller nye avtaler.

Hvis regnskapsførervirksomheten blir klar over at formålsendringen fra oppdragsgiver ikke er i tråd med personopplysningsregelverket, eksempelvis at det mangler samtykke for nytt formål, skal oppdragsgiver varsles umiddelbart.

18. Rutiner for sletting av personopplysninger, forholdet til andre lover

Oppdragsgiver er ansvarlig for at personopplysninger slettes når formålet med behandlingen av opplysningene ikke lenger er tilstede. Regnskapsførervirksomheten skal kun slette

personopplysninger etter avtale med, eller instruks fra, oppdragsgiver. I avtalen mellom oppdragsgiver og regnskapsførervirksomheten kan partene bli enige om faste sletterutiner. Regnskapsførervirksomheten skal varsle oppdragsgiver hvis regnskapsførervirksomheten blir klar over at oppdragsgiver ikke følger reglene for sletting.

Regnskapsførervirksomheten kan ikke oppbevare personopplysninger etter slettetidspunktet for oppdragsgivers analyseformål med mindre dette er avtalt med oppdragsgiver og formålet er gyldig, alternativt at personopplysningene anonymiseres. Om regnskapsførervirksomheten er i tvil om formålet er tilstrekkelig hjemlet i personopplysningsloven, skal oppdragsgiver varsles om dette.

I den grad det er avtalt at regnskapsførervirksomheten skal oppbevare regnskapsopplysninger og regnskapsmateriale på vegne av oppdragsgiver i henhold til bokføringsloven, og opplysninger og materialet inneholder personopplysninger, må regnskapsførervirksomheten ha rutiner for sletting. Sletting skal skje i originalt arkiv og i andre reproduksjoner, herunder sikkerhetskopier etter bokføringsforskriften.

Sletting kan ikke utføres hvis opplysningene er nødvendig for å ivareta oppbevaringskrav i regnskapsførerloven (oppdragsdokumentasjon), bokføringsloven (regnskapsmateriale), hvitvaskingsloven eller annen relevant lovgivning.

19. Rutiner for avvikshåndtering og rapportering

Regnskapsførervirksomheten skal umiddelbart varsle oppdragsgiver hvis regnskapsførervirksomheten blir kjent med at oppdragsgiver behandler personopplysninger i strid med personopplysningsloven.

Regnskapsførervirksomheten skal umiddelbart varsle oppdragsgiver hvis regnskapsførervirksomheten har fått kjennskap til at personopplysninger om den registrerte er kommet på avveie og ser at dette kan ha en konsekvens for den registrerte.

20. Dokumentasjon av prosedyrer og intern kontroll

Personvern skal bygges inn i daglige rutiner og prosedyrer for regnskapsførervirksomheten der hvor personopplysninger behandles. Alle flytskjema, rutinebeskrivelser og prosedyrer som har relevans for behandling av personopplysninger skal være skriftlige og lett tilgjengelige for regnskapsførere som behandler opplysningene og når tilsynsmyndigheter og oppdragsgiver ber om innsyn i dokumentasjonen. Dokumentasjonen skal underbygge krav om åpenhet i behandlingen.

Dokumentasjonen rundt prosedyrer og intern kontroll skal oppdateres når det har skjedd endringer som tilsier at dette er nødvendig.

21. Kontroll av etterlevelse av atferdsnormen

Medlemmer av Regnskap Norge og Revisorforeningen er underlagt bransjeorganisert kvalitetskontroll som Finanstilsynet bygger på i sitt tilsyn av autoriserte regnskapsførere og regnskapsførervirksomheter. Kvalitetskontrollen omfatter blant annet kontroll av at regnkapsførervirksomhetene virker på hensiktsmessig og betryggende måte i samsvar med lovgivningen. Kvalitetskontrollen vil inkludere kontroll av etterlevelse av atferdsnormen.

22. Vedlegg

a) Kartleggingsmal, minimum kolonneinnhold:

- Personopplysningene som behandles på vegne av oppdragsgiver
- Hjemmelsgrunnlaget (etter artikkel 6 i forordningen)
- Formålet med behandlingen av personopplysningene
- Kategori personopplysning (ordinær / særskilt kategori)
- Hvor personopplysningene blir behandlet (system)
- Hvor personopplysningene oppbevares (system/land)
- Særskilte forhold (sletteregler, oppbevaringstid mv)

b) Risikovurderingsmal, minimum kolonneinnhold:

- Personopplysningene som behandles på vegne av oppdragsgiver (Jamfør over)
- Identifisert risiko knyttet til personopplysningen
- Sannsynlighet for eksponering (Lav/Middels/Høy)
- Konsekvens ved eksponering hvis risikoen inntreffer (Lav/Middels/Høy)
- Risikoklasse (sannsynlighet x konsekvens)
- Intern kontroll etablert for personopplysningen / klasse av personopplysninger
- Forslag til forbedring av intern kontroll (tiltaksanalyse)