Datatilsynets krav til akkreditering av kontrollorganer for atferdsnormer

Februar 2024

Datatilsynet
The Norwegian Data Protection Authority

Innhold

INTRODUKSJON 3

1. UAVHENGIGHET 5
2. INTERESSEKONFLIKTER 9
3. DYBDEKUNNSKAP 11
4. FASTSATTE PROSEDYRER OG STRUKTURER 12
5. ÅPENHET I KLAGEBEHANDLINGEN 14
6. KOMMUNIKASJON MED DATATILSYNET 16
7. MEKANISMER FOR GJENNOMGANG AV NORMEN 17
8. RETTSSTILLING 18
9. BRUK AV UNDERLEVERANDØRER 19

Introduksjon

I tråd med artikkel 41 nr. 1 i europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 (**personvernforordningen**) og det europeiske personvernrådet (**EDPB**) sine retningslinjer nr. 01/2019 om atferdsnormer og kontrollorganer under personvernforordningen (**EDPBs retningslinjer**), må nasjonale og transnasjonale atferdsnormer (**Norm -en**, **-er**, **-ene**) overvåkes av et kontrollorgan som er akkreditert av en kompetent tilsynsmyndighet (**Datatilsynet**). Ifølge artikkel 41 nr. 6 i personvernforordningen, og som spesifisert i EDPBs retningslinjer, gjelder ikke kravet om at kontrollorganet skal være akkreditert for behandling som utføres av offentlige myndigheter.

Kontrollorganet kan enten være eksternt eller internt for eieren av Normen (**Normeieren**). Et internt kontrollorgan kan være en intern avdeling hos Normeieren, eller en intern komité på *ad hoc*-basis. Personvernforordningen artikkel 41 nr. 2 lister opp en rekke krav som det utnevnte kontrollorganet må oppfylle for å få akkreditering. Bestemmelsen angir at et kontrollorgan må

- vise at det er **uavhengig** og har **dybdekunnskap** om temaet for Normen i henhold til personvernforordningen artikkel 41 nr. 2 bokstav a
- fastsette **fremgangsmåter** som gjør det mulig å vurdere om berørte behandlingsansvarlige og databehandlere oppfyller vilkårene for anvendelse av Normen, **føre tilsyn med at den overholdes** og foreta regelmessige **gjennomgåelser** av Normens virkemåte, i henhold til personvernforordningen artikkel 41 nr. 2 bokstav b
- fastsette framgangsmåter og rutiner for **behandling av klager** på overtredelser av Normen eller måten den har blitt eller blir gjennomført på av den behandlingsansvarlige eller databehandleren, og gjøre nevnte fremgangsmåter og rutiner åpne for de registrerte og allmennheten, i henhold til personvernforordningens artikkel 41 nr. 2 bokstav c
- vise, på en måte som oppfyller Datatilsynets krav, at oppgavene eller pliktene **ikke fører til en interessekonflikt**, i henhold til personvernforordningens artikkel 41 nr. 2 bokstav d

EDPBs retningslinjer gir viktig praktisk veiledning og tolkningshjelp i forbindelse med anvendelsen av personvernforordningens artikkel 41 nr. 2. EDPBs retningslinjer kategoriserer akkrediteringskravene i personvernforordningens artikkel 41 nr. 2 i følgende åtte kategorier:

- Uavhengighet
- Interessekonflikt
- Dybdekunnskap
- Fastsatte prosedyrer og strukturer
- Åpenhet i klagebehandlingen
- Kommunikasjon med kompetent tilsynsmyndighet
- Mekanismer for gjennomgang
- Rettsstilling

Kravene som er nevnt i dette dokumentet er basert på kravene i personvernforordningens artikkel 41 nr. 2 og kravene nevnt i kapittel 12 i EDPBs retningslinjer, og de følger strukturen til EDPBs retningslinjer.

Det følger av personvernforordningen artikkel 41 nr. 3 at Datatilsynet må legge utkast til akkrediteringskriterier for kontrollorganer frem for EDPB i henhold til konsistensmekanismen (jf. personvernforordningen artikkel 63 og 61 nr. 1 bokstav c). Ifølge personvernforordningen artikkel 57 nr. 1 bokstav p må Datatilsynet offentliggjøre disse kriteriene.

Søknadskrav

Søkere må oppfylle alle akkrediteringskravene i dette dokumentet for å bli akkreditert av Datatilsynet.

Med mindre annet er spesifisert, skal kravene gjelde for kontrollorganet uavhengig av om kontrollorganet er internt eller eksternt.

Det er kun mulig å akkrediteres som kontrollorgan i tilknytning til temaet for én eller flere spesifikke Normer i henhold til personvernforordningen artikkel 41 nr. 1.

Søknader om akkreditering må leveres i skriftlig form til Datatilsynet. Vi aksepterer kun søknader på norsk eller engelsk. Søknaden skal inneholde bevis på at kravene som er listet opp i dette dokument er oppfylt, i form av relevant dokumentasjon, sertifikater e.l., slik disse kravene spesifiserer.

Akkrediteringen av et kontrollorgan skal ikke være til hinder for utviklingen av Normer. Vurderingen av søknaden om akkreditering skal derfor ta hensyn til særegenheter ved behandlingen av personopplysninger i hver sektor. Vurderingen skal også være så fleksibel som mulig, men samtidig overholde de juridiske rammene pålagt i personvernforordningen, EDPBs retningslinjer samt relevante uttalelser fra EDPB.

Søknaden skal minst inneholder følgende informasjon:

1. Informasjon om hvem søkeren er, for eksempel identifikasjonsnumre som organisasjonsnummer.
2. Søkerens bosted eller forretningsadresse, som i begge tilfeller må være i EØS.
3. Kontaktinformasjon som skal brukes i forbindelse med kommunikasjon om akkrediteringssøknaden.
4. Spesifisering av typen kontrollorgan (om det er internt eller eksternt).
5. Spesifisering av Normen som det søkes akkreditering for.
6. Virkeområdet for Normen (hvorvidt den skal gjelde nasjonalt eller transnasjonalt).
7. Relevante dokumenter og tidligere korrespondanse med Datatilsynet.

Utover dette følger mer detaljerte dokumentasjonskrav under hvert akkrediteringskrav nedenfor.

Akkrediteringens varighet

Datatilsynet kan, basert på en risikobasert tilnærming, gjennomgå akkrediteringen til kontrollorganet periodisk for å sikre at kontrollorganet fremdeles oppfyller akkrediteringskravene. Slike gjennomganger kan blant annet settes i gang på bakgrunn av endringer i Normen, vesentlige endringer i kontrollorganet eller dersom kontrollorganet ikke utfører sine kontrolloppgaver. Dersom det oppstår vesentlige endringer i kontrollorganet relatert til dets evne til å fungere uavhengig og effektivt, skal Datatilsynet alltid utføre slike evalueringer.

Kontrollorganet beholder akkrediteringsstatusen på ubestemt tid med mindre utfallet av en gjennomgang er at akkrediteringskriteriene ikke lenger er oppfylt. Gjennomgangen kan resultere i tilbaketrekning av kontrollorganets akkreditering i henhold til personvernsforordningen artikkel 41 nr. 5.

1. Uavhengighet

Kontrollorganet skal være tilstrekkelig uavhengig.

Et kontrollorgans uavhengighet kan forstås som en rekke formelle regler og prosedyrer som gjelder for kontrollorganets utnevnelse, mandat, rammevilkår og drift. Slike regler og prosedyrer skal gjøre det mulig for kontrollorganet å overvåke etterlevelsen av Normen i full autonomi, uten å påvirkes direkte eller indirekte, og uten å utsettes for noen form for press som kan påvirke kontrollorganets beslutninger.

Kontrollorganet skal ikke være i en posisjon til å motta instrukser knyttet til utøvelsen av dets oppgaver fra medlemmer av Normen (**Norm-medlem**), yrket, bransjen eller sektoren som Normen gjelder, eller fra selve Normeieren. Det må fastsettes regler og prosedyrer for å sikre at kontrollorganet handler autonomt og uten noen form for press fra Norm-medlemmer, yrket, bransjen eller sektoren som Normen gjelder, eller fra Normeieren. Når kontrollorganet er internt, må det være særskilt fokus på kontrollorganets evne til å opptre uavhengig.

Uavhengigheten skal påvises innenfor fire hovedområder:

- Juridiske prosedyrer og beslutningsprosedyrer
- Økonomiske ressurser
- Organisatoriske ressurser og struktur
- Ansvarlighet

Kravene for disse områdene er angitt nedenfor.

1.1 Juridiske prosedyrer og beslutningsprosedyrer

1.1.1 Kontrollorganet må være tilstrekkelig uavhengig med hensyn til Norm-medlemmene, yrket, bransjen eller sektoren som Normen gjelder, samt Normeieren. Det skal særlig tas hensyn til enhver juridisk og økonomisk kobling som kan eksistere mellom kontrollorganet og Normeieren eller Norm-medlemmene. Kontrollorganet må implementere egnede beslutningsprosedyrer for å sikre sin egen autonomi og uavhengighet.

1.1.2 Kontrollorganet skal opptre uavhengig i valget sitt og i bruk av tiltak og sanksjoner mot en behandlingsansvarlig eller databehandler som følger Normen.

1.1.3 Varigheten eller utløpet av mandatet til kontrollorganet må reguleres på en slik måte at man unngår at overavhengighet av en fornyelse eller frykt for å miste utnevnelsen kan påvirke uavhengigheten til kontrollorganet i dets utøvelse av kontrollaktiviteter.

1.1.4 Kontrollorganet skal ikke tilby tjenester til Norm-medlemmer eller Normeieren som kan påvirke kontrollorganets uavhengighet.

Eksempel

Slike tjenester kan relatere seg til utvikling eller forbedring av Normen eller rådgivning om implementasjon av Normen.

1.1.5 Kontrollorganet skal i søknadsprosessen dokumentere at kontrollorganet og dets personell kan opptre uavhengig og uten utilbørlig press.

Kontrollorganets uavhengighet i juridiske prosedyrer og beslutningsprosedyrer kan påvises gjennom:

a) formelle regler for utnevnelse
b) mandat, rammevilkår og stillingsbeskrivelser
c) dokumentert rekrutteringsprosesser for personelle
d) informasjon om personer i kontrollorganet som er autoriserte til å ta avgjørelser, som viser at det ikke foreligger noen sammenfallende interesser med de som skal kontrolleres
e) en beskrivelse av Normeieren
f) informasjon om kontrollorganets varighet eller opphør
g) evaluering og håndtering av risiko relatert til uavhengighet
h) dokumentasjon av forretningsmessige, økonomiske, avtalemessige eller andre forhold mellom kontrollorganet og Normeieren eller Norm-medlemmer.
i) for interne kontrollorganer, en beskrivelse av driften av enhver komité, separat avdeling eller personell som kan være involvert i kontrollorganet, og potensielle informasjonsbarrierer mellom og separate rapporteringslinjer for organisasjonen, virksomheten eller organet (dvs. Normeieren) og kontrollorganet.

1.2 Økonomiske ressurser

1.2.1 Kontrollorganet må være tilstrekkelig økonomisk uavhengig. Når den økonomiske uavhengigheten skal sikres, må kontrollorganet ta hensyn til antallet og størrelsen på Norm-medlemmer (som kontrollerte enheter), arten og omfanget av behandlingsaktivitetene deres (gjenstanden for Normen) og risikoen(e) knyttet til behandlingsaktiviteten(e).

1.2.2 Kontrollorganet må kunne håndtere budsjettet sitt og ressursene sine uavhengig og uten noen form for påvirkning fra Normeieren og Norm-medlemmene. Interne kontrollorganer må bevise at de er tildelt et eget og spesifikt budsjett av Normeieren.

Eksempel

Dersom reglene for økonomisk støtte tillater at et Norm-medlem, som er under granskning av kontrollorganet, stopper sine økonomiske bidrag for å unngå en potensiell sanksjon, vil ikke kontrollorganet bli ansett som økonomisk uavhengig.

1.2.3 Måten kontrollorganet får økonomisk støtte på (for eksempel gjennom medlemskontingent fra Norm-medlemmer) må ikke være egnet til å påvirke dets uavhengighet negativt.

1.2.4 Kontrollorganet må kunne påvise at det har økonomisk stabilitet og ressurser til å kunne utføre kontrolloppgavene sine på en effektiv og konsistent måte. Det må i tillegg foreligge nødvendige prosedyrer for å sikre at Normen fungerer over tid.

Eksempel

Dette kan demonstreres gjennom angivelse av inntektskilder, tidligere eller forventede inntekter og utgifter, samt detaljer om relevante eiendeler og gjeld.

1.2.5 Under søknadsprosessen skal kontrollorganet påvise ovenfor Datatilsynet hvordan det sikrer økonomisk støtte til dets kontrollvirksomhet, og forklare hvordan dette ikke svekker kontrollorganets uavhengighet.

1.3 Organisatoriske ressurser og struktur

1.3.1 Kontrollorganet må være organisert på en måte som gjør det i stand til å utføre oppgavene sine og utøve myndighet uavhengig av Normeieren og Norm-medlemmer innenfor Normens virkeområde.

1.3.2 Kontrollorganet må ha nødvendige menneskelige og tekniske ressurser for å kunne utføre oppgavene sine på en effektiv måte.

1.3.3 Kontrollorganet må være satt sammen av et tilstrekkelig og forholdsmessig antall personer slik at det kan utføre kontrolloppgavene sine. Sammensetningen skal gjenspeile den aktuelle sektoren, samt arten, omfanget, kompleksiteten og risikoene knyttet til behandlingsaktivitetene som omfattes av Normen.

1.3.4 Kontrollorganet skal stå til ansvar for – og beholde myndighet for – beslutningene sine vedrørende kontrolloppgavene. Personell i kontrollorganet kan holdes ansvarlige for handlingene sine i henhold til norsk lov.

1.3.5 Interne kontrollorgan må ha eget personell og egen ledelse for å sikre ansvarlighet og drift atskilt fra andre områder i organisasjonen (dvs. Normeieren). Det interne kontrollorganet må kunne opptre uten instrukser, og det skal være beskyttet fra enhver form for sanksjon eller forstyrrelser (enten direkte eller indirekte) som følge av utførelsen av dets oppgave.

Eksempel

Dette kan oppnås ved å bruke effektive organisatoriske barrierer og informasjonsbarrierer, separate rapporteringslinjer, eller andre former for logisk skille mellom kontrollorganet og Normeieren eller Norm-medlemmer.

1.3.6 Under søknadsprosessen skal kontrollorganet påvise sin organisatoriske uavhengighet ovenfor Datatilsynet.

Kontrollorganets bevis på organisatorisk uavhengighet kan gis ved

a) identifisering av risiko for organisatorisk avhengighet, samt hvordan kontrollorganet vil fjerne eller minimere risikoen og bruke av en egnet mekanisme for å ivareta upartiskhet
b) for interne kontrollorganer, organisasjonens oppsett og informasjon angående forhold til den større enheten som kontrollorganet inngår i (dvs. Normeieren).

1.4 Ansvarlighet

1.4.1 Kontrollorganet må kunne demonstrere at det står til ansvar for dets avgjørelser og tiltak for å kunne bli ansett som uavhengig.

Eksempel

Kontrollorganet kan påvise sin ansvarlighet ved å utarbeide et rammeverk for roller og beslutninger, rapporteringsprosedyrer samt tiltak for å øke bevisstheten blant personell om styringsstrukturer og gjeldende prosedyrer.

1.4.2 Enhver beslutning som tas av kontrollorganet relatert til dets funksjoner, skal ikke betinges av godkjennelse fra andre, herunder Normeieren.

1.4.3 Under søknadsprosessen må kontrollorganet kunne dokumentere ovenfor Datatilsynet at kontrollorganet er upartisk hva gjelder ansvarlighet.

Eksempel

Bevis på upartiskhet angående ansvarlighet kan blant annet være:

a) Stillingsbeskrivelser.
b) Rapporter fra ledelsen og opplæring av personalet (deriblant tiltak for å øke bevissthet blant personell om styringsstrukturer og gjeldende prosedyrer.

2. Interessekonflikter

Normeieren må påvise at kontrollorganets utøvelse av de angitte oppgavene og pliktene ikke kan føre til interessekonflikter. Det må derfor påvises at kontrollorganet og dets personell vil avstå fra handlinger som er uforenlige med kontrollorganets angitte oppgaver og plikter, og at det foreligger garantier som sikrer at kontrollorganet og dets personell ikke påtar seg uforenlig arbeid.

Kravene nedenfor skal bidra til å sikre at kontrollorganet kan utføre kontrolloppgavene på en upartisk måte, identifisere situasjoner som sannsynligvis fører til interessekonflikt, samt iverksette tiltak for å unngå dem.

2.1 Kontrollorganet må ha eget personell som er valgt av kontrollorganet selv, eller som er valgt av en annen virksomhet eller et annet organ som er uavhengig av Normen. Personellet skal kun være underlagt kontrollorganets ledelse.

Eksempel

Et eksempel på personell valgt av en virksomhet eller et organ som er uavhengig av Normen, er kontrollorganpersonell som har blitt rekruttert av et uavhengig, eksternt selskap som tilbyr rekrutterings- og HR-tjenester.

2.2 Kontrollorganet skal være fritt for ytre påvirkning, enten direkte eller indirekte. Kontrollorganet skal heller ikke etterspørre eller ta imot instrukser fra andre personer, virksomheter eller foreninger.

2.3 Kontrollorganet må ved utførelsen av dets oppgaver være beskyttet mot enhver form for sanksjon eller innblanding (enten direkte eller indirekte) fra Normeieren, andre relevante virksomheter eller organer eller Norm-medlemmer.

2.4 Kontrollorganet må identifisere situasjoner som sannsynligvis kan føre til interessekonflikter (på bakgrunn av dets personell, organisering, prosedyrer e.l.) og ha interne prosedyrer for å håndtere effektene av slike situasjoner. Prosedyrenes utforming vil variere avhengig av den gjeldende Normen.

Eksempel

Et eksempel på en interessekonflikt er et tilfelle der kontrollorganets personell skal undersøke og behandle klager mot virksomheten de jobber for. Eierskap, styring, ledelse, personell, delte ressurser, økonomi, kontrakter, tjenesteutsetting, opplæring, markedsføring og betaling av salgsprovisjoner er andre potensielle kilder til interessekonflikter.

Et eksempel på **ingen** interessekonflikt: å tilby tjenester som er rent administrative eller organisatorisk bistand eller støtteaktiviteter.

2.5 Dersom det oppstår interessekonflikter hos kontrollorganets personell, må de det gjelder gjøre rede for interessene sine, og arbeidet skal omfordeles.

2.6 Kontrollorganet skal fortløpende identifisere og fjerne risiko knyttet til dets upartiskhet.

2.7 Kontrollorganet må gjennomføre opplæringstiltak for å øke bevisstheten hos personellet sitt om situasjoner som sannsynligvis kan føre til interessekonflikt og de interne prosedyrene som gjelder i slike situasjoner.

2.8 Under søknadsprosessen må kontrollorganet informere Datatilsynet om kontrollorganets tilnærming til interessekonflikter. Kontrollorganets tilnærming til risikostyring (som påkrevd i punkt 2.4) og tilhørende prosedyrer må inkluderes i søknaden.

3. Dybdekunnskap

Kontrollorganet må ha det nødvendige nivået av dybdekunnskap for å kunne oppfylle rollen sin på en effektiv måte. Kravene nedenfor har som mål å sørge for at kontrollorganet har tilstrekkelig dybdekunnskap for å effektivt kunne kontrollere overholdelsen og etterlevelsen av Normen.

Datatilsynet bemerker at alle Normer som krever et kontrollorgan, må beskrive kompetansenivået som kontrollorganet må ha for å kunne levere Normens kontrollaktiviteter på en effektiv måte. Dybdekunnskapen til kontrollorganet må vurderes i henhold til den aktuelle Normen. Normspesifikke kriterier vil avhenge av faktorer som den aktuelle sektoren, behandlingsaktiviteten, de ulike interessene involvert og risikoen ved behandlingsaktivitetene som Normen dekker. Disse normspesifikke kriteriene vil regnes som en del av akkrediteringen. I alle tilfeller må kontrollorganet oppfylle kravene som listes opp under. Krav om ytterligere, eller mer spesifikk kompetanse, trenger kun å oppfylles i fall Normen forutsetter det.

Når Datatilsynet vurderer om kontrollorganet oppfyller kravene til dybdekunnskap, blir kontrollorganet vurdert som en helhet. Kvalifikasjonene og erfaringene til alt personell i kontrollorganet, blir derfor inkludert i denne vurderingen.

3.1 Kontrollorganet må ha dyptgående kunnskap om og erfaring med personvernlovgivningen samt sektoren og de aktuelle behandlingsaktivitetene som Normen gjelder.

3.2 Kontrollorganet må sørge for at personell som utfører kontrolloppgaver eller tar avgjørelser på vegne av kontrollorganet, har tilstrekkelig dybdekunnskap om sektoren og personopplysningsvern samt tilstrekkelig operativ erfaring, opplæring og kvalifikasjoner innen f.eks. revisjon, kontroll og kvalitetssikring.

3.3 Under søknadsprosessen må kontrollorganet påvise ovenfor Datatilsynet at det, i tillegg til å oppfylle kravene i punkt 3.1–3.2, også oppfyller de relevante kompetansekravene som er definert i Normen.

Dokumentasjon av kontrollorganets dybdekunnskap kan inkludere, men er ikke begrenset til:

a) kontrollorganets dokumenterte tidligere erfaring med å opptre i en kontrollerende egenskap innen en bestemt sektor
b) beskrivelse av personellets kompetanse og tidligere erfaringer i kontrollorganet
c) dokumentasjon på at personellet i kontrollorganet har gjennomgått opplæring i å utføre kontroll med etterlevelsen av Normen.
d) dokumentasjon relatert til personellets dybdekunnskap innen vern av personopplysninger, eksempelvis utdanning og personvernsertifikater.

4. Fastsatte prosedyrer og strukturer

Kontrollorganet må ha en kontrollmekanisme som er operasjonelt gjennomførbar. Kravene nedenfor skal sikre at kontrollorganets kontrollprosess er effektiv hva gjelder ressurser og prosedyrer.

Datatilsynet bemerker at selve Normen skal definere de korrigerende tiltakene og at kontrollorganet må bruke disse tiltakene slik definert i Normen.

4.1 Kontrollorganet må ha økonomisk stabilitet og få de ressursene som er nødvendige for at det effektivt skal kunne utføre oppgavene sine. Ressursene skal være forholdsmessige til den forventede størrelsen av og det forventede antallet Norm-medlemmer, samt til kompleksiteten eller graden av risiko ved den relevante databehandlingen og forventede mottatte klager.

4.2 Kontrollorganet må fastsette prosedyrer for å vurdere om behandlingsansvarlige og databehandlere er kvalifiserte og er i stand til å overholde Normen. Prosedyrene skal inkludere en vurdering av hvorvidt Norm-medlemmers behandling av personopplysninger faller innenfor virkeområdet til Normen. I tillegg skal kontrollorganet fremvise dokumentasjon på prosedyrer for å på forhånd, på ad hoc-basis og regelmessig kontrollere Norm-medlemmers etterlevelse innen klare tidsrammer, og sjekke Norm-medlemmers egnethet før de tilslutter seg Normen.

4.3 Kontrollorganet må fastsette prosedyrer for regelmessig, innen en klar og definert tidsperiode, å aktivt og effektivt kontrollere Norm-medlemmenes etterlevelse med Normens bestemmelser.

Eksempel

En kontrollprosedyre som angir metodikken som skal brukes, dvs. kravene som skal vurderes, kontrolltypen (egenevaluering, revisjon på stedet eller på avstand, bruk av anerkjente revisjonsstandarder, osv.), dokumentasjon av funnene, og lignende.

En prosedyre for undersøkelse, identifisering og håndtering av brudd på Normen og, der påkrevd, de korrigerende tiltakene som definert i Normen.

4.4 Kontrollorganet må fastsette prosedyrer for å aktivt og effektivt overvåke Norm-medlemmenes etterlevelse av Normens bestemmelser på ad hoc-basis. Ad hoc-kontroll kan blant annet etableres på grunnlag av en henvendelse eller klage fra en registrert.

4.5 Prosedyrene i punkt 4.3 og 4.4, og valget mellom disse, skal gjennomføres etter en risikobasert vurdering.

4.6 Kontrollorganets kontrollprosedyrer må ta for seg hele kontrollprosessen, fra forberedelsene av en evaluering og frem til det skal konkluderes. Prosedyrene må også inkludere ytterligere kontrollforanstaltninger som sikrer at passende tiltak treffes for å bøte på overtredelser og hindre gjentatte overtredelser.

4.7 Prosedyrer for å kontrollere etterlevelse av Normer må være tilstrekkelig spesifikke for å sikre en konsistent utøvelse av kontrollorganets forpliktelser.

4.8 Kontrollorganet må fastsette prosedyrer for å utføre periodiske gjennomganger av Normens drift. Ytterligere krav om mekanismer for gjennomgang av Normen er angitt i avsnitt 7.

4.9 Når de nødvendige prosedyrene etableres (for å undersøke egnethet, kontroll og gjennomgang), må kontrollorganet ta hensyn til risikoen som oppstår ved databehandlingen, forventet størrelse av og antall Norm-medlemmer, geografisk omfang, mottatte klager og andre relevante faktorer.

4.10 Kontrollorganet og dets personell har ansvaret for håndteringen av all informasjon som samles inn eller dannes under kontrollprosessen. Kontrollorganet og dets personell skal holde all informasjon som samles inn eller dannes gjennom utøvelsen av kontrollorganets kontrollaktiviteter konfidensielt, med mindre noe annet er påkrevd av lov eller kravene i dette dokumentet.

4.11 Med mindre annet følger av norsk lov, må kontrollorganet gjøre beslutninger om utfallet av sine fullførte kontroll- og gjennomgangsprosedyrer offentlig tilgjengelige, når de gjelder gjentatte og/eller alvorlige overtredelser, f.eks. slike som kan føre til suspensjon eller ekskludering av den aktuelle behandlingsansvarlige eller databehandleren fra Normen. Kontrollorganet må ellers gjøre publikasjoner eller oppsummeringer av avgjørelser eller statistiske data angående dets gjennomførte kontroll- og gjennomgangsprosedyrer, offentlig tilgjengelige.

4.12 Under søknadsprosessen må kontrollorganet påvise sine prosedyrer for vurdering av egnethet, samt kontroll- og gjennomgangsprosedyrer, ovenfor Datatilsynet.

5. Åpenhet i klagebehandlingen

Åpenhet og offentlig tilgjengelige prosedyrer og strukturer for å behandle klager fra ulike kilder i relasjon til Norm-medlemmer, er et essensielt element i kontroll med Koden. Kravene nedenfor skal bidra til å sikre implementeringen av et effektivt klagebehandlingssystem.

Datatilsynet bemerker at tilgjengelige klageprosedyrer skal være dekket i Normen.

5.1 Kontrollorganet må etablere effektive og klare prosedyrer og strukturer for behandling av klager.

> **Eksempel**
>
> Klagebehandlingsprosedyrer kan være en beskrevet prosess for hvordan kontrollorganet mottar, evaluerer, holder oversikt over, registrerer og løser klager.

5.2 Kontrollorganet må inkludere en rett til å bli hørt for klageren og Norm-medlemmet i prosedyrene sine.

5.3 Kontrollorganet må gjøre klageprosessen offentlig tilgjengelig og lett tilgjengelig. Veiledningen må være tilstrekkelig klar og åpen slik at klagere forstår den.

5.4 Kontrollorganet må etablere en tidsramme for å løse klager og gjøre denne informasjonen offentlig tilgjengelig. Klagene må løses innen rimelig tid. Hvis klagen ikke kan bli løst innen den anslåtte tidsrammen, må kontrollorganet informere klageren om forsinkelsen, årsaken til dette, og oppgi en ny tidsramme for å løse klagen. Datatilsynet forventer vanligvis at ikke-komplekse klager løses innen tre måneder.

5.5 Kontrollorganet må bekrefte mottak av klagen innen én måned.

5.6 I tilfelle brudd på en Norm, må kontrollorganet ha fastsatte prosedyrer for å umiddelbart iverksette handling og treffe korrigeringstiltakene som definert i Normen. Målet med slike prosedyrer må være å stanse overtredelsen og forhindre gjentakelse i fremtiden.

5.7 Kontrollorganet må være i stand til å informere klageren, Norm-medlemmet og Normeieren om tiltakene som er iverksatt, og begrunnelsen for dem, uten unødig forsinkelse.

5.8 Kontrollorganet må fastsette prosedyrer for gjenopptakelse av klager.

5.9 Kontrollorganet må føre protokoll over alle mottatte klager og trufne tiltak. Datatilsynet skal til enhver tid ha tilgang til denne protokollen.

5.10 Kontrollorganet må offentliggjøre informasjon om enhver sanksjon som fører til suspensjon eller ekskludering av Norm-medlemmer – og enhver eventuell påfølgende opphevelse av dette.

Eksempel

Eksempler på sanksjoner: opplæring, utstedelse av advarsel, rapportering til Norm-medlemmets styre, en formell meddelelse som krever gjennomføring av spesifikke tiltak innen en gitt frist, eller midlertidig utestengelse av Norm-medlemmet fra Normen inntil utbedrende tiltak er truffet. Disse tiltakene kan offentliggjøres av kontrollorganet, spesielt der det er alvorlige brudd på Normen.

5.11 Kontrollorganet må publisere informasjon om beslutningene som er tatt i forbindelse med klagebehandlingen. Den påkrevde informasjonen kan gis i form av generell statistisk informasjon om antall og type klager/overtredelser og beslutningene/de korrigerende tiltak som er utstedt.

5.12 Datatilsynet har kompetansen til å kontrollere kontrollorganets etterlevelse av artikkel 41 nr. 1, 2 og 4 i personvernforordningen, i henhold til personvernforordningen artikkel 57 nr. 1. Kontrollorganet må derfor fastsette prosedyrer for å informere klagere om dette og for å videresende relevante henvendelser om kontrollorganets kontrollaktivitet til Datatilsynet.

5.13 Under søknadsprosessen må kontrollorganet påvise dets klagebehandlingsprosedyrer og -strukturer ovenfor Datatilsynet.

6. Kommunikasjon med Datatilsynet

Kravene nedenfor skal sikre at kontrollorganets rammeverk legger til rette for effektiv kommunikasjon til Datatilsynet om tiltak iverksatt av kontrollorganet med hensyn til Normen. Dette inkluderer informasjon om enhver suspensjon eller ekskludering av Norm-medlemmer utstedt av kontrollorganet og alle vesentlige endringer i kontrollorganet. En vesentlig endring vil føre til en gjennomgang av akkrediteringen.

6.1 Kontrollorganet må fastsette klare rapporteringsmekanismer for å muliggjøre rapportering uten unødig opphold av enhver gjentatt eller alvorlig overtredelse (som kan føre til strenge reaksjoner fra kontrollorganet, slik som suspensjon eller ekskludering fra Normen) til Datatilsynet. Denne rapporten skal som minimum:

a) skriftlig og uten unødig opphold informere Datatilsynet om det korrigerende tiltaket med gyldig begrunnelse for avgjørelsen
b) gi informasjon om detaljene ved overtredelsen
c) gi informasjon om, og bevis for, tiltakene som er truffet

6.2 Kontrollorganet må være i stand til å gi all relevant informasjon om enhver av dets tiltak ved forespørsel fra Datatilsynet.

6.3 Kontrollorganet må ha en dokumentert prosedyre for gjennomgang og oppheving av en suspensjon eller ekskludering av et Norm-medlem og varsling om utfallet av gjennomgangen til Norm-medlemmet og Datatilsynet.

6.4 Kontrollorganet må fastsette rapporteringsmekanismer som gjør det mulig å gi regelmessige rapporteringer til Datatilsynet om resultatet av kontrollorganets gjennomganger av Normen.

6.5 Kontrollorganet må, uten unødig opphold, informere Datatilsynet om enhver vesentlig endring i kontrollorganet.

Vesentlige endringer kan blant annet omfatte:

a) endringer i kontrollorganets juridiske, kommersielle, eierskaps- eller organisatoriske status og nøkkelpersonell
b) endringer i ressurser og lokasjoner
c) enhver endring i grunnlaget for akkreditering
d) all annen informasjon som sannsynligvis kan sette spørsmålstegn ved kontrollorganets uavhengighet, dybdekunnskap og fraværet av enhver interessekonflikt eller som sannsynligvis kan påvirke kontrollorganets fulle drift.

6.6 Under søknadsprosessen må kontrollorganet påvise dets rapporteringsmekanismer ovenfor Datatilsynet.

7. Mekanismer for gjennomgang av Normen

Kravene nedenfor skal sikre at kontrollorganet kontinuerlig gjennomgår Normen i samsvar med gjennomgangsmekanismene angitt i Normen. Dette for å sikre at Normen forblir relevant og fortsetter å bidra til riktig anvendelse av personvernforordningen.

Datatilsynet bemerker at det er Normeierens ansvar å sikre at Normen fortsatt er relevant og etterlever gjeldende lovgivning. Kontrollorganet har ikke ansvar for gjennomføring av den oppgaven, men det skal bidra til enhver gjennomgang av Normen. Som et resultat av en gjennomgang av en Norm kan Normeieren endre eller utvide Normen.

7.1 Kontrollorganet må bidra til å gjennomføre gjennomganger av Normen slik angitt i Normen.

7.2 Kontrollorganet må sikre at det har dokumenterte planer og prosedyrer for å gjennomgå driften av Normen.

7.3 Når Normen gjennomgås, må kontrollorganet vurdere om Normen fortsatt er relevant for Norm-medlemmene og fortsetter å oppfylle anvendelsen av personvernforordningen. En slik vurdering skal som et minimum ta hensyn til eventuelle endringer i anvendelsen og tolkningen av loven og nye teknologiske utviklinger som kan ha en påvirkning på behandlingen som gjøres av Norm-medlemmer eller bestemmelser i Normen.

7.4 Kontrollorganet skal gi Normeieren og enhver annen enhet som er nevnt i Normen en årsrapport om driften av Normen. Rapporten skal inkludere:

a) bekreftelse av at det er blitt gjort en gjennomgang av Normen og informasjon om kontrollorganets funn og vurderinger som følge av gjennomgangen, samt hvorvidt det kreves endringer i Normen
b) informasjon om brudd på informasjonssikkerheten hos Norm-medlemmer, behandlede klager, samt type og utfall av kontrollfunksjoner som har funnet sted. Denne informasjonen kan inkludere, men er ikke begrenset til, generell statistisk informasjon om antallet og typen brudd på informasjonssikkerheten, klager, overtredelser og beslutningene/de korrigerende tiltak som er utstedt
c) bekreftelse på at det ikke er vesentlige endringer i kontrollorganet
d) informasjon om nye Norm-medlemmer

7.5 Kontrollorganet skal anvende oppdateringer av Normen som fastsatt av Normeieren.

7.6 Kontrollorganet skal påse at informasjon om dets fullførte gjennomganger, samt årsrapporten om driften av Normen, er dokumentert og tilgjengelig for Datatilsynet ved forespørsel.

7.7 Under søknadsprosessen skal kontrollorganet påvise dets gjennomgangsprosedyrer ovenfor Datatilsynet.

8. Rettsstilling

Kontrollorganet kan bli satt opp eller etablert på flere ulike måter, for eksempel som et aksjeselskap, en forening, en intern avdeling i Normeierens organisasjon eller som en fysisk person. Uansett hvilken form kontrollorganet har, må kontrollorganet påvise at formen egner seg for overvåkingsrollen, at organet har eget rettsstilling og at det kan utføre sin kontrollrolle og oppfylle de resulterende forpliktelsene.

Ordningen for etablering og medlemskap i kontrollorganet, dets beslutningsprosess, operasjonelle regler og varighet samt ressursene til dets disposisjon skal sikre at kontrollorganet kan utføre sine kontrolloppgaver og oppfylle de resulterende forpliktelsene gjennom hele dets varighet.

Datatilsynet bemerker at et kontrollorgan bare er ansvarlig for sin funksjon og sine oppgaver angitt i personvernforordningen artikkel 41. Kontrollorganet er ikke ansvarlig for Norm-medlemmers etterlevelse av bestemmelsene i personvernforordningen.

8.1 Kontrollorganet må være etablert i EØS.

8.2 Kontrollorganet må være i stand til å bli holdt juridisk ansvarlig for sine kontrollaktiviteter. Dette innebærer at overtredelsesgebyr etter personvernsforordningen artikkel 83 nr. 4 bokstav c og personopplysningsloven § 26 skal kunne ilegges kontrollorganet.

8.3 Under søknadsprosessen må kontrollorganet påvise ovenfor Datatilsynet at det er i stand til å treffe egnede tiltak i tråd med personvernforordningen artikkel 41 nr. 4 og at det kan oppfylle de resulterende forpliktelsene.

Dokumentasjon på dette vil være avhengig av kontrollorganets struktur, men kan omfatte:

a) informasjon om virksomheten og firmaet, eksempelvis i relasjon til stiftelsesdato, virksomhetenes identifikasjonsnummer (organisasjonsnummer), ansvarlige personer i virksomheten, antall ansatte, eventuelle relasjoner til andre virksomheter/organisasjoner, eierskapsdiagrammer, osv.
b) detaljer om relevante ressurser
c) relevante kontrakter, avtaler, mandat, rammevilkår, osv.

8.4 Under søknadsprosessen må kontrollorganet bekrefte ovenfor Datatilsynet at det påtar seg ansvar for sin kontrollrolle.

8.5 Kontrollorganet må påvise at det er i stand til å levere Normens overvåkingsmekanisme over et passende tidsrom. Normen i seg selv vil påvise at driften av Normens kontrollmekanismen er bærekraftig over tid.

8.6 Når kontrollorganet er en fysisk person, må det påvises at tilstrekkelige ressurser er tilgjengelige for den fysiske personens spesifikke oppgaver og plikter som kontrollorgan. Videre må det overveies og dokumenteres hvordan kontrollmekanismen er garantert over et passende tidsrom, og i fall oppsigelse eller midlertidig manglende evne hos personen det gjelder. I tillegg må det påvises at den fysiske personen har den nødvendige dybdekunnskapen (juridisk og teknisk).

9. Bruk av underleverandører

Kontrollorganet har det endelige ansvaret for beslutningstaking og etterlevelse når det bruker underleverandører. Kontrollorganet kan delegere noen av dets aktiviteter til andre parter, det vil si i forbindelse med gjennomføring av revisjoner. Ved bruk av underleverandører vil forpliktelsene som gjelder for kontrollorganet også gjelde tilsvarende for underleverandøren. Bruk av en underleverandør fjerner ikke kontrollorganets ansvar. Kravene nedenfor skal sikre at kontrollorganets aktiviteter satt til underleverandør er dokumenterte og har tilstrekkelige garantier.

9.1 Beslutningsprosesser kan ikke delegeres til underleverandør.

9.2 Når et kontrollorgan bruker underleverandører, skal kontrollorganet sikre effektiv kontroll av tjenestene som de kontraherte underleverandørene yter. I tillegg må kontrollorganet sørge for at tilstrekkelige garantier er på plass med hensyn til dybdekunnskapen, uavhengigheten, påliteligheten og ressursene til underleverandøren og at forpliktelsene som gjelder for kontrollorganet gjelder tilsvarende for underleverandøren.

Dette kan påvises gjennom dokumentasjon som kan inkludere:

a) skriftlige kontrakter eller avtaler med underleverandøren som skisserer forpliktelsene dens, herunder bestemmelser om konfidensialitet, hvilke typer data som blir behandlet og et krav om at dataene blir behandlet og oppbevart sikkert
b) klare prosedyrer for delegering til underleverandører skal også dokumenteres, og disse må inkludere vilkårene for når delegering til underleverandør kan finne sted, en prosess for godkjenning og kontroll med underleverandøren.

9.3 Når et kontrollorgan bruker underleverandører, må kontrollorganet sikre at underleverandørene etterlever personvernforpliktelsene sine. I tillegg skal det særlig sikre vilkårene for opphør av kontrakt for å sørge for at databehandleren oppfyller personvernforpliktelsene. Kontrakten eller avtalen med underleverandøren skal særlig spesifisere tilbakelevering eller sletting av personopplysninger ved opphør av kontrakten eller avtalen for å sikre at underleverandøren oppfyller personvernforpliktelsene, jf. artikkel 28 punkt 3 bokstav g i personvernforordningen.

9.4 Når kontrollorganet søker om akkreditering, skal kontrollorganet identifisere alle sine underleverandører og gi Datatilsynet informasjon om oppgavene deres og rollen de utfører. Kontrollorganet skal gi den samme informasjonen til Datatilsynet dersom kontrollorganet skaffer en ny underleverandør etter akkrediteringen. Datatilsynet må også informeres dersom kontrollorganet slutter å bruke noen av sine underleverandører.