

Internkontroll AS Arbeidsinstruks; Gjennomførings av bakgrunnssjekk

Internkontroll AS
Steinhaugen 11
7049 Trondheim

Svein Roar Holt
Oppdatert 11.12.2025



DOKUMENTNAVN

Dokumentnr.:	
Versjonsnr.:	
Dokumenteier:	
Vedtaksdato:	
Overordnet ansvarlig:	
Gjennomføringsansvarlig:	
Kvalitetssikringsansvarlig:	
Overvåkingsansvarlig:	
Dokumenthjemmel:	

1. Formål:

Formålet med denne instruks er å etablere et lovhemlet, systematisk og proporsjonalt rammeverk for bakgrunnssjekk. Instruks er et dokumentert nødvendig kontrolltiltak for å sikre virksomhetens forsvarlige drift, integritet og etterlevelse av gjeldende lovverk (herunder GDPR og Arbeidsmiljøloven).

2. Omfang:

Instruks omfatter og er bindende for alle interne prosesser knyttet til bakgrunnssjekk. Den gjelder for alt personell involvert i rekruttering, ansettelse og overvåking av etterlevelse. Omfanget av bakgrunnssjekken skal alltid være proporsjonalt med stillingens dokumenterte risiko, jf. Del 2 og 3.

3. Avvik:

Ethvert identifisert avvik fra instruks skal uten opphold registreres for avviksbehandling iht. gjeldende instruks for dette.

I de tilfeller det blir identifisert avvik som skyldes forsettlig- eller grovt uaktsom fravikelse av arbeidsinstruks skal daglig leder og virksomhetens Internkontrollansvarlige vurdere hvorvidt det er begått et alvorlig brudd på inngått arbeidsavtale.

4. Personinformasjon:

All behandling av personopplysninger skal skje i fullt samsvar med GDPRs grunnprinsipper (lovlighet og nødvendighet). Behandlingen må være dokumentert i virksomhetens register over behandlingsaktiviteter og skal kun omfatte opplysninger som er strengt nødvendige og saklige for stillingen. Virksomhetens personvernerklæring skal til enhver tid være ajourført og reflektere behandlingen beskrevet i denne instruks.

5. Helse-, miljø- og sikkerhet:

Gjennomføringen av bakgrunnssjekken er et obligatorisk forebyggende tiltak i virksomhetens systematiske HMS-arbeid, slik det kreves i Internkontrollforskriften. Instruks skal bidra til å sikre at ansatte med tilgang til kritiske områder, sensitiv informasjon, eller som har et særskilt HMS-ansvar, har den nødvendige integriteten og påliteligheten. Dette reduserer risikoen for personell som kan

utgjøre en trussel mot arbeidstakernes sikkerhet, det fysiske arbeidsmiljøet, eller som kan forårsake skade på kritiske systemer.

6. Gjennomføringsinstruks

Instruksen er delt i tre nivåer basert på risiko og lovpålagte krav (AML, GDPR og Sikkerhetsloven). Instruksen må følges for å sikre lovlighet og redusere virksomhetsrisiko.

Del 1: Etablering og Forankring av Instruksen (Systemansvar)

Denne delen definerer det juridiske og organisatoriske grunnlaget for å iverksette bakgrunnssjekker, og skal gjennomføres én gang før Instruksen tas i bruk.

1.0. Bakgrunn og formål (Risikoreduksjon)

Denne instruksjonen etableres som et obligatorisk beredskapstiltak etter at gjennomført risiko- og råbarhetsanalyse (ROS-analyse) har konkludert med at:

a)
Sannsynligheten og konsekvensen av en uønsket hendelse forårsaket av manglende integritet hos ansatte er uakseptabelt høy.

b)
Implementering av denne instruksjonen er et nødvendig styringstiltak for å eliminere eller redusere denne identifiserte risikoen til et akseptabelt nivå, i tråd med virksomhetens krav til forsvarlig drift.

1.1. Juridisk hjemmelsgrunnlag og interesseavveining (GDPR)

Virksomhetens behandling av personopplysninger i forbindelse med bakgrunnssjekk skal utelukkende baseres på følgende rettslige grunnlag og lovkrav:

a)
Lovlighet og saklighet: All innhenting av opplysninger må ha saklig grunn i stillingen (Arbeidsmiljøloven § 13-4) og må være nødvendig for å fastslå kandidatens kvalifikasjoner eller egnethet.

b)
Rettslig grunnlag (GDPR): Behandlingen baseres primært på interesseavveining (GDPR artikkel 6 (1) f).

1.1.1. Dokumentasjon av interesseavveiningen

Før denne instruksjonen iverksettes, skal det dokumenteres at virksomhetens interesse i bakgrunnssjekken veier tyngre enn kandidatens personvern, ved å vurdere de tre følgende punktene:

a)
Formålstesten (Legitimt Interesse): Virksomhetens interesse i å beskytte vesentlige forretningsinteresser og sensitiv informasjon ved å ansette personell med dokumentert integritet, anses som en berettiget og legitim interesse.

b)
Nødvendighetsprinsippet: Bakgrunnssjekken er nødvendig fordi enkle intervjuer og CV-gjennomgang alene er utilstrekkelige for å vurdere risikoen knyttet til stillinger med høy tillit og tilgang til kritiske systemer/data.

c)

Avveiningen (Proporsjonalitet): Virksomhetens interesse i å redusere risikoen veier tyngre enn inngrepet i kandidatens personvern, forutsatt at:

- Omfanget av sjekken er proporsjonalt med risikoen (Standard vs. Utvidet).
- Kun saklige og nødvendige opplysninger behandles (Dataminimering).

1.2. Obligatorisk risikovurdering av behandlingen (ROS-analyse)

Før denne Instruksen tas i bruk, skal det gjennomføres én systematisk ROS-analyse av selve Instruksen for bakgrunnssjekk, som skal dokumenteres i internkontrollsystemet.

Formål:

Identifisere og vurdere risiko for de registrertes rettigheter og friheter som følge av prosessen.

Tiltak:

ROS-analysen må bekrefte at alle sikkerhetstiltak i denne instruksen er tilstrekkelige for å redusere risikoen til et akseptabelt nivå.

1.3. Krav til samtykke for særlige opplysninger og kontakter

Uavhengig av Interesseavveiningen, må det innhentes eksplisitt, informert samtykke fra kandidaten før følgende handlinger utføres:

a)

Kontakt med uoppgitte referanser: Før det tas kontakt med personer, ledere eller tidligere arbeidsgivere som ikke er oppgitt av kandidaten i søknaden.

b)

Særlige kategorier av personopplysninger og straffedommer/lovovertridelser:

Før det behandles informasjon som faller inn under enten GDPR Artikkel 9 eller Artikkel 10, da dette i utgangspunktet er forbudt uten særskilt hjemmel:

Kategori (GDPR Artikkel 9)	Omfatter (eksempler)
Helseopplysninger	Medisinske diagnoser, behandlinger, fraværsmønstre som indikerer helsetilstand.
Biometriske opplysninger	Fingeravtrykk, ansiktsgjenkjenning (brukt til identifisering).
Genetiske opplysninger	Informasjon om arvelige egenskaper.
Etnisk/Rasesmessig Opprinnelse	Informasjon om nasjonalitet eller kulturell bakgrunn.
Politisk/Religiøs Overbevisning	Opplysninger om politisk tilhørighet, religiøs tro eller livssyn.
Fagforeningsmedlemskap	Opplysninger om medlemskap i en fagforening.
Seksuell Orientering/Forhold	Opplysninger om en persons seksuelle liv eller orientering.
Straffedommer og Lovovertridelser (GDPR Artikkel 10)	Før det innhentes eller behandles opplysninger om straffedommer, straffbare forhold eller sikkerhetstiltak (med mindre det foreligger særskilt lovhjemmel, f.eks. Politiattest).

Dersom virksomheten ser behov for å behandle informasjon fra disse kategoriene, må det enten foreligge særskilt lovhjemmel (f.eks. for politiattest ved lovpålagt krav) eller det må innhentes eksplisitt samtykke (Art. 9(2)a) for å sikre lovlig behandling.

1.4. Endringer i personvernerklæringen og styringsdokumenter

Innføring av bakgrunnssjekk som fast Instruks krever umiddelbar oppdatering av virksomhetens personvernerklæring.

Krav til personvernerklæringen:

Erklæringen må oppdateres for å inkludere: Formålet, det rettslige grunnlaget (Interesseavveining), og kategorier av opplysninger som samles inn, samt kravet om samtykke ved behov.

Krav til stillingsannonser:

Alle stillingsannonser for stillinger som omfattes av utvidet omfang eller sikkerhetsloven, må informere om at grundig bakgrunnssjekk vil bli gjennomført.

Del 2: Operativ gjennomføring av bakgrunnssjekk (Linjeansvar – AML/GDPR)

Denne delen beskriver den obligatoriske saksbehandlingen som må følges for hver enkelt kandidat til ordinære stillinger som *ikke* omfattes av Sikkerhetsloven.

2.1. Innledende krav og samtykke

Informasjonsplikt:

Kandidaten må informeres skriftlig og tydelig om formålet og omfanget av bakgrunnssjekken (Standard eller Utvidet).

Samtykke må innhentes:

Ansvarlig rekrutterer må innhente eksplisitt samtykke fra kandidaten for handlingene spesifisert i Punkt 1.3.

2.2. Standard omfang (Ordinære stillinger)

Dette omfanget er tilstrekkelig for stillinger uten tilgang til kritiske IKT-systemer eller store økonomiske verdier.

Sjekkpunkt	Gjennomføring	Fokus
Dokumentvurdering	Kontrollere konsistens i CV og attester/vitnemål.	Sikre at kvalifikasjonene er som oppgitt.
Referansesjekk (Oppgitte)	Gjennomfør intervju med minimum to referanser oppgitt av kandidaten.	Få bekreftet faglige kvalifikasjoner, arbeidskapasitet og samarbeidsevne.
Offentlig Tilgjengelig Info	Gjennomgå LinkedIn/faglige profiler for å bekrefte karrierehistorikk.	Unngå innsyn i private sosiale medier.

2.3. Utvidet omfang (Høyrisikostillinger)

Dette omfanget er obligatorisk for stillinger som krever høy integritet (f.eks. Økonomisjef, IT-driftssjef, HR-ansvarlig).

Sjekkpunkt	Gjennomføring	Fokus
Alt i Standard Omfang	Obligatorisk.	
Tilleggsreferanser	Innhent eksplisitt samtykke for å kontakte tidligere nærmeste leder/relevant	Integritet, etisk dømmekraft, håndtering av

	kollega som ikke er oppgitt som referanse.	konfidensialitet og tillitsbrudd.
Negativ Pressekontroll	Gjennomfør åpent søk (Google) for å avdekke offentlig kjent, relevant negativ medieomtale (f.eks. økonomisk kriminalitet, varslingsaker, etiske brudd) som har saklig relevans for stillingen.	Redusere omdømmerisiko og forhindre uegnethet.
Politiattest (ved lovhjemmel)	Dersom lovhjemmel foreligger (f.eks. for stillinger med arbeid med barn), kreves godkjent attest.	Lovpålagt sikkerhet.
Reiseaktivitet til Høyrisikoland	MÅ IKKE innhentes, med mindre det foreligger særskilt dokumentert behov i ROS-analysen. Dersom det er relevant, sjekkes kun offentlig tilgjengelig informasjon.	Kun tillatt hvis relevant for sikkerhetsrisiko/eksportkontroll, og aldri som et generelt krav.

2.4. Dokumentasjon og avvikshåndtering

Protokoll:

Resultatet av bakgrunnssjekken må nedfelles i Protokoll for bakgrunnssjekk.

Saklighetsvurdering:

Dersom bakgrunnssjekken avdekker forhold som kan føre til avslag, må det foretas en skriftlig saklighetsvurdering som begrunner hvorfor funnet gjør kandidaten uegnet for stillingen.

Dataminimering og sletting (GDPR):

All informasjon om ikke-ansatte må slettes umiddelbart etter at ansettelsesprosessen er avsluttet.

Avvikshåndtering:

Ethvert brudd på denne Instruksen (f.eks. uautorisert innsamling av data) må behandles som et avvik i styringssystemet.

2.5. Forbud mot Innhenting av Diskriminerende opplysninger

Det er strengt forbudt å innhente, behandle eller basere ansettelsesbeslutninger på informasjon om Egen Nasjonalitet, Etnisitet, Hudfarge eller Nasjonalitet på familiemedlemmer.

Slike handlinger er i strid med norsk lov og GDPR og utgjør et alvorlig avvik i virksomhetens styringssystem.

Del 3: Tilleggskrav for stillinger omfattet av sikkerhetsloven (Gradert Informasjon)

Denne delen er obligatorisk for alle stillinger som har tilgang til gradert informasjon eller skjermingsverdige objekter/infrastruktur som er underlagt den norske Sikkerhetsloven.

3.1. Definisjon og omfang

Omfang:

Omfatter stillinger som krever enten sikkerhetsklarering (tilgang til gradert informasjon) eller autorisasjon (tilgang til skjermingsverdige objekter/IKT-systemer).

Formål:

Primærfunksjonen er å verifisere kandidatens lojalitet, pålitelighet og sårbarhet for ytre påvirkning (f.eks. spionasje/sabotasje).

3.2. Den obligatoriske sikkerhetsklareringsprosessen

For disse stillingene må prosessen følge Sikkerhetslovens kapittel 8 og tilhørende forskrifter:

Sikkerhetsinstruks:

HR/rekruttering må orientere kandidaten om kravet til klarering og innhente samtykke til sikkerhetsundersøkelse i henhold til Sikkerhetsloven.

Sikkerhetsundersøkelse:

Kandidaten må gjennomføre en sikkerhetsundersøkelse utført av autorisert organ (PST/NSM). Denne undersøkelsen er lovhjemlet og går foran GDPR og AMLs generelle regler for innhenting av informasjon.

Klareringsvedtak:

Virksomheten må ikke gi tilgang til gradert informasjon før et gyldig klareringsvedtak er fattet av klareringsmyndigheten.

3.3. Avslag på grunnlag av sikkerhetsrisiko

Avslag på grunn av risiko for spionasje/skadeverk kan kun gis basert på følgende:

a)

Avslått klarering/autorisasjon: Dersom klareringsmyndigheten konkluderer med at det foreligger en sikkerhetsrisiko (f.eks. risiko for spionasje eller sabotasje fra fiendtlig nasjon) og nekter å klarere kandidaten for stillingen.

b)

Virksomhetens Rolle: Virksomheten som arbeidsgiver må da avvise kandidaten på grunnlag av at vedkommende ikke oppfyller lovpålagte sikkerhetskrav for stillingen. Avslaget dokumenteres med henvisning til det formelle vedtaket om nektet klarering/autorisasjon.

7. Kvalitetssikringsinstruks

Virksomhetens internkontrollansvarlig-e skal kvalitetssikre at nødvendig ROS-analyse er gjennomført før instruksen blir tatt i bruk, og at resultatet av denne verifiserer instruksens innhold.

Virksomhetens internkontrollansvarlig-e skal kvalitetssikre at virksomhetens personvernerklæring er rettmessig ajourført før instruksens innhold blir tatt i bruk.

Virksomhetens internkontrollansvarlig-e skal kvalitetssikre at det er innført nødvendige regulatoriske grep for å sikre at stillingsannonser for stillinger som omfattes av utvidet omfang eller sikkerhetsloven er rettmessig ajourført mht. informasjon om bakgrunnssjekk før instruksens innhold blir tatt i bruk.

Rekrutterende leder skal utøve kvalitetssikring av etterlevelse i samsvar med instruksens innhold i form av

egenkontroll dokumentert ved signering av de respektive bakgrunnssjekksprotokollene.

8. Overvåking

Virksomhetens internkontrollansvarlig-e skal overvåke etterlevelse av instruksen.