Veileder om kontroll og overvåking i arbeidslivet

Arbeidstilsynet · Datatilsynet · Petroleumstilsynet · Partene i arbeidslivet

Innhold

Innhold 2
Innledning 3
Om denne veilederen 4
5 grunnleggende råd om kontrolltiltak på arbeidsplassen 6
Kort om nøkkelbegrepene 7
Hva er et kontrolltiltak? 7
Hva er en personopplysning? 7
Hva er internkontroll? 8
Roller og ansvar 9
Arbeidsgiver 10
Arbeidstakere med lederansvar 10
Verneombud 10
Tillitsvalgte 10
Behandlingsansvarlig 10
Databehandler 11
Personvernombud 11
Slik går dere frem ved innføring av kontrolltiltak 12
Fase 1: Vurder behov og kartlegg risiko 15
Fase 2: Ta en beslutning, planlegg og forbered 19
Fase 3: Gjennomfør 23
Fase 4: Evaluer og følg opp 25
Vanlige kontrolltiltak 28
Kameraovervåking 29
Innsyn i e-post 31
Adgangskontroll 33
Tidsregistrering 34
Veskekontroll 35
«Hemmelig kunde/gjest» 36
Bruk av styringsverktøy utenfor fast arbeidssted 37
Opptak av telefonsamtaler 38
Tilgang til ansattes mobiltelefon – Mobile Device management 39
GPS-sporing og annen lokalisering i yrkesbiler 40
Innhenting av helseopplysninger ved ansettelse 42
Medisinske undersøkelser og rus-testing av arbeidssøkere og arbeidstakere 43
Regelverket 46
Balansen mellom arbeidsgivers styringsrett og arbeidstakers rett til personvern 47
Myndighetene: 54
Arbeidstilsynet 55
Datatilsynet 55
Personvernnemnda 56
Petroleumstilsynet 56
Bakgrunnsmateriale og forskning: 57
Ni gode råd ved innføring av kontrolltiltak på arbeidsplassen 58

Innledning

Ny teknologi bidrar til det høye velstands- og velferdsnivået i Norge, men kan også gi arbeidsmiljø- og personvernutfordringer.

I noen sammenhenger brukes opplysninger til kontroll og overvåking av arbeidstakere.

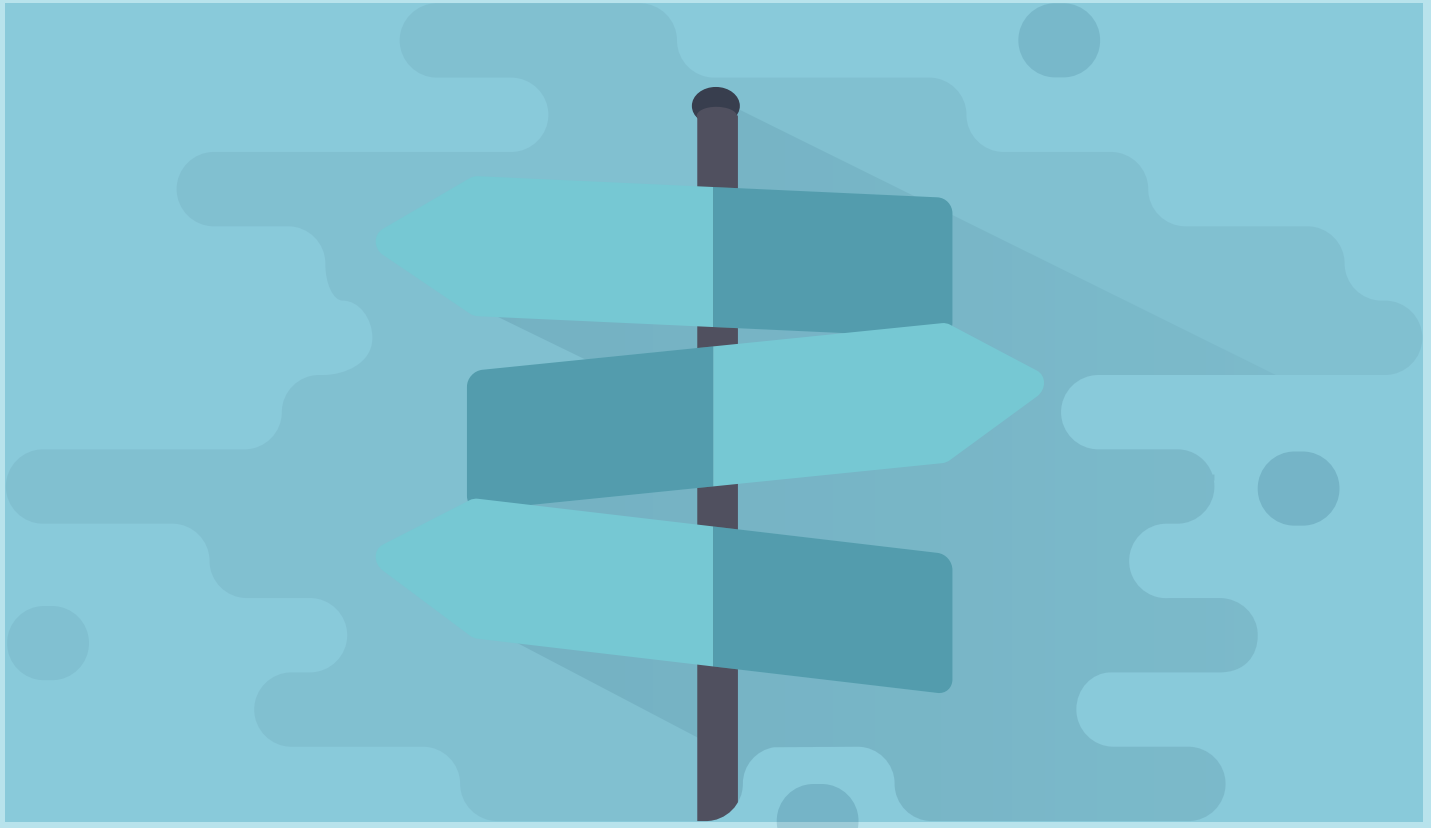
Kontroll og overvåking av ansatte handler i hovedsak om to motstridende interesser på arbeidsplassen: arbeidsgiverens ønske om og behov for kontrolltiltak og arbeidstakerens arbeidsmiljø og personverninteresser. Samtidig kan det ofte være i felles interesse å innføre nyttige arbeidsverktøy som også kan falle inn under regelverket. Viktige spørsmål er hvilke konsekvenser den nye teknologien kan få for arbeidsmiljøet, og hvordan virksomhetene skal ta vare på arbeidstakernes rett til personvern. Et grunnleggende prinsipp er at alle har krav på personvern og privatliv – også på jobb.

Kontrolltiltak rettet mot arbeidstakere er regulert i arbeidsmiljøloven kapittel 9.

Virksomheter innfører ofte styringsverktøy av driftsmessige årsaker og ikke fordi de planlegger å overvåke de ansatte. Likevel bør virksomheten alltid vurdere om verktøyene gjør det teknisk mulig å kontrollere eller overvåke arbeidstakerne. For å sikre at arbeidstakerne har fått tilstrekkelig informasjon om tiltakene, kan det være hensiktsmessig at arbeidsgiveren følger samme fremgangsmåte som når virksomheten planlegger kontrolltiltak.

Personopplysningsloven regulerer innsamling og bruk av personopplysninger. I dagens digitaliserte arbeidsliv vil innføring av de fleste kontrolltiltak føre til at det samles inn og brukes personopplysninger.

Dette innebærer at både personvernregelverket og arbeidsmiljøregelverket må etterleves samtidig. De to regelverkene har en del krav som er svært like, mens andre krav er særegne. Denne veilederen skal gjøre det enklere å etterleve alle kravene samtidig.



Om denne veilederen

Kapittel 1

Om denne veilederen

Formålet med denne veilederen er å gi virksomheten en enkel oppskrift på hvordan man kan finne frem i regelverket og gjennomføre gode medvirkningsprosesser.

På den måten ivaretas arbeidsmiljøet og personopplysningsvernet ved vurdering, planlegging og innføring av kontrolltiltak.

Veilederen er skrevet for deg som er leder eller arbeidsgiver, men den er også aktuell for verneombud, tillitsvalgte, personvernombud, arbeidstakere og andre som arbeider med personvern, kontroll og overvåking på arbeidsplassen. Veilederen gir svar på vanlige spørsmål om arbeidsgiverens ansvar, plikter og muligheter når det innføres kontrolltiltak. De fleste virksomheter må etterleve flere regelverk samtidig, blant annet arbeidsmiljøloven og personopplysningsloven.

Det finnes også bestemmelser om kontrolltiltak i Hovedavtalene som er inngått mellom de ulike arbeidsgiver- og arbeidstakerorganisasjonene, og som gjelder for tariffbundne bedrifter. Eksempelvis gjelder *Tilleggsavtale V til Hovedavtalen LO-NHO* for bedrifter som er bundet av Hovedavtalen LO–NHO. Arbeidsgiverens plikter etter denne avtalen samsvarer i grove trekk med lovgivningen, og omtales ikke nærmere her. Andre tariffavtaler har lignende formuleringer.

Veilederen er laget av Arbeidstilsynet, Datatilsynet og Petroleumstilsynet sammen med partene i arbeidslivet.

5

grunnleggende råd om kontrolltiltak på arbeidsplassen

1. Innføring av kontrolltiltak skal drøftes med arbeidstakernes tillitsvalgte. Husk at verneombudet skal tas med på råd, og at arbeidsmiljøutvalget skal behandle planer som kan få vesentlig betydning for arbeidsmiljøet.

2. De ansatte skal være informert om
   - at kontroll og overvåking finner sted
   - hvordan kontroll og overvåking skjer
   - hva opplysningene skal brukes til
   - eventuelle endrede formål med kontrollen og overvåkingen

3. Arbeidsgiveren skal vurdere om andre metoder er tilstrekkelige, og må velge den minst inngripende løsningen.

4. Kontrolltiltak skal
   - være saklige i forhold til den virksomheten som drives
   - stå i forhold til problemene virksomheten ønsker å løse
   - samlet sett ikke være for inngripende

5. Kontrolltiltak skal evalueres jevnlig.

Kort om nøkkelbegrepene

Hva er et kontrolltiltak?

Kontrolltiltak i arbeidslivet kan dreie seg om en rekke forskjellig forhold – fra fysisk kontroll til teknologisk overvåking. Fysisk kontroll kan være alt fra kontroll av vesker til rusmiddeltesting eller andre helseundersøkelser. Mest utbredt er likevel ulike former for elektronisk overvåking.

Eksempler på kontrolltiltak kan være:

- Helseundersøkelser og innhenting av helseopplysninger
- Overvåking av telefonbruk
- Kameraovervåking i arbeidslokalene
- Tilgangskontroll
- Produksjonskontroll og styringssystemer
- Sporingsteknologi i virksomhetens kjøretøy og flåtestyring
- Kontroll av e-post og besøk på internettsider
- Ransaking eller kroppsvisitering
- Testing for å avdekke rusmiddelbruk bruk av private etterforskere – for eksempel såkalte «hemmelige kunder»

Hva er en personopplysning?

En personopplysning er en opplysning eller vurdering som kan knyttes til en enkeltperson, slik som navn, telefonnummer, bilder, fingeravtrykk eller fødselsnummer.

Personopplysninger kan handle om hva som helst. Opplysninger om atferdsmønstre, personlighet, meninger eller smak kan være personopplysninger. Detaljopplysninger om når du kommer på jobb, hvor du beveger deg i løpet av en dag, og hva du søker etter på nettet, er også personopplysninger. I dagens arbeidsliv legger vi igjen mange personopplysninger i form av ulike digitale spor.

Informasjon kan være personopplysninger selv om det ikke går frem hvem den handler om. Det er tilstrekkelig at det er *mulig å finne ut* hvem opplysningene handler om. Det er heller ikke et krav at opplysningene er sanne, for at de skal regnes som personopplysninger – det holder at de er knyttet til en person.

Sensitive personopplysninger er opplysninger om rasemessig eller etnisk bakgrunn, politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,seksuelle forhold, helseforhold eller medlemskap i fagforeninger. Det er strengere regler for når sensitive personopplysninger kan samles inn og brukes, enn for alminnelige personopplysninger. Bruk av sensitive personopplysninger vil i en del tilfeller innebære at virksomheten må søke Datatilsynet om konsesjon.

Begrepet behandling av personopplysninger betyr ganske enkelt bruk av personopplysninger, som innsamling, registrering, sammenstilling, lagring og utlevering, eller en kombinasjon av slike bruksmåter.

Hva er internkontroll?

Internkontroll er et planmessig og systematisk styringssystem som virksomheter må etablere for å oppdage brudd på regelverket.

Krav om internkontroll finnes på en rekke områder, for eksempel krav etter HMS-lovgivingen, helse- og omsorgslovgivningen, næringsmiddellovgivningen og lovgivningen om personvern og informasjonssikkerhet.

Mange virksomheter synes det er hensiktsmessig å bruke et felles styringssystem for å oppfylle de ulike internkontrollpliktene. Små bedrifter med lite risikofylt aktivitet behøver som oftest ikke noe omfattende system.

Internkontroll som gjelder helse, miljø og sikkerhet, skal sikre at problemer blir oppdaget og tatt hånd om i tide.*

Internkontroll brukes også for å sikre etterlevelse av personopplysningsloven med forskrift. Virksomheten må etablere og vedlikeholde planlagte og systematiske tiltak for å sikre at den oppfyller lovens krav til behandling av personopplysninger.**

Dette betyr at eksisterende internkontroll må suppleres, slik at det nye tiltaket blir inkludert i internkontrollsystemet/-systemene.

Videre lesning

* Les om internkontroll og HMS på arbeidstilsynet.no

** Les om internkontroll og personopplysninger på datatilsynet.no

Roller og ansvar

Kapittel 2

Lær mer om:

- Arbeidsgiver
- Arbeidstakere med lederansvar
- Verneombud
- Tillitsvalgte
- Behandlingsansvarlig
- Databehandler
- Personvernombud

Roller og ansvar

Arbeidsgiver

Arbeidsgiveren har ansvar for at hensynet til helse, miljø og sikkerhet blir ivaretatt, og for at arbeidstakerne ikke utsettes for uheldige fysiske eller psykiske belastninger som følge av kontrolltiltak.

Arbeidstakere med lederansvar

Arbeidstakere med lederansvar skal sørge for at hensynet til helse, miljø og sikkerhet (HMS) blir ivaretatt.

Verneombud

Verneombudet skal ivareta arbeidstakernes interesser i arbeidsmiljøsaker. Verneombudet skal tas med på råd ved planlegging og gjennomføring av tiltak som har betydning for arbeidsmiljøet.

Tillitsvalgte

Tillitsvalgte ivaretar medlemmenes interesse i henhold til lov- og avtaleverk. Tillitsvalgte er viktige samarbeidspartnere for arbeidsgiverne i det systematiske HMS-arbeidet. De kan drøfte, forhandle og inngå eventuelle avtaler med arbeidsgiveren om kontrolltiltak.

Behandlingsansvarlig

Behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysningene og hvilke hjelpemidler som skal brukes. For kontrolltiltak er behandlingsansvarlig nesten alltid virksomheten selv (arbeidsgiveren), representert ved virksomhetens øverste administrative leder. Den behandlingsansvarlige har ansvaret for at kravene i personopplysningsloven blir fulgt.

Databehandler

En databehandler er den som behandler personopplysninger på vegne av den behandlingsansvarlige. Mange virksomheter bruker eksterne IT-leverandører. Disse vil være databehandlere dersom de samler inn, lagrer eller bruker personopplysninger for den ansvarlige virksomheten.

Databehandleren har ingen egen råderett over opplysningene, men har et selvstendig ansvar for å ha tilfredsstillende informasjonssikkerhet for å verne personopplysningene. Det må inngås en skriftlig avtale mellom den behandlingsansvarlige og databehandleren, en databehandleravtale. Avtalen skal beskrive hva databehandleren skal gjøre på vegne av den ansvarlige virksomheten. Databehandleren kan ikke gjøre noe med personopplysningene utover det som er avtalt.

Personvernombud

Et personvernombud skal styrke virksomhetens personvernkompetanse og bistå den behandlingsansvarlige i å følge personopplysningsloven med forskrift. Ombudet kan være ansatt internt i virksomheten eller en ekstern ressursperson. Ordningen er frivillig.

Ved oppnevning av personvernombud kan virksomheter søke Datatilsynet om fritak fra meldeplikt, og Datatilsynet fatter et vedtak om dette. Datatilsynet tilbyr kurs og annet faglig tilbud til personvernombud i disse virksomhetene.

Slik går dere frem ved innføring av kontrolltiltak

Kapittel 3

Slik går dere frem ved innføring av kontrolltiltak

De aller fleste virksomheter er underlagt krav om å drive systematisk helse-, miljø- og sikkerhetsarbeid.

Innføring av kontrolltiltak bør knyttes til det overordnede systematiske HMS-arbeidet. Når virksomheten vurderer å innføre kontrolltiltak, må den gjennomføre en kartlegging og en risikovurdering av tiltakene.

Arbeidstakerne og deres tillitsvalgte har en sentral rolle i arbeidet med helse, miljø og sikkerhet. For å lykkes er det nødvendig at arbeidstakerne deltar i planleggingen, i kartleggingen, i den daglige driften og i å finne gode løsninger.

Verneombudet skal tas med på råd under planleggingen av alle tiltak som har betydning for arbeidsmiljøet, også når det planlegges kontroll- og overvåkingstiltak.

Modell – fire faser og gjøremål for å ivareta både arbeidsmiljø- og personvernbestemmelsene

Figuren på neste side beskriver fire faser ved innføring av kontrolltiltak: vurdering av behov og kartlegging, beslutning, planlegging og forberedelser, gjennomføring, samt evaluering og oppfølging. Figuren gjenspeiler at det systematiske arbeidet i virksomheten er et kontinuerlig arbeid.

Til hver fase er det knyttet noen sentrale spørsmål og et sett av oppgaver og sjekkpunkter. Når dere går igjennom alle fasene, ivaretar dere hensynet til både arbeidsmiljø og personvern.

Regelverkslenke

Arbeidsmiljøloven kap. 6 om verneombud

1

Hva ønsker virksomheten å oppnå?

Hvilke løsninger dekker behovet?

Er den arbeidsmiljømessige risikoen og personvernkonsekvensene kartlagt og vurdert?

Har arbeidsgiveren drøftet tiltakene med arbeidstakernes tillitsvalgte?

2

Har arbeidstakerne fått informasjon om tiltaket?

Er kontrolltiltaket innarbeidet i virksomhetens system for internkontroll?

Er tiltaket melde- eller konsesjonspliktig?

Er det laget planer for opplæring?

3

Har kontrolltiltaket den ønskede virkningen?

Bør det gjøres endringer?

Har virksomheten gode rutiner for revisjon av egen informasjonssikkerhet og internkontroll?

4

Fungerer systemer og rutiner som planlagt?

Gjøres nødvendige utbedringer underveis?

Blir informasjonsplikt og henvendelser om innsyn, retting og sletting ivaretatt?

Fase 1:

Vurder behov og kartlegg risiko

Denne fasen handler om tiden fra arbeidsgiveren ser et behov for å innføre et kontrolltiltak, frem til det tas en beslutning om en konkret løsning.

De sentrale oppgavene i denne fasen handler om å kartlegge behov og vurdere risiko ved ulike tiltak. Målet er å skaffe et godt beslutningsgrunnlag for hva bedriften skal velge, og å sikre at kontrolltiltaket vil være lovlig å gjennomføre.

Sentrale spørsmål:

1. Hva ønsker virksomheten å oppnå?

Alle kontrolltiltak må være godt begrunnet i praktiske forhold som angår driften av virksomheten. Virksomheten må ha klart for seg hva som skal oppnås med kontrolltiltaket, og sørge for at tiltaket er egnet til å oppnå formålet. Personopplysninger skal bare samles inn og brukes til det på forhånd angitte formålet. Opplysninger kan ikke senere brukes til andre formål eller til formål som er uforenlige med det opprinnelige formålet.

2. Hvilke løsninger dekker behovet?

Arbeidsgiverens behov for kontrolltiltak kan ofte dekkes på flere forskjellige måter. Arbeidsgiveren skal derfor vurdere fordeler og ulemper ved ulike løsninger. Vurder også tiltak som allerede finnes i virksomheten, og se om disse kan justeres for å dekke behovet.

Det er viktig at kontrolltiltak ikke blir en uforholdsmessig stor belastning for de ansatte. Derfor må arbeidsgiveren velge det tiltaket som er minst belastende med tanke på både personvern og arbeidsmiljø.

Enkle kontrolltiltak som adgangskontroll og produksjonskontroll blir vanligvis ikke regnet som spesielt belastende. Mer inngripende tiltak som kroppsvisitering vil ofte ikke være tillatt. Hvor grensen går, må imidlertid vurderes konkret i den enkelte saken.

Arbeidsgiveren må vurdere om kontrolltiltaket skal omfatte alle ansatte. Hvis noen grupper skal velges ut, må utvalget gjøres basert på en saklig begrunnelse.

Arbeidsgiveren må også vurdere den samlede belastningen av alle kontrolltiltakene i bedriften.

3. Er den arbeidsmiljømessige risikoen og personvernkonsekvensene kartlagt og vurdert?

Alle tiltak som kan påvirke arbeidstakernes fysiske eller psykiske helse og sikkerhet, samt arbeidstakernes personvern, skal kartlegges og vurderes. Risikovurderingen skal være skriftlig og inngå i det systematiske helse-, miljø- og sikkerhetsarbeidet i virksomheten.

Virksomheten må også kartlegge og vurdere hvilke konsekvenser tiltaket kan føre med seg for arbeidstakernes personvern.

4. Er det gjort en risikovurdering av informasjonssikkerheten?

Virksomheten må sørge for at personopplysningene er godt nok sikret. Ved innføring av nye tiltak som får følger for IKT-systemer og informasjonssikkerhet, må virksomheten foreta en risikovurdering. En risikovurdering skal identifisere uønskede hendelser og redusere risikoen for at de skjer. Virksomheten må ta stilling til om den er villig til å akseptere risikoen tiltaket fører med seg.*

Videre lesning

* Datatilsynets veileder forklarer hvordan virksomheten bør gjennomføre en risikovurdering

5. Har arbeidsgiver drøftet tiltakene med arbeidstakernes tillitsvalgte?

Arbeidsgiver skal så tidlig som mulig drøfte behov, utforming og gjennomføring av kontrolltiltak med arbeidstakerne og deres representanter, og verneombudet skal tas med på råd i planleggingen. Drøftingene skal foregå så tidlig som mulig, slik at arbeidstakerne har en reell mulighet til å komme med innvendinger og innspill. Målet er at partene kommer fram til løsninger som i størst mulig grad begrenser ulempene for arbeidstakerne.

Klare rammer ved bruk av personopplysninger

Etter personopplysningsloven kan innsamling og bruk av personopplysninger bare skje til uttrykkelig angitte formål. Det skal altså være klart på forhånd hvorfor personopplysningene skal samles inn, og hva de videre kan brukes til. Formålet bør formuleres slik at det er enkelt å forstå hva som faller innenfor dette formålet, og hva som faller utenfor. Opplysningene kan ikke senere brukes til formål som er uforenlige med det opprinnelige formålet. Det er imidlertid tillatt hvis den opplysningene gjelder, samtykker til dette.

Flere formål? Det er i prinsippet ikke noe i veien for at et tiltak kan ha mer enn ett formål. For eksempel kan et formål være å dokumentere leveranser til kunder, samtidig som formålet også er å kontrollere hvordan ansatte utfører arbeidet. I så fall er det ikke tillatt å kommunisere kun ett av formålene, for eksempel det formålet virksomheten mener er viktigst, mens andre formål ikke blir nevnt. Det må være full åpenhet og informasjon om alle eksisterende formål. Bruken til hvert enkelt formål må også la seg forsvare i regelverkskravene.

Endring av formål? Det er mulig for en virksomhet å endre formålet med et tiltak, for eksempel fordi en evaluering tilsier at det er tjenlig. Virksomheten må da være bevisst sine informasjonsplikter og at bruk av personopplysninger som tidligere er samlet inn, er begrenset av den opprinnelige formålsbeskrivelsen.

Sjekkliste for fase 1:

- [ ] Kartlegg behovet og hvilke konkrete utfordringer som skal løses.
- [ ] Vurder om behovet kan dekkes av de tiltakene bedriften har fra før.
- [ ] Lag en skriftlig beskrivelse av formålet med kontroll- og overvåkingstiltaket.
- [ ] Kartlegg fordeler og ulemper ved tiltakene:
    - [ ] Vurder om og hvordan tiltaket vil gripe inn i arbeidstakernes rett til personvern, for eksempel hvor følsomme opplysningene er, og hvor mye tiltaket vil påvirke arbeidstakernes hverdag.
    - [ ] Vurder om tiltaket kan få negative arbeidsmiljømessige konsekvenser, for eksempel i form av økt tidspress og stress, mindre selvbestemmelse og frihet i jobben eller andre arbeidsorganisatoriske utfordringer.
    - [ ] Gjennomfør en risikovurdering med tanke på informasjonssikkerhet. Vurder om risikoen er akseptabel.
- [ ] Drøft behov, utfordringer og mulige løsninger med de tillitsvalgte så tidlig som mulig.
- [ ] Involver vernetjenesten når kontrolltiltakene kan få betydning for arbeidsmiljøet.
- [ ] Ta stilling til om tiltaket står i forhold til problemene det skal løse.
- [ ] Velg det minst inngripende tiltaket.
- [ ] Vurder konkret hva slags informasjon om de ansatte som skal samles inn. Opplysningene skal være relevante, korrekte og ikke for inngripende.
- [ ] Vurder hvor lenge bedriften trenger informasjonen. Når opplysningene ikke lenger er nødvendige, skal de slettes.
- [ ] Sjekk om personvernulemper kan reduseres ved hjelp av gode tekniske og/eller organisatoriske løsninger, for eksempel innebygd personvern, personvernvennlig teknologi mv.
- [ ] Vurder om den totale mengden og belastningen ved alle kontrolltiltakene i virksomheten er forsvarlig.

Regelverkslenker

- Arbeidsmiljøloven § 3-1 (2) bokstav c og d
- Arbeidsmiljøloven § 4-1 Generelle krav til arbeidsmiljøet
- Arbeidsmiljøloven § 9-1 Vilkår for kontrolltiltak i virksomheten
- Arbeidsmiljøloven § 9-2 (1)
- Personopplysningsloven § 11 Grunnkrav til behandling av personopplysninger
- Personopplysningsloven § § 8 og 9, spesielt § 8 bokstav f Behandlingsgrunnlag for alminnelig og sensitive personopplysninger
- Personopplysningslovens § 28 Sletting
- Personopplysningsforskriften §2-4 Risikovurdering

Fase 2:

Ta en beslutning, planlegg og forbered

Denne fasen starter med at arbeidsgiveren tar beslutningen om hvilken løsning som skal innføres og eventuelt kjøpes inn hos eksterne ved behov.

Arbeidsgiveren skal drøfte dette med de ansattes tillitsvalgte og ta verneombudet med på råd. Dette skal være en del av beslutningsgrunnlaget. Når beslutningen er tatt, må det gjøres en rekke forberedelser før tiltaket kan settes i gang.

Sentrale spørsmål:

1. Har arbeidstakerne fått informasjon om tiltaket?

Før kontroll- og overvåkingstiltaket iverksettes, skal berørte arbeidstakere informeres om formålet med tiltaket, varigheten av det, praktiske konsekvenser og hvordan tiltaket vil bli gjennomført. Arbeidstakerne må blant annet informeres om hvor det eventuelle kontrollutstyret skal plasseres, hvordan utstyret virker, undersøkelsesmetoder og lignende.

Informasjonsplikten gjelder uansett om det er tillitsvalgte ved virksomheten eller ikke. Det er ikke nødvendig å informere hver gang kontrollen gjennomføres, så lenge det har vært informert om at kontroller kan forekomme.

Om informasjonsplikten:

Både arbeidsmiljøloven og personopplysningsloven krever at arbeidsgiveren

aktivt informerer de ansatte. Lovene stiller noe ulike krav til hvilken informasjon som må gis. En praktisk løsning for virksomheten kan derfor være å informere etter begge regelverkene samtidig. I så fall må det skje før tiltaket trer i kraft.

Arbeidsmiljølovens krav til informasjon

Arbeidsgiverens behov for kontrolltiltak kan ofte dekkes på flere forskjellige måter. Arbeidsgiveren skal derfor vurdere fordeler og ulemper ved ulike løsninger. Vurder også tiltak som allerede finnes i virksomheten, og se om disse kan justeres for å dekke behovet.

Før tiltaket iverksettes, skal arbeidsgiveren informere de berørte arbeidstakerne om

- formålet med kontrolltiltaket
- praktiske konsekvenser av kontrolltiltaket, blant annet hvordan kontrolltiltaket vil bli gjennomført
- hvor lenge kontrolltiltaket varer

Personopplysningslovens krav til informasjon

Før tiltaket iverksettes, skal virksomheten informere ansatte og eventuelle kunder eller andre berørte om

- navn og adresse på den virksomheten som er ansvarlig for å behandle opplysningene (behandlingsansvarlig)
- hva som er formålet med å samle inn opplysningene
- hvorvidt opplysningene vil bli utlevert til andre, og i så fall til hvem
- hvorvidt det er frivillig å gi fra seg opplysningene
- hvor lenge opplysningene blir lagret
- annet som gjør at de som blir registrert, kan ivareta rettighetene sine, for eksempel retten til innsyn, retting og sletting

Når opplysningene samles inn fra andre enn den ansatte selv, skal arbeidsgiveren i tillegg informere den ansatte om hvilke personopplysninger som samles inn.

2. Er kontrolltiltaket innarbeidet i virksomhetens system for internkontroll?

Internkontroll innebærer at virksomheten skal ha oversikt over hvilke personopplysninger som blir samlet inn, og hvordan de blir behandlet. Eventuelle nye tiltak må derfor føres inn i virksomhetens internkontrollsystem. Sammen med kravet til internkontroll følger også krav til nødvendig opplæring og rutiner for å sikre at personopplysningene blir brukt i tråd med regelverket.*

3. Er tiltaket melde- eller konsesjonspliktig?

Hovedregelen er at behandling av personopplysninger er meldepliktig, og at behandling av sensitive personopplysninger er konsesjonspliktig. Det finnes imidlertid flere unntak fra hovedreglene, og mange vanlige tiltak krever verken melding eller konsesjon.

Hvis tiltaket er meldepliktig, må det sendes meldingsskjema til Datatilsynet senest 30 dager før oppstart. Konsesjonsplikt innebærer at du må søke Datatilsynet om tillatelse. Personopplysningene kan ikke brukes før det er gitt tillatelse.**

4. Er det laget planer for opplæring?

Dersom kontroll- og overvåkingstiltaket fører til endrede rutiner og bruk av nytt utstyr, må arbeidsgiveren sørge for at arbeidstakerne får nødvendig opplæring. Dette gjelder for eksempel bruk av utstyr, arbeidsteknikk og organisering av arbeidet.

Videre lesning

* Les mer om internkontrollsystem hos Datatilsynet.

** Les mer om melding og konsesjon hos Datatilsynet.

Sjekkliste for fase 2:

- [ ] Beslutt hvilke tiltak som skal gjennomføres.
- [ ] Vurder om tiltaket er melde- eller konsesjonspliktig til Datatilsynet, eventuelt om det er unntatt fra både melde- og konsesjonsplikt. Lag en skriftlig beskrivelse av formålet med kontroll- og overvåkingstiltaket.
- [ ] Sørg for at eventuelle innkjøp og kravspesifikasjoner sikrer at det som etableres, er i tråd med hva som var tenkt.
- [ ] Før inn tiltaket i virksomhetens internkontroll (se veileder: Internkontroll og informasjonssikkerhet). Etabler et tilstrekkelig sett av rutiner for å sikre at personopplysningene blir brukt på den måten virksomheten har bestemt, og i tråd med regelverket.
    - [ ] Utarbeid rutiner for hvordan virksomheten skal håndtere forespørsler om innsyn og eventuelle andre rettigheter for dem opplysningene handler om.
    - [ ] Avklar hvem som har det daglige ansvaret for at plikter blir fulgt.
    - [ ] Sørg for nødvendige informasjonssikkerhetstiltak, for eksempel hvem som skal ha tilgang til opplysninger.
    - [ ] Sørg for at ansatte som behandler personopplysninger, får nødvendig opplæring.
    - [ ] Sørg for at arbeidstakerne får nødvendig opplæring og øvelse i bruk av utstyr og arbeidsteknikk.
    - [ ] Sørg for rutiner for sletting av opplysninger.
- [ ] Inngå en databehandleravtale med eventuelle leverandører dersom de håndterer personopplysninger på vegne av virksomheten.
- [ ] Sørg for at virksomheten har et avvikssystem, slik at eventuelle avvik i forbindelse med kontrolltiltaket kan bli registrert og behandlet.
- [ ] Lag en plan for hvordan arbeidstakerne og eventuelle andre skal informeres.
    - [ ] Vurder om tiltaket bør testes ut i mindre skala. Merk at regelverket også gjelder prøvedrift.
    - [ ] Utarbeid en plan for evaluering av tiltaket.

Regelverkslenker

- Arbeidsmiljøloven § 9-2 (1)
- Arbeidsmiljøloven § 4-2 (2) bokstav e
- Internkontrollforskriften § 5
- Personopplysningsloven § 14 og forskriften kapittel 3 om internkontroll
- Personopplysningsloven § 13 og forskriften kapittel 2 om informasjonssikkerhet
- Personopplysningsloven § 15 om databehandleravtale
- Personopplysningsloven § 19 Informasjonsplikt når det samles inn opplysninger fra den registrerte
- Personopplysningsloven § 20 Informasjonsplikt når det samles inn opplysninger fra andre enn den registrerte
- Personopplysningsloven §§ 31–33 og forskriften kapittel 7 om melde- og konsesjonsplikt og unntak

Fase 3:

Gjennomfør

Nå kan kontrolltiltaket igangsettes og eventuelle IKT-systemer tilknyttet tiltaket settes i drift.

I tillegg må en del andre oppgaver gjøres underveis, for eksempel håndtere avvik, gi informasjon til nyansatte og innsyn i egne opplysninger til dem som ber om det. Nye systemer og tiltak må følges nøye opp i tiden rett etter at kontrolltiltaket er igangsatt, for å sikre at kontrolltiltaket fungerer slik det er ment.

Sentrale spørsmål:

1. Fungerer systemer og rutiner som planlagt?

Virksomheten bør så tidlig som mulig sjekke om IKT-systemer og rutiner fungerer slik det var tenkt. Eksempelvis bør frister for sletting sjekkes for å påse at det ikke lagres unødvendig informasjon. Sjekk at rutinene for å håndtere personopplysninger fungerer, og at de ansatte har fått nødvendig opplæring.

2. Gjøres nødvendige utbedringer underveis?

Dersom det kommer avviksmeldinger eller henvendelser fra ansatte, må virksomheten vurdere om det bør gjøres endringer med det samme. Det kan bli nødvendig med tekniske endringer og endringer i rutiner som ikke kan vente til etter evalueringen (se fase 4).

3. Blir informasjonsplikt og henvendelser om innsyn, retting og sletting ivaretatt?

Virksomheten må løpende sørge for at rettigheter blir ivaretatt. Dette dreier seg særlig om å informere nyansatte og håndtere henvendelser om innsyn. Henvendelser om innsyn, retting eller sletting skal besvares så raskt som mulig og senest innen 30 dager.

Sjekkliste for fase 3:

- [ ] Gjør en tidlig gjennomgang av systemet. Sjekk at alt fungerer som det skal, og at rutinene er kjent, fungerer og blir fulgt i praksis.
- [ ] Kontroller spesielt at virksomhetens rutiner for sletting blir fulgt.
- [ ] Sørg for å dokumentere erfaringer underveis, slik at de er tilgjengelige ved en senere evaluering.
- [ ] Ta vare på henvendelser om innsyn, retting og sletting.
- [ ] Husk å informere nyansatte.
- [ ] Gjør nødvendige utbedringer underveis. Det kan oppstå behov for rutiner man i første omgang ikke hadde tenkt på.
- [ ] Sørg for å sende avviksmeldinger når feil skjer. Eventuelle svakheter må utbedres underveis.

Regelverkslenker

- Personopplysningsloven § 2 (7)
- Personopplysningsloven § 8 Vilkår for å behandle personopplysninger
- Personopplysningsloven § 14 og forskriften kapittel 3 om internkontroll
- Personopplysningsloven § 13 og forskriften kapittel 2 om informasjonssikkerhet, spesielt forskrift § 2-6 om avvik
- Personopplysningsloven §§ 19 og 20 om informasjonsplikter
- Personopplysningsloven § 18 om innsyn
- Personopplysningsloven §§ 27 og 28 om retting og sletting

Fase 4:

Evaluer og følg opp

Med jevne mellomrom må arbeidsgiveren, sammen med arbeidstakernes tillitsvalgte, vurdere og drøfte behovet for tiltaket. Dere bør fastsette hvor ofte tiltaket skal evalueres, allerede under planleggingen.

Behovet for et kontrolltiltak i en virksomhet vil oftest endres over tid. Målet med evaluerings- og oppfølgingsfasen er å sørge for at tiltaket er forsvarlig og tilpasset dagens situasjon. Én gang i året vil det vanligvis være behov for en mer helhetlig gjennomgang av virksomhetens systemer. Det skal sikre at praksis er i tråd med regelverkskrav, i særlig grad det som gjelder informasjonssikkerhet og internkontroll.

Sentrale spørsmål:

1. Har kontrolltiltaket den ønskede virkningen

Virksomheten bør vurdere om tiltaket bidrar til å nå det opprinnelig fastsatte målet, eller om det ikke har effekt. Viser erfaringene at riktig virkemiddel er valgt?

- om tiltaket har mangler
- om tiltaket av ulike grunner ikke lenger er aktuelt
- om det er behov for å gjøre vesentlige endringer
- om tiltaket har negative konsekvenser for arbeidsmiljøet eller personvernet

I evalueringen må man også ta stilling til om formålsbeskrivelsen virksomheten laget i fase 1, bør justeres (se faktaboks). Vær oppmerksom på at denne formålsbeskrivelsen binder videre bruk av opplysningene. Et mer snevert formål kan

begrense bruken av personopplysningene og gjøre den mer forutsigbar. Dermed reduseres også personvernulempene.

2. Bør det gjøres endringer?

Evalueringen kan føre til at tiltaket bør endres, i noen tilfeller nedskaleres eller avsluttes. Evalueringen kan også føre til det motsatte, nemlig at tiltaket utvides. I noen tilfeller kan det tenkes at man har valgt et uhensiktsmessig tiltak, og at det heller bør etableres andre tiltak.

Virksomheten skal vurdere om tiltaket kan gjøres mindre inngripende. Det kan for eksempel handle om at færre skal ha tilgang til personopplysningene, at lagringstiden bør endres, eller at informasjonen kan gjøres mindre identifiserbar eller behandles på gruppenivå.

En viktig del av vurderingen er om noen av personopplysningene som samles inn i dag, egentlig er nødvendige. Hvis opplysningene er unødvendige, skal de slettes.

3. Har virksomheten gode rutiner for revisjon av egen informasjonssikkerhet og internkontroll?

Hvis det nye kontrolltiltaket er en del av virksomhetens eksisterende internkontroll, vil de generelle rutinene for internkontroll og informasjonssikkerhet også gjelde dette tiltaket.

Virksomheten må ha en planlagt og systematisk tilnærming til hvordan internkontroll og informasjonssikkerhet skal revideres og vedlikeholdes. Noen deler av internkontrollen eller informasjonssikkerheten må gjennomgås med korte intervaller. For andre deler kan det gå noen år mellom hver gang. Lag en plan for året, og bestem hva som skal gjennomgås i år.

Egenkontroll av rutiner og tekniske tiltak bør skje jevnlig. Virksomheten skal ha rutiner for å rapportere til ledelsen og ansvarlige om sikkerhetshendelser, avvikshåndtering og egenkontroll.

Videre lesning

* Les mer i Datatilsynets veileder om internkontroll og informasjonssikkerhet.

Virksomheten bør årlig gjennomgå sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssystemene. Arbeidsgiveren skal kontrollere at disse er i samsvar med virksomhetens behov, og eventuelt oppdatere mål, strategi og organisering. Ved gjennomgangen deltar representanter fra virksomhetens øverste ledelse sammen med den sikkerhetsansvarlige og IT-driftslederen.

Sjekkliste for fase 4:

- [ ] Ta stilling til om kontrolltiltaket har den ønskede virkningen.
- [ ] Vurder om det fremdeles er bruk for kontrolltiltaket, og om det er innført nye og andre tiltak som gjør dette tiltaket overflødig.
- [ ] Vurder om virksomheten samler inn flere opplysninger enn nødvendig.
- [ ] Utfør jevnlig en sikkerhetsrevisjon med vurderinger av hvem som skal ha tilgang til systemet.
- [ ] Gjør jevnlig en systematisk gjennomgang av internkontrollen med rutinene.

Regelverkslenke

- Arbeidsmiljøloven § 9-2 (3)
- Personopplysningsloven § 14 og forskriften kapittel 3 om internkontroll
- Personopplysningsloven § 13 og forskriften kapittel 2 om informasjonssikkerhet, spesielt forskriften § 2-3 om sikkerhetsledelse og § 2-5 om sikkerhetsrevisjon

Vanlige kontrolltiltak

Kapittel 4

Lær mer om:

- Kameraovervåking
- Innsyn i e-post
- Adgangskontroll
- Tidsregistrering
- Veskekontroll
- «Hemmelig kunde/gjest»
- Bruk av styringsverktøy utenfor fast arbeidssted
- Opptak av telefonsamtaler
- Tilgang til ansattes mobiltelefon – Mobile Device management
- GPS-sporing og annen lokalisering i yrkesbiler
- Innhenting av helseopplysninger ved ansettelse
- Medisinske undersøkelser og rus-testing av arbeidssøkere og arbeidstakere

Vanlige kontrolltiltak

I dette kapittelet finner du informasjon om ulike former for kontrolltiltak og hvordan du kan sikre at tiltakene ikke går ut over personvernet og arbeidsmiljøet.

Oversikten er ikke uttømmende, men viser eksempler på tiltak som er vanlige på mange arbeidsplasser.

Kameraovervåking

Kameraovervåking er et relativt vanlig kontrolltiltak. Kameraovervåking er definert i personopplysningsloven som

> «vedvarende eller regelmessig gjentatt personovervåking ved hjelp av fjernbetjent eller automatisk virkende overvåkningskamera eller annet lignende utstyr som er fastmontert. Som kameraovervåking anses både overvåking med og uten mulighet for opptak av lyd- og bildemateriale. Det samme gjelder utstyr som lett kan forveksles med en ekte kameraløsning.»

Definisjonen favner altså noe videre enn alminnelige kameraovervåkingsanlegg lik dem vi ofte ser i butikker. En kameraløsning som automatisk tar et bilde av samme område med jevne intervaller, vil være kameraovervåking. Også utstyr som ligner på opptaksutstyr, såkalte dummy-kameraer, faller inn under definisjonen. Bruk av håndholdte kameraer regnes ikke som kameraovervåking.

Personopplysningslovens vanlige bestemmelser gjelder for kameraovervåking. I tillegg har både loven og tilhørende forskrift egne bestemmelser som bare gjelder for kameraovervåking. For at en arbeidsgiver skal kunne kameraovervåke en arbeidsplass, må de generelle vilkårene for kameraovervåking være oppfylt. I tillegg må det foreligge et særskilt behov dersom man skal overvåke områder der bare de ansatte ferdes.

Kameraovervåking er et forholdvis inngripende middel. For de fleste arbeidstakere vil det oppleves som belastende å få innsatsen sin kontrollert eller overvåket kontinuerlig. Det finnes en grense for hvor intensiv overvåking som kan tillates på en arbeidsplass.

Før kameraovervåking tas i bruk, er det derfor viktig å vurdere om andre midler kan ivareta virksomhetens behov på en tilstrekkelig måte.

I vurderingen av om, og i så fall hvor, det skal overvåkes på arbeidsplassen, må virksomheten særlig merke seg følgende:

- Overvåkingen må være forholdsmessig, det vil si at den må la seg forsvare i en interesseavveining mellom behovet for overvåkingen på den ene siden og personvernulemper på den andre siden.
- Overvåking av pauserom, toalettrom eller garderober er i utgangspunktet ikke tillatt uansett hvor god grunn man måtte mene å ha.
- Kameraovervåking skal ha et klart formulert formål, og hva som vises fra hvert kamera, må være relevant for dette formålet.
- Arbeidsgiveren kan overvåke områder der bare de ansatte ferdes, bare hvis det foreligger et særskilt behov, for eksempel behov for å ivareta ansattes eller andres sikkerhet. Det vil si at det skal mer til for å overvåke disse områdene enn steder som er tilgjengelige for alle, som for eksempel et butikklokale.

Hvis formålet er å ivareta de ansattes helse og sikkerhet, vil overvåkingen normalt være tillatt. Det vil da være et krav at arbeidsplassen er vurdert til å ha en spesielt høy sikkerhetsrisiko. Steder der det drives risikofylt produksjon, eller der det er store sjanser for ran, som banker og postkontor, er typiske eksempler. Dette vil likevel bare gjelde på de konkrete områdene hvor det er en betydelig risiko, som steder der det håndteres kontanter, eller der det er plassert pengeskap.

Kameraovervåking for å forhindre svinn og underslag fra ansatte kan være tillatt dersom det foreligger et dokumentert problem eller en konkret fare for svinn eller underslag. Ettersom man alltid skal ta i bruk det minst inngripende tiltaket og kameraovervåking på arbeidsplassen ofte vil oppleves som svært belastende, må arbeidsgiveren forsøke å komme problemet til livs på andre måter før kameraovervåkingen innføres.

Vinklingen av kameraene kan ha betydning for om tiltaket er lovlig. For eksempel kan kravene være oppfylt med hensyn til å overvåke en kasse der det oppbevares penger, men ikke resten av området bak butikkdisken. I vurderingen vil det også ha betydning om overvåking skal skje i sanntid eller i videoopptak som blir lagret for senere bruk.

I tillegg til å vurdere hva hvert kamera fanger opp, må virksomheten sørge for at kameraovervåkingen totalt sett ikke blir for omfattende i de ansattes arbeidshverdag.

Både tilgang til opptak og overvåking i sanntid (monitorering) skal avgrenses etter hvem som trenger det i arbeidet sitt. Som oftest vil det være nok at noen svært få har tilgang.
Hovedregelen er at opptak skal slettes senest etter sju dager.

Dersom det er sannsynlig at et opptak vil bli utlevert til politiet, kan det oppbevares i inntil 30 dager. Opptak fra bank eller postlokaler, inkludert opptak fra kasse i Bank i Butikk og Post i Butikk, kan oppbevares i inntil tre måneder.
Overvåkingen må varsles gjennom skilting.

Saksbehandlingsreglene om informasjon og drøfting i arbeidsmiljøloven gjelder også kameraovervåking. Det betyr at arbeidsgiveren ikke bare må drøfte om det skal være kameraovervåking og hva som skal være formålet, men også hvordan overvåkingen i praksis skal gjennomføres. Alle ansatte skal gjøres kjent med hva slags rutiner man har i virksomheten på dette området (se fase 1).

Fra januar 2017 er kameraovervåking unntatt fra meldeplikten.*

Du kan lese mer om kameraovervåking, hvilke vurderinger som må gjøres, krav til sletting, varslingsskilter, regler for når opptak kan utleveres, krav til informasjonssikkerhet mv. i Datatilsynets kameraovervåkingsveileder.

Innsyn i e-post

Arbeidsgiveren kan som hovedregel ikke kreve innsyn i de ansattes e-post eller private filer. Det er imidlertid noen unntak. Reglene er gitt i personopplysningsforskriften kapittel 9. Reglene gir adgang til innsyn i enkeltstående tilfeller for konkrete formål og ikke kontinuerlig innsyn – som har karakter av overvåking.

Reglene åpner for innsyn i følgende situasjoner:

- når det er nødvendig for å ivareta den daglige driften
- når det er nødvendig for å ivareta andre berettigede interesser ved virksomheten
- ved begrunnet mistanke om at bruk av e-postkassen medfører grove brudd på de pliktene som følger av arbeidsforholdet
- ved begrunnet mistanke om at arbeidstakerens bruk av e-postkassen kan gi grunnlag for oppsigelse eller avskjed

Hva som er nødvendig, må vurderes konkret i hvert enkelt tilfelle. Dersom det samme formålet kan oppnås på andre og mindre belastende måter, vil innsyn i e-postkassen ikke være nødvendig, og dermed heller ikke tillatt.

Reglene gjelder for den ansattes e-postkasse, men også for arbeidstakers personlige område i virksomhetens datanettverk og i andre elektroniske kommunikasjonsmedier eller elektronisk utstyr som

Regelverkslenker

- Arbeidsmiljøloven § 9-1
- Arbeidsmiljøloven § 9-2
- Personopplysningsloven kap. VII Kameraovervåkning
- Personopplysningsforskriften kap. 8 Kameraovervåkning
- Personopplysningsforskriften § 7-11b

arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet. Typiske eksempler er arbeidstakerens hjemmeområde på serveren, PC-en som arbeidstakeren bruker på jobb, mobiltelefonen som arbeidsgiveren har utstyrt arbeidstakeren med, nettbrett osv.

Arbeidsgiverens innsynsrett omfatter ikke privat utstyr – mobiltelefon, nettbrett, PC mv. – private e-postkontoer eller lignende.

Det er ikke anledning til å avtale innsyn i andre situasjoner enn de som er nevnt over, men arbeidstakeren kan selv uoppfordret gi arbeidsgiveren rett til innsyn, for eksempel ved uventet sykdom.

Arbeidstakeren skal så langt det er mulig, få et begrunnet varsel og anledning til å uttale seg før innsynet blir foretatt. Likevel kan arbeidsgiveren ta en sikkerhetskopi, ofte kalt speilkopi, før det varsles eller foretas innsyn, dersom det er fare for at informasjon kan gå tapt.

I tillegg skal arbeidstakerne så langt det er mulig, få anledning til å være til stede under innsynet, om ønskelig sammen med en tillitsvalgt eller annen representant.

Saksbehandlingsreglene om informasjon og drøfting i arbeidsmiljøloven kommer også til anvendelse for dette kontrolltiltaket. Det innebærer at arbeidsgiveren må drøfte med de ansatte på systemnivå i hvilke tilfeller det kan antas å være behov for innsyn, og hvordan et slikt innsyn kan gjennomføres. Alle ansatte skal gjøres kjent med hva slags rutiner man har i virksomheten på dette området (se fase 1).

Råd til arbeidsgivere

- Lag rutiner for gjennomføring av innsyn som sørger for at
  - innsyn blir forsvarlig vurdert og begrunnet
  - arbeidstakeren blir forhåndsvarslet og gitt anledning til å være til stede så langt det er mulig
  - gjennomføringen av innsynet blir så skånsom og begrenset som mulig
  - innsynet blir skriftlig begrunnet og dokumentert, og at det føres protokoll fra gjennomføringen
- Lag rutiner og systemer for arbeidstakernes bruk av IKT-utstyr og e-post. Virksomhetsrelaterte e-poster, dokumenter mv. som andre kan trenge tilgang til, bør ikke ligge i arbeidstakerens e-postkasse eller på vedkommendes PC, men fortløpende overføres til områder der andre har tilgang.
- Lag rutiner for ansattes egen opprydding i e-postkasse mv. når de skal slutte. Virksomhetsrelatert materiale skal om nødvendig flyttes over til områder andre har tilgang til, og alt privat skal slettes.

Adgangskontroll

Elektronisk adgangskontroll er tekniske løsninger som sørger for at bare de som rettmessig har adgang til et bestemt område, kan passere. Et vanlig tiltak er bruk av elektroniske nøkkelkort, der det er mulig å logge hvilke kort som er brukt på forskjellige dører (kortlesere), og når det skjedde. Passeringsdata av denne typen er opplysninger om den enkelte ansatte som kortet er utstedt til. Systemene kan normalt også stilles inn slik at det er mulig å åpne døren uten at kortbruken logges.

Slike ordinære former for adgangskontroll vil vanligvis være et saklig og lite inngripende kontrolltiltak. Virksomheten må imidlertid ha gjennomtenkte valg for om passeringsdata skal loggføres, og i så fall for hvilke soner eller rom (kortlesere), og på hvilken tid av døgnet. For mange virksomheter er det hensiktsmessig å operere med et skille mellom tiden innenfor og tiden utenfor normal arbeids- eller åpningstid.

Selv om hensikten med elektronisk adgangskontroll kan virke selvinnlysende, skal det være et skriftlig nedfelt formål med tiltaket. Formålet gir føringer for hvilke passeringsdata det kan være relevant å samle inn, hvem som skal ha tilgang til opplysningene, og hva lagrede data kan brukes til.

Tidsregistrering og adgangskontroll skal ikke blandes. For bruk av adgangskontroll vil formålet normalt være å sikre verdier, bygg og lignende. Å kontrollere om den ansatte gjør jobben sin eller fører riktige timelister, vil ikke være i samsvar med dette formålet.

I utgangspunktet kan ikke opplysningene i adgangskontrollsystemet brukes til andre formål, som for eksempel registrering av arbeidstid. Hvis registrering av arbeidstid krever at arbeidstakeren utfører en aktiv handling, for eksempel ved bruk av «stemplingsur», kan systemet likevel brukes til begge formål. Arbeidstidsinformasjonen må lagres adskilt fra passeringsloggen. Passeringsdata og arbeidstidsinformasjon må behandles videre som data med ulike formål, og som informasjon som i utgangspunktet ikke skal kobles sammen.

Ved lagring av passeringsopplysninger må opplysningene ha god nok kvalitet. Dersom dataene skal kunne brukes til å følge opp hendelser, må det være tilstrekkelig sikkerhet for at det er korteieren selv som har brukt kortet. Derfor kan passeringer bare lagres når det skjer en sterk autentisering, for eksempel ved at den ansatte bruker PIN-kode sammen med adgangskortet.

Regelverkslenker

- Arbeidsmiljøloven § 9-2
- Arbeidsmiljøloven § 9-5 Innsyn i arbeidstakers e-post
- Personopplysningsforskriften kapittel 9 Innsyn i e-postkasse mv.

Under normale omstendigheter vil 90 dager, i henhold til Datatilsynets praksis, være maksimal lagringstid for passeringsopplysninger.

Fra januar 2017 er behandling av personopplysninger i aktivitetslogg i adgangskontrollanlegg unntatt fra meldeplikten.*

Tidsregistrering

Arbeidsgiveren kan kreve at arbeidstakerne selv registrerer seg automatisk når de kommer på arbeid, og når de forlater arbeidsplassen. Det kan også kreves at de registrerer seg ut på forskjellige koder dersom de forlater arbeidsplassen i avtalt arbeidstid, for eksempel for å gå til eksterne møter, til tannlegen eller lignende. Dette følger av arbeidsgiverens styringsrett og arbeidsavtalen, der de ansatte stiller sin tid til arbeidsgiverens disposisjon mot betaling.

Tidsregistrering vil derfor vanligvis være uproblematisk som kontrolltiltak.

I enkelte bransjer har ikke arbeidstakerne et fast arbeidssted. Dette gjelder ofte for sjåfører, håndverkere og arbeidstakere i servicevirksomheter. Her kan arbeidsgiveren ha et ønske om eller behov for å vite hvor den enkelte ansatte befinner seg til enhver tid.

For slike grupper med ansatte vil det på samme måte kunne kreves en rapportering om arbeidsoppstart og -slutt, for eksempel via tekstmelding.

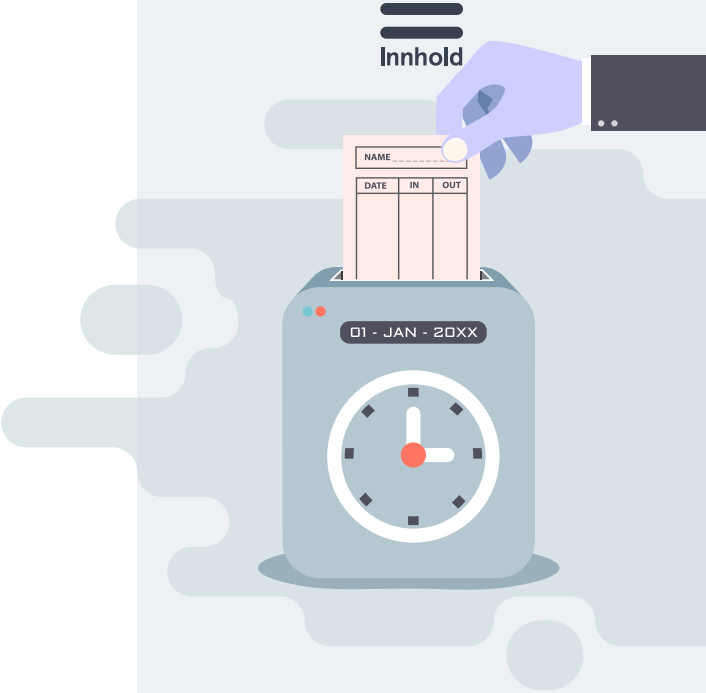
Dersom arbeidsgiveren vil bruke lokaliseringsdata til å registrere arbeidstid, skal ikke kontrollen generere mer informasjon enn det som er nødvendig. Registreringen skal gjennomføres på den måten som er minst inngripende overfor den ansatte, og reglene for saksbehandling skal følges.

Dette må arbeidsgiveren vurdere før det innhentes opplysninger. Det er vanligvis ikke tillatt å bruke allerede innhentede personopplysninger til noe annet enn det som var det opprinnelige formålet (*se faktaboks*).

Tidsregistrering og adgangskontroll skal normalt ikke blandes. Se avsnittet om adgangskontroll.

Eksempel:
En bedrift som samler inn GPS-data for å effektivisere leveransene til kundene, kan ikke senere bruke de samme dataene til å kontrollere arbeidstiden til de ansatte.

Innhold



Regelverkslenke

Personopplysningsforskriften § 7-11a

Videre lesning

* Les mer i Datatilsynets veiledning om adgangskontroll på arbeidsplassen.

Veskekontroll

Veskekontroll innebærer undersøkelser av personlige eiendeler, som vesker eller bagasje. Denne typen kontroll er særlig aktuell i virksomheter der de ansatte har tilgang til verdifulle eller farlige produkter, eller der det er risiko for svinn.

Arbeidsgiverens styringsrett gir en forholdsvis vid adgang til rutinemessige kontrolltiltak, for eksempel kontrollere garderobeskap eller de ansattes vesker når de forlater bedriftslokalene.

Slike rutinemessige kontrolltiltak må likevel være saklig begrunnet og ikke medføre en uforholdsmessig belastning for de ansatte (les mer om denne vurderingen her).

Eksempel:

Kontroll av vesker i en bryggeribedrift

Arbeidsgiveren innførte et kontrolltiltak der alle som forlot bryggeriet, måtte trykke på en knapp. Lyste knappen rødt, måtte de gjennom en veskekontroll. Personene ble altså plukket tilfeldig ut. En gruppe elektroinstallatører som ikke var ansatt ved bryggeriet, nektet å la seg kontrollere.

Saken endte i Arbeidsretten. Retten gjorde en avveining mellom arbeidsgiverens behov for kontrolltiltaket og behovet for å beskytte arbeidstakernes personlige integritet. Resultatet ble at installatørene måtte underkaste seg kontrollen. Retten mente det var tungtveiende grunner til kontrolltiltakene, og at installatørene ikke hadde grunn til å føle seg krenket ved kontrollen.

Ved veskekontroll gjelder de ordinære kravene om saklighet, drøfting og informasjon, se fremgangsmåte og sjekklister for innføring av kontrolltiltak i fase 1 og 2.

«Hemmelig kunde/gjest»

Bruk av «hemmelige kunder» er et kontrolltiltak der virksomheten får besøk av anonyme observatører. Observatøren kommer uanmeldt for å registrere blant annet kundeservice, omgivelser og produkter. Dette kan gjøres på en slik måte at virksomheten ikke vet hvem som utfører undersøkelsen, eller når det blir gjort. Rapporter fra observatørene kan gi arbeidsgiveren innsikt i hvordan kundene opplever virksomheten, og danne grunnlag for forbedringer.

Arbeidsgiveren må sørge for at kontrolltiltaket er saklig begrunnet og ikke uforholdsmessig inngripende overfor de ansatte, les mer om denne vurderingen her.

«Hemmelig kunde» brukes også der man har konkret mistanke om svinn fra ansatte.

Eksempel:
«Hemmelig kunde»

Kontrolltiltaket besto i at en anonym vekter besøkte butikken. Under påskudd av å ha det travelt tok vekteren en bukett blomster og la igjen nøyaktig beløp for buketten på disken. Målet med kontrollkjøpet var å sjekke om den ansatte registrerte kjøpene korrekt.

Gulating lagmannsrett kom i kontrollkjøpdommen LG-2006-128425 til at arbeidsgiverens kontrolltiltak var akseptable.

Bruk av styringsverktøy utenfor fast arbeidssted

Styringsverktøy kan ha flere formål, som å dokumentere for kunder at tjenesten er utført, sørge for effektiv oppdragsfordeling eller fungere som et sikkerhetstiltak for arbeidstakerne.

Etter hvert er det blitt mer vanlig å benytte ulike former for styringsverktøy på arbeidsplasser der arbeidet foregår andre steder enn i arbeidsgiverens egne lokaler. Eksempler er transportoppdrag og arbeid som utføres i kundens lokaler eller i kundens eller brukerens hjem.

En *personlig digital assistent (PDA)* er en liten håndholdt datamaskin som kan brukes til fortløpende å føre elektroniske timelister. Slike verktøy kan ha stor betydning for virksomhetens rapporterings- og faktureringsmuligheter. Virksomheten kan også benytte programvare som sikrer en best mulig arbeidsflyt ved at arbeidsoppgaver logges og fordeles elektronisk. Slik programvare kan også kobles mot sporingsutstyr som *GSM* og *GPS*.

Innenfor hjemmehjelptjenesten kan de ansatte registrere når de møter opp hos en bruker, hvilke tjenester de har utført, når de drar, og hvor lang tid de bruker på transport mellom hver bruker.

Vekterbransjen har systemer der ulike kontrollpunkter på ruten skal skannes. Også renholdsvirksomheter bruker lignende systemer.

Ofte blir styringsverktøyene innført uten tanke på å kontrollere eller overvåke de ansatte. Likevel gjør teknologien det mulig å følge arbeidstakernes bevegelser, tidsbruk og utføring av arbeidsoppgaver svært nøyaktig. Det kan gi økt trygghet og effektivitet, men også føre til stress og mistrivsel. En detaljert logging av bevegelser og handlinger vil kunne være en inngripen i personvernet.

Det er viktig for ansatte å kunne forutsi hvordan data fra tiltaket vil bli brukt. Arbeidsgiveren må derfor sørge for at plikten til å drøfte er fulgt, og at de ansatte har fått tilstrekkelig informasjon om hva som registreres, og hva opplysningene skal brukes til (se fase 1 og 2).

Det hender at informasjon fra tiltak som i utgangspunktet ikke ble innført for å kontrollere, likevel brukes til kontroll av arbeidstakere i ettertid. Merk derfor at arbeidsgiveren ikke kan bruke innsamlede personopplysninger til nye formål (for eksempel kontroll), dersom dette er uforenlig med det opprinnelige formålet (se faktaboks).

Det er viktig at alle formålene nedtegnes skriftlig, slik at det er enkelt å forstå hva opplysningene kan og ikke kan brukes til. Klare rutiner for bruken av systemene, god tilgangsstyring og klar informasjon til de ansatte vil være gode virkemidler for å sikre at opplysningene blir brukt på en forutsigbar måte.

Eksempel:
Bruk av PDA i hjemmebaserte tjenester

I kommunale hjemmebaserte tjenester blir PDA ofte brukt for å skape en lettere arbeidshverdag for ansatte, samtidig som brukernes interesser skal bli ivaretatt på en sikker måte. De ansatte kan oppleve at de mister mye av fleksibiliteten når det gjelder utføringen av arbeidet – både hos den enkelte bruker og i løpet av arbeidsdagen totalt sett. Både arbeidsoppgavene og rekkefølgen på disse kan være lagt inn på en PDA, og det kan være få muligheter for å endre på dette. Det er derfor viktig å utarbeide gode avtaler for bruk av styringsverktøy og ha en god dialog mellom arbeidsgiver og tillitsvalgte omkring avtaleutformingen.

Opptak av telefonsamtaler

Opptak av telefonsamtaler brukes i dag til en rekke formål, for eksempel kvalitetssikring, oppfølging og opplæring eller dokumentasjon ved avtaleinngåelser.

Hvis virksomheten ønsker å bruke lydopptak, må visse vilkår være oppfylt. Virksomheten må blant annet sørge for at behandlingen oppfyller et av behandlingsgrunnlagene i personopplysningsloven. Det gjelder både med hensyn til den ansatte og den andre parten i samtalen, for eksempel kunder.

Opptak av ansattes samtaler

På visse vilkår kan arbeidsgiveren beslutte at det skal gjennomføres lydopptak av ansattes telefonsamtaler. Opptak av ansattes samtaler kan ikke baseres på samtykke fra den enkelte, da arbeidstakere sjelden vil oppleve en reell frivillighet i slike sammenhenger.

Arbeidsgiveren skal i alle tilfeller benytte det minst inngripende tiltaket overfor den ansatte. Når formålet for lydopptaket er opplæring eller oppfølging av ansatte, vil man som regel kunne benytte andre metoder, som for eksempel medlytt. Det vil si at den som står for opplæringen, lytter til samtalen mens den pågår, uten at det blir gjort lydopptak. Hvis formålet kan oppnås ved hjelp av medlytt, skal denne metoden alltid benyttes fremfor avlytting eller opptak. I de fleste tilfeller vil medlytt ikke omfattes av personopplysningsloven, ettersom personopplysninger ikke behandles i lovens forstand.

Merk at verdipapirforetak omfattes av egne regler. Verdipapirforetak har plikt til å gjøre opptak i forbindelse med kunderådgivning og kjøp og salg av verdipapirer.

Les mer om lydopptak av samtaler hos Datatilsynet. Her beskrives også hva som må ligge til grunn for at et opptak skal være lovlig med hensyn til personvernet til den andre parten i samtalen, for eksempel en kunde.

Tilgang til ansattes mobiltelefon – Mobile Device management

Mobile Device Management (MDM) er en programvare som kan installeres på mobiltelefonen (en app), og som gir arbeidsgiveren tilgang til og kontroll over den ansattes jobbtelefon. Mange arbeidstakere har en mobiltelefon gjennom jobben som brukes både til jobb og privat. I noen tilfeller har arbeidsgiveren et nødvendig og saklig grunnlag for å be om tilgang til innholdet på mobiltelefonen.

Sikring av mobiltelefonen i jobbsammenheng er viktig fordi mobiltelefoner ofte inneholder konfidensielle personopplysninger. Virksomheten har da et behov for og en plikt til å sørge for tilfredsstillende informasjonssikkerhet på mobiltelefonene.

Se bestemmelsene om informasjonssikkerhet i personopplysningsloven med forskrift.

Bruk av *MDM* er normalt tillatt for sikkerhetsformål, men virksomheten må vurdere om andre, mindre inngripende, tiltak kan oppfylle sikkerhetsformålet. Dersom mindre inngripende tiltak kan brukes, er bruk av mobiltelefonovervåking ikke tillatt.

Eksempler på bruk av *MDM* som normalt er tillatt, er fjernsletting av innhold på telefonen dersom den blir stjålet eller mistet, eller å sette restriksjoner på telefonen for hva slags programvare arbeidstakeren kan laste ned og bruke på telefonen. Etter Datatilsynets vurdering er det ikke tillatt å bruke mobilovervåking for å få innsyn i e-post, spore arbeidstakeren, sjekke privat innhold eller lignende, dersom det gjøres av annet enn sikkerhetsgrunner eller i forbindelse med administrasjon av IT-systemet.

Bruk av *MDM* kan innebære at virksomheten får fullstendig kontroll over og tilgang til mobiltelefonen. Programvaren gjør det ofte mulig å velge hva arbeidsgiveren skal ha tilgang til. Virksomheten skal derfor ikke kreve tilgang til annen informasjon enn det som er strengt nødvendig, og sperre tilgangen til informasjon av privat karakter, som bilder, tekstmeldinger, nettbank og Facebook.

Arbeidsgiveren skal gi arbeidstakerne klar og tydelig informasjon om for hvilke formål de trenger tilgang til telefonen, hvilken tilgang virksomheten faktisk har, og hvordan denne informasjonen kan brukes i praksis.*

Regelverkslenke

Personopplysningsforskriften § 9-2 siste ledd

Videre lesning

* Les mer om bruk av Mobile Device Management på Datatilsynets nettsider

GPS-sporing og annen lokalisering i yrkesbiler

En sporingsenhet er en elektronisk innretning som lar arbeidsgiveren eller oppdragsgiveren registrere bevegelsene til virksomhetens kjøretøy. Sporingsenheten lar arbeidsgiveren få detaljert informasjon om posisjonen til kjøretøyet (ofte i sanntid) og dermed hvor arbeidstakeren befinner seg.

For alle praktiske formål baseres det rettslige grunnlaget for ulik bruk av GPS-sporing på en interesseavveining mellom hensynet til den registrerte på den ene siden, og den som ønsker å behandle personopplysninger, på den andre.

Personopplysningene som genereres av GPS-sporingen, må være egnet til å oppfylle det beskrevne formålet med kontrolltiltaket og være saklig i forhold til dette behovet. GPS-sporing i yrkesbiler brukes vanligvis som en elektronisk kjørebok eller til flåtestyring.

Flere arbeidsgivere ønsker å bruke personopplysningene fra sporingsverktøyet til flere formål. (se faktaboks). Det er i prinsippet ikke noe i veien for det, men da må arbeidsgiveren beskrive alle formålene på forhånd og sørge for at drøftings- og informasjonsplikten er overholdt (se fase 1 og 2).

Beskrivelsen av formålene vil være styrende for hva slags personopplysninger som kan behandles, hvor lenge de kan lagres, og hvem i virksomheten som skal ha tilgang til dem.

Eksempel: Avfallsservice-dommen

En arbeidsgiver sammenstilte opplysninger fra et GPS-system med timelistene til en av sine ansatte for å undersøke en mistanke om uberettiget krav om overtidsbetaling. Resultatet fra sammenstillingen ble brukt som grunnlag for å si opp arbeidstakeren. Tingretten kom til at arbeidsgiverens bruk av GPS-data til kontrollformål var i strid med regelverket, men resultatet fra den ulovlige behandlingen ble likevel tillatt ført som bevis. Retten kom til at oppsigelsen var saklig, og uttalte videre at arbeidsgivere i slike saker kan bli ilagt overtredelsesgebyr. (Rt.2013-143)

Elektronisk kjørebok

Formålet med en elektronisk kjørebok er å gi ligningsmyndighetene dokumentasjon på at kjøringen har vært yrkesrettet. Hvilke personopplysninger det vil være relevant å registrere, må vurderes med bakgrunn i skatteetatens dokumentasjonskrav. Hvis virksomheten registrerer flere personopplysninger enn det som kreves dokumentert, behandler arbeidsgiveren personopplysninger utenfor formålet. Slik overskuddsinformasjon har man i utgangspunktet ikke adgang til å behandle etter personopplysningsloven (se faktaboks).

Flåtestyring

Virksomheter som har flere kjøretøy ute i trafikken, kan ha behov for såkalt flåtestyring. Ved flåtestyring benytter virksomheten sporingsenheter som gir oversikt over hvor bilene i bilparken er til enhver tid. På den måten kan henvendelser fra kunder betjenes og følges opp på en mest mulig effektiv måte.

Formålet med flåtestyring er i hovedsak å effektivisere virksomheten, redusere kostnadene og bedre servicen.

Hvis formålet er å styre bilparken i sanntid, vil det ikke være relevant å lagre opplysningene. Hensikten er da å vite hvor bilene er, og ikke hvor bilene har vært.

Detaljregistrering – sensorteknologi

Enkelte sporingsenheter kan registrere til dels svært detaljerte personopplysninger (sensordata), for eksempel hvor hardt sjåføren tråkker på gass- eller bremsepedalen, hvor lenge bilen går på tomgang, om sjåføren foretar en krapp sving, bilens hastighet eller hvilke gravitasjonskrefter kjøretøyet utsettes for.

Datatilsynets praksis viser at adgangen til å behandle slike detaljopplysninger er relativt liten. En slik behandling vil oppleves som inngripende, og virksomheten vil av den grunn neppe klare å oppfylle kravet til interesseovervekt.

Det kan være ulike årsaker til at virksomheter ønsker å registrere slike personopplysninger. I noen tilfeller stilles det som et kontraktsvilkår av en avtalepart.

En avtaleinngåelse gir ikke arbeidsgiveren større adgang til å behandle detaljopplysninger enn de ellers ville hatt, selv om de har inngått en avtale eller vunnet en anbudskonkurranse der de forplikter seg til å utlevere den typen personopplysninger til medkontrahenten.

Det hender at arbeidsgivere ikke er klar over hvilke registreringsmuligheter som ligger i de løsningene de har anskaffet. Uansett er arbeidsgiveren forpliktet til å ha en oversikt over hvilke personopplysninger sporingsenheten registrerer.

Arbeidsgiveren må vurdere om personopplysningene er nødvendige for å oppnå formålet med kontrolltiltaket, og sørge for at tiltaket innføres i tråd med regelverket (se fase 1–4).

Fra januar 2017 er bruk av personopplysninger i forbindelse med elektronisk kjørebok eller flåtestyring unntatt fra meldeplikten. Dette gjelder bare dersom formålet er å dokumentere yrkesrettet kjøring, eller å gi en oversikt over hvor bilene i bilparken er til enhver tid, slik at virksomhetens ressurser kan bli brukt på en effektiv måte.*

Innhenting av helseopplysninger ved ansettelse

I stillingsutlysninger kan ikke arbeidsgiveren be søkere om å gi andre helseopplysninger enn de som er strengt nødvendige for kunne fungere i stillingen. Arbeidsgiveren har heller ikke lov til å innhente slike opplysninger på annen måte. Dette gjelder selv om den som søker på stillingen, samtykker. Søkere vil sannsynligvis tenke at det å si nei vil innebære at man ikke får jobben, og at de dermed ikke har noe reelt valg.

I noen tilfeller kan arbeidsgiveren ha saklig behov for å avklare visse sider ved søkerens helsetilstand.

Arbeidsgiveren kan for eksempel spørre om arbeidssøkeren er i fysisk stand til å gjøre en jobb som krever tunge løft. Det er også tillatt å spørre om søkeren takler stress og høyt arbeidstempo, dersom arbeidet innebærer dette.

Det er ikke tillatt å stille spørsmål om risiko for fremtidige sykdommer eller helseproblemer.

For enkelte yrker er det særlig aktuelt å gjennomføre helseundersøkelser og psykologiske undersøkelser ved ansettelse.

Eksempler på slike yrkesgrupper er

- piloter og dykkere, hvor formelle helsekrav følger av særskilt lov og forskrift
- flere yrker i petroleumsvirksomheten hvor det er krav til helsesertifikater i helsekravforskriften
- loser og andre arbeidstakere på skip
- deltakere i internasjonale fredsoperasjoner

Regelverkslenke

- Arbeidsmiljøloven § 9-3
- Personopplysningsforskriften § 7-11d

Videre lesning

* Les mer om GPS og sporing i yrkesbiler og Datatilsynets veileder for dette.

Medisinske undersøkelser og rus-testing av arbeidssøkere og arbeidstakere

Alle former for helsekontroller er i utgangspunktet et inngrep i den enkelte arbeidstakers personlige integritet. Slike kontroller må derfor begrenses til det som er strengt nødvendig. Samtykke fra arbeidstakeren er ikke et grunnlag for å gjøre medisinske undersøkelser.

Ifølge arbeidsmiljøloven kan arbeidsgiveren bare kreve at medisinske undersøkelser skal gjøres

- når det følger av lov eller forskrift
- ved stillinger som innebærer særlig risiko
- når arbeidsgiveren finner det nødvendig for å verne liv eller helse

Dette omfatter stillinger der arbeidstakeren rutinemessig kommer i situasjoner der konsekvensene av feil er særlig store for arbeidstakeren selv, for tredjeperson eller for samfunnet og det derfor må stilles særlige krav til aktsomhet og oppmerksomhet.

Eksempler på slike stillinger kan være stillinger innen petroleumsvirksomheten (maskinoperatører på borerigger og lignende), luftfarten (kabin- og flypersonale), sjøfarten, jernbanesektoren og helsesektoren.

Begrepet «liv og helse» omfatter både arbeidstakeren selv, andre arbeidstakere og tredjeperson. For at undersøkelsen skal regnes som nødvendig, må faren være alvorlig og fremstå som konkret.

Den enkelte virksomhet skal selv utføre egne risikovurderinger. Dette skal gjøres i samarbeid med de ansattes tillitsvalgte. Det er strenge krav til hvem som gjennomfører tiltakene på stedet, og hvilken form for testing virksomheten kan gjennomføre. Enkelte tiltak kan for eksempel kreve spesielt utdannet helsepersonell. Rutiner for hvordan selve prøvetakingen skal skje, er utarbeidet av Helsedirektoratet (se Kvalitetskrav til rutiner for rusmiddeltesting).

Selv om kravene i arbeidsmiljøloven er oppfylt, kan ikke arbeidsgiveren gjennomføre kontrollen med tvang. Dersom en arbeidstaker nekter, kan det få personalmessige konsekvenser, men arbeidsgiveren kan ikke fysisk tvinge arbeidstakeren til å la seg underkaste medisinske undersøkelser. I ytterste konsekvens kan det å nekte regnes som brudd på arbeidsavtalen og medføre oppsigelse eller avskjed.

Arbeidsgiveren kan også iverksette nødvendige tiltak som bortvisning av en arbeidstaker som for eksempel er ruspåvirket, selv om hjemmel til å foreta en rustest mangler.

Eksempel:

Et fiskebåtrederi praktiserte nulltoleranse overfor ethvert rusmiddel om bord. Det var også nulltoleranse for bruk av ulovlige rusmidler på friturer. Mannskapet var informert om at arbeidsgiveren ville gjennomføre rustester i form av urinprøver og hårprøver. Etter funn av en kanyle på arbeidsplassen ble alle arbeidstakerne avkrevd hårprøve. Et besetningsmedlem som nektet å avgi hårprøve, ble ansett å ha testet positivt. Som følge av dette ble han avskjediget. Retten kom til at avskjedigelsen var gyldig. (RG-2013-620)

Eksempel:

Et vekterselskap ønsket å foreta rusmiddeltest av sine ansatte. Personvernnemnda kom til at både personopplysningsloven og arbeidsmiljøloven er til hinder for at et vekterselskap kan gjennomføre en generell testing av alle sine ansatte. Nemnda uttaler at dersom selskapet begrenser testingen til dem som utfører vektertjenester for sikring av personer mv., vil en testing kunne være tilstrekkelig begrunnet hvis arbeidsgiveren vurderer det slik at dette er nødvendig for å verne «liv eller helse». (PVN-2005-06)

Eksempel:

Arbeidsgiveren innførte tilfeldig rusmiddeltesting ved heliporten, av personer med sikkerhetskritiske stillinger offshore. Petroleumstilsynet vurderte om testingen var lovlig i henhold til arbeidsmiljøloven. I vurderingen la de blant annet vekt på at arbeidsgiveren hadde foretatt en konkret vurdering av i hvilken grad svekket dømmekraft er sikkerhetskritisk, og av antall barrierer som vil kunne fange opp avvik i den forbindelse. Basert på disse vurderingene kom arbeidsgiveren frem til hvilke arbeidstakere som hadde stillinger «som innebærer særlig risiko» og derfor var omfattet av testingen. Det ble blant annet lagt vekt på at forbedrede rutiner for gjennomføring av testingen hadde bidratt til å redusere belastningen for de berørte arbeidstakerne.

Petroleumstilsynet konkluderte med at operatørselskapets praksis var innenfor rammene av regelverket.

Arbeidsgiveren må også i slike tilfeller kunne vise til saklig grunn og sørge for at tiltaket ikke blir en uforholdsmessig belastning. Les mer om denne vurderingen her.

En medisinsk undersøkelse kan være ulovlig dersom dette tiltaket medfører at summen av kontrolltiltak i virksomheten blir for høy. For eksempel kan en blodprøve isolert sett være akseptabel, mens innføring av daglige blodprøver vil kunne overskride tålegrensen.

Regelverkslenke

Arbeidsmiljøloven § 9-4

Regelverket

Kapittel 5

Regelverket

Kontroll og overvåking i arbeidslivet reguleres i hovedsak av to lover: arbeidsmiljøloven og personopplysningsloven:

- Arbeidsgiverens *adgang til å innføre kontrolltiltak* og de ansattes plikt til å medvirke er et arbeidsrettslig spørsmål som først og fremst reguleres av *arbeidsmiljøloven*.
- Arbeidsgiverens *adgang til å behandle opplysningene* som hentes inn gjennom kontrolltiltaket, og som kan knyttes til bestemte ansatte, er et personvernrettslig spørsmål som først og fremst reguleres av personopplysningsloven. Det gjelder blant annet innsamling, lagring, videreformidling mv.
- Arbeidsmiljølovens regler om innføring av kontrolltiltak og *personopplysningslovens* regler om behandling må derfor tolkes og praktiseres i lys av hverandre.

Balansen mellom arbeidsgiverens styringsrett og arbeidstakerens rett til personvern

Arbeidsgiverens styringsrett innebærer at arbeidsgiveren har rett til å organisere, lede, kontrollere og fordele arbeidet. Det er styringsretten som danner grunnlaget for at arbeidsgiveren kan innføre kontrolltiltak i virksomheten.

Arbeidsgiveren står likevel ikke fritt til å innføre kontrolltiltak. Ansatte har rett til personvern og privatliv også på jobb, og styringsretten kan være begrenset gjennom lovverk, tariffavtaler, individuelle avtaler og rettspraksis.

For å balansere arbeidsgiverens og arbeidstakerens behov må det gjøres en avveining av

- virksomhetens behov for kontroll
- typen tiltak
- hvor inngripende kontrollen vil virke overfor arbeidstakeren

For at kontrolltiltaket skal være lovlig, må virksomhetens behov for kontrolltiltaket veie tyngre enn ulempene for arbeidstakeren.

Kontroll og overvåking må være saklig begrunnet

Både arbeidsmiljøloven og personopplysningsloven legger vekt på at det må finnes en saklig grunn for å kontrollere og samle inn opplysninger om arbeidstakere.

I arbeidsmiljøloven heter det at *«tiltaket må ha saklig grunn i virksomhetens forhold»*.

Ifølge personopplysningsloven må virksomheten kunne vise til en *«berettiget interesse»*, det vil si et saklig behov for opplysningene ut fra de oppgavene den skal løse. Det må være en naturlig sammenheng mellom grunnen til at opplysningene samles inn, og den virksomheten som drives.

I arbeidsmiljøloven omfatter begrepet «saklig grunn» («saklig formål») en lang rekke forhold. Både teknologiske, økonomiske, sikkerhets-, arbeidsmiljø- og helsemessige forhold er eksempler på forhold som vil kunne utgjøre saklig grunn for et kontrolltiltak.

Saklighetskravet i arbeidsmiljøloven § 9-1 inneholder to hovedelementer:

1. Formålet med kontrolltiltaket må være forankret i virksomhetens drift. I tillegg må det være egnet til å avdekke det man ønsker å kontrollere.

2. Kontrolltiltaket må avsluttes når behovet for kontroll ikke lenger er til stede (krav om vedvarende saklighet).

Saklighetsvilkåret innebærer også et forbud mot usaklig forskjellsbehandling av arbeidstakere eller grupper av ansatte i forbindelse med kontrolltiltaket.

Kravet til saklig grunn innebærer at tiltaket må ha et tydelig formål. Ifølge personopplysningsloven må arbeidsgiveren (den behandlingsansvarlige) gjøre det klart både for seg selv og for den registrerte (den det behandles opplysninger om) hva formålet er. Formålet må være klart før opplysningene samles inn eller registreres, og er med på å sette en klar ramme for hva opplysningene kan og ikke kan brukes til.

Forbud mot gjenbruk av opplysninger

Personopplysningsloven tillater ikke at opplysningene brukes til nye formål som er uforenlige med det opprinnelige formålet (se faktaboks) Det eneste unntaket fra forbudet er hvis den registrerte samtykker til behandlingen til det nye formålet. I mange tilfeller vil det imidlertid være problematisk å oppfylle kravet til frivillig samtykke i et arbeidsforhold. Hvis den nye bruken er uforenlig med innsamlingsformålet, er arbeidsgiveren avskåret fra å gjennomføre kontrolltiltaket.

Et nytt formål vil ofte være uforenlig med det opprinnelige hvis det skiller seg klart fra det opprinnelige og/eller går utover det arbeidstakerne forventer. Hvor mye som skal til før det nye behandlingsformålet regnes som uforenlig med det gamle, må vurderes konkret og individuelt.

Formålsbegrensningen i personopplysningsloven begrenser adgangen til å ta i bruk opplysninger som opprinnelig er samlet inn for ett bestemt formål, til nye formål.

Arbeidsgivere bør derfor være nøye når de beskriver hvilket formål opplysningene skal brukes til.

Tiltakene må stå i forhold til belastningen

Arbeidsmiljøloven legger vekt på at tiltakene skal stå i forhold til den belastningen de påfører arbeidstakerne. Selv om et tiltak er saklig begrunnet, vil det kunne medføre en for stor ulempe for arbeidstakerne. Det kan for eksempel innebære inngrep i rettigheter som personlig integritet, verdighet, privatlivets fred eller «legemets ukrenkelighet». I så fall vil vilkårene for å gjennomføre kontrollen bare unntaksvis være oppfylt.

Det skal mye til for at tradisjonelle kontrolltiltak i arbeidslivet skal kunne anses som uforholdsmessige. Dette gjelder blant annet tidsregistrering, adgangskontroll, produksjons- og resultatkontroll og kontroll i forbindelse med konkret mistanke om straffbare forhold og andre mislighold i arbeidsforholdet.

Av arbeidsmiljøloven fremgår det også at det ikke er nok å vurdere ett tiltak isolert. Arbeidsgiveren må vurdere summen av kontrolltiltak i virksomheten.

Selv om et kontrolltiltak er i samsvar med lovens krav, vil gjennomføringen av det kunne være ulovlig dersom summen av tiltakene fører til at tålegrensen for arbeidstakeren eller arbeidsmiljøet blir overskredet.

Også personopplysningsloven veier belastningen på den registrerte *(arbeidstakeren)* opp mot arbeidsgiverens behov for registrering.

Loven sier at personopplysninger bare kan behandles dersom

- den enkelte har gitt samtykke til behandlingen, eller
- behandlingen har hjemmel i lov *(det vil si hjemmel i annet regelverk enn personopplysningsloven)*, eller
- behandlingen er nødvendig og faller inn under et av de oppgitte kriteriene i personopplysningsloven

Når arbeidsgiveren ber om samtykke, kan arbeidstakeren oppleve det som vanskelig å nekte. Kravet om frivillig samtykke kan derfor være problematisk å oppfylle i arbeidsforhold. Dette er grunnen til at inngrep i den ansattes personvern normalt må ha et annet rettslig grunnlag enn samtykke, ifølge Datatilsynets praksis.

Hjemmel i lov kan være aktuelt for noen typer overvåking og kontroll i arbeidslivet, men det er relevant bare for en liten andel tiltak.

Det aktuelle rettslige grunnlaget er derfor oftest et av nødvendighetskriteriene. Personopplysningsloven § 8 bokstav f innebærer at personopplysninger kan

behandles dersom dette er nødvendig for å «ivareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen.

Da må arbeidsgiver veie virksomhetens behov for personopplysninger opp mot den enkeltes behov for personvern. For å kunne behandle personopplysninger etter dette alternativet må virksomhetens behov veie tyngst.

Både arbeidsmiljøloven og personopplysningsloven legger vekt på at virksomheten må sørge for at det er den minst inngripende fremgangsmåten som velges, og at behandlingen samlet sett er forholdsmessig.

Kontrolltiltak som registrerer sensitive personopplysninger

Hvis virksomheten vil behandle sensitive personopplysninger, vil det være mer krevende å oppfylle kravet til behandlingsgrunnlag. Det er fordi *personopplysningsloven § 9* ikke åpner opp for en avveining av interesser som i *personopplysningsloven § 8 bokstav f.*

For arbeidsgivere vil personopplysningsloven § 9 bokstav f være det mest aktuelle behandlingsgrunnlaget. Sensitive personopplysninger kan behandles dersom det er «nødvendig for at den behandlingsansvarlige kan gjennomføre sine arbeidsrettslige plikter eller rettigheter.» I lovforarbeidene står det at uttrykket «arbeidsrettslige plikter eller rettigheter» omfatter alle plikter og rettigheter som hviler på et arbeidsrettslig grunnlag, uansett om grunnlaget er lovgivning, avtale mellom partene i arbeidslivet eller individuelle arbeidsavtaler.

Arbeidsgiveren kan for eksempel behandle nødvendige helseopplysninger i forbindelse med oppfølging og rehabilitering av arbeidstakere eller for å kunne vurdere et krav om erstatning for usaklig oppsigelse.

Kravet til nødvendighet gjelder også i disse tilfellene. Det vil si at den aktuelle behandlingen er den minst inngripende fremgangsmåten, og at behandlingen samlet sett er forholdsmessig.

Saksbehandlingsregler – krav om åpenhet og informasjon

Konsekvensen av kontrolladgangen er at arbeidstakerne har plikt til å godta og medvirke til kontrolltiltaket. Derfor har arbeidsmiljøloven § 9-2 en bestemmelse om drøfting, informasjon og evaluering av kontrolltiltak. Her er det gitt saksbehandlingsregler. Disse gjelder prosessen i forkant av innføring av kontrolltiltak, samt krav om evaluering av tiltakene etter at de er satt i verk.

Plikten til å drøfte omfatter alle de sentrale elementene i forbindelse med etablering og gjennomføring av kontrolltiltak, og den gjelder også ved endringer av eksisterende kontrolltiltak. Målet er at partene gjennom drøftelsen kommer frem til løsninger som i størst mulig grad begrenser inngrepet i arbeidstakerens personlige forhold. Også andre ulemper ved kontrollen bør unngås, for eksempel forringelse av arbeidsmiljøet. Kontrollvolumet i virksomheten bør holdes så lavt som mulig.

Drøftelsene skal finne sted så tidlig som mulig, slik at arbeidstakerne har en reell mulighet til å komme med innvendinger og innspill. Informasjonsplikten gjelder uansett om det finnes tillitsvalgte ved virksomheten eller ikke. Dette er viktig fordi informasjonsplikten også omfatter hvordan kontrollen vil bli innrettet, for eksempel hvor kontrollutstyret blir plassert, hvordan utstyret virker, undersøkelsesmetoder etc.

Arbeidsgiveren skal sammen med de tillitsvalgte jevnlig evaluere behovet for kontrolltiltakene. Det skal sikre at tiltak som ikke lenger har saklig grunn, avsluttes.

Jevnlig evaluering er et viktig virkemiddel for at summen av kontrolltiltak i virksomheten ikke skal bli for stor.

Personopplysningsregelverket bygger også på et prinsipp om at behandlingen av personopplysninger skal være gjennomsiktig. Det er derfor gitt egne regler om informasjon, og arbeidsgiver skal klart og åpent informere om sine handlinger.

Personopplysningsloven gir den enkelte krav på å få informasjon når opplysninger om vedkommende behandles. Informasjonen skal gis uoppfordret. Det skal alltid gis informasjon blant annet om hva slags opplysninger som behandles, hvilke formål opplysningene skal brukes til, om det er frivillig å gi fra seg opplysninger, og annet som gjør den registrerte i stand til å ivareta sine rettigheter etter personopplysningsloven. Ansatte har, som alle andre, rett til å få innsyn i de personopplysningene som gjelder ham eller henne.

Oppsummering

Arbeidsmiljølovens regler om innføring av kontrolltiltak og personopplysningslovens regler om behandling av personopplysninger stiller i stor grad de samme kravene til arbeidsgiveren. De ulike regelverkene må derfor tolkes og praktiseres i lys av hverandre.

De arbeidsrettslige reglene inneholder de samme normene som personopplysningsloven bygger på, men begrepene som brukes, varierer.

Kravet til saklighet og forholdsmessighet i arbeidsmiljøloven § 9-1 vil normalt være det samme som kravet til «berettiget interesse» i personopplysningsloven § 8 bokstav f. Det betyr at dersom vilkårene for å gjennomføre selve kontrollen er til stede, vil normalt også vilkårene etter *personopplysningsloven § 8 bokstav f* være oppfylt. Arbeidsgiveren vil da kunne behandle personopplysningene som stammer fra kontrolltiltaket.

Arbeidsgiveren må likevel være oppmerksom på at alle personopplysningslovens regler, for eksempel saksbehandlingsreglene, gjelder fullt ut ved behandling av opplysningene.

Myndighetene

Kapittel 6

Les mer om:

- Arbeidstilsynet
- Datatilsynet
- Personvernnemnda
- Petroleumstilsynet

Myndighetene

Arbeidstilsynet

Arbeidstilsynets viktigste oppgave er å bidra til at arbeidsmiljølovens bestemmelser blir fulgt opp i virksomhetene. Arbeidstilsynet skal medvirke til et trygt og sikkert arbeidsliv og bidra til å forebygge arbeidsrelatert sykdom og skade.

Arbeidstilsynet fører tilsyn med at virksomhetene forebygger ulykker og helseskader og på den måten forebygger sykefravær og utstøting.

I tilsynene kontrolleres risikoforhold, dokumentasjon av rutiner og systemer og om det er samsvar mellom dokumentasjon og virkelighet.

Overfor virksomheter som ikke følger opp ansvaret knyttet til arbeidsmiljølovens krav, kan Arbeidstilsynet gi reaksjoner som pålegg, tvangsmulkt, overtredelsesgebyr og eventuelt stansing. Alvorlige forhold kan bli politianmeldt.

Arbeidstilsynet har en egen veiledningstjeneste, Svartjenesten, som svarer på spørsmål fra både personer og virksomheter.

Datatilsynet

Datatilsynet er den norske personvernmyndigheten og har oppgaver både som tilsynsorgan og som ombud. Datatilsynet skal medvirke til at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem.

Datatilsynet skal kontrollere at lover og forskrifter for behandling av personopplysninger blir fulgt, og at feil og mangler blir rettet. Det gjøres blant annet gjennom tilsyn og saksbehandling. Ved brudd på kravene i personopplysningsloven med forskrift kan Datatilsynet gi pålegg om nødvendige endringer. Datatilsynet kan også fatte vedtak om overtredelsesgebyr og tvangsmulkt.

Datatilsynet har en egen veiledningstjeneste som svarer på spørsmål fra både personer og virksomheter.

Kontaktinformasjon

Arbeidstilsynet
tlf. 73 19 97 00
www.arbeidstilsynet.no

Datatilsynet
tlf. 22 39 69 00
www.datatilsynet.no

Myndighetene

Personvernnemnda

Personvernnemnda behandler klager på vedtak fattet av Datatilsynet. Personvernnemndas vedtak blir lagt ut på nettsidene deres.

Petroleumstilsynet

Petroleumstilsynet har myndighetsansvar for sikkerhet og arbeidsmiljø i petroleumsvirksomheten på norsk sokkel og på enkelte landanlegg og tilknyttede rørledninger.

Petroleumstilsynet har myndighetsansvar for teknisk og operasjonell sikkerhet, herunder beredskap, samt for arbeidsmiljø i alle faser av virksomheten, som ved planlegging, prosjektering, bygging og bruk og ved eventuell senere fjerning av innretninger og anlegg.

Petroleumstilsynet har med andre ord en rolle både som høyrisiko-/teknologitilsyn og som arbeidstilsyn.

På samme måte som Arbeidstilsynet fører Petroleumstilsynet tilsyn med at virksomhetene innen petroleumsnæringen forebygger ulykker og helseskader, herunder sykefravær og utstøting, gjennom et systematisk helse-, miljø- og sikkerhetsarbeid.

Petroleumstilsynet har, på samme måte som Arbeidstilsynet, ulike sanksjonsmidler som kan tas i bruk overfor virksomheter som ikke følger opp regelverkets krav.

Kontaktinformasjon

Personvernnemnda
www.personvernnemnda.no

Petroleumstilsynet
tlf. 51 87 60 50
www.ptil.no

Bakgrunnsmateriale og forskning:

Mona Bråten:

Digital kontroll og overvåking av arbeid – Omfang og praksis, Fafo-rapport 2016:05

Tommy Tranvik:

Det gjennomsiktige arbeidslivet. Erfaringer med feltteknologi i utvalgte yrker

Dag Wiese Schartum:

Rettslige aspekter ved feltteknologi i arbeidslivet, Complex 3/2013

Mona Bråten:

Kontroll og overvåking – utfordringer for personvern og arbeidsmiljø. En kunnskapsstatus, Fafo-notat 2013:17

Stortingsmelding:

Meld. St. 11 (2012–2013) Personvern – utsikter og utfordringer

Mona Bråten og Tommy Tranvik:

Kontroll med ansatte utenfor fast arbeidssted. Ansattes erfaringer med feltteknologi, Fafo-rapport 2012:50

Utredning fra Personvernkommisjonen:

NOU 2009: 1 Individ og integritet — Personvern i det digitale samfunnet

Kontroll og overvåking i arbeidslivet, Fafo-rapport 2010:46

Mona Bråten:

Personvern under press – hvor går grensene i arbeidslivet?, Fafo-rapport 2008:34

9 gode råd ved innføring av kontrolltiltak på arbeidsplassen

1. Start prosessen i god tid, og hold en åpen og lyttende dialog. Forklar hvorfor virksomheten ønsker å innføre ny teknologi, og hvordan.
2. La de ansatte få komme med sine synspunkter tidlig – lytt, og utfør nødvendige justeringer.
3. Legg arbeid i avveiningen mellom behovet for å ivareta virksomhetens interesser kontra hensynet til den enkeltes personvern. Kan målet nås på en mindre belastende måte? Skaff deg grundig kjennskap til hvilke data systemet faktisk genererer – det kan være mer enn behovet tilsier.
4. Fastsett tidspunkt for evaluering av tiltaket tidlig.
5. Skriv referat fra møter med de ansatte eller tillitsvalgte der saken er drøftet.
6. Vær bevisst på hva som nedfelles i eventuelle avtaler med tillitsvalgte.
7. Vurder behovet for lagring og hvor lenge lagring er nødvendig.
8. Vær forsiktig med kobling av data – vurder alltid om bruk av informasjonen er i tråd med det opprinnelige formålet med tiltaket.
9. Søk bistand om du er usikker!