Ansattes rett på personvern
vs.
virksomhetens behov for sikkerhetstiltak

Hva er lov og hva er ikke lov?

Hanne Gulseth, personvernombud

Agenda

- Oversikt
- Personvern i arbeidslivet
  - *Personvernerklæring for ansatte og konsulenter*
- Informasjonssikkerhet og behov for sikkerhetstiltak
  - *Hva er lov og hva er ikke lov?*
- Hvilke sikkerhetstiltak har vi?

Oversikt

Ansattes krav på personvern

- **Rett til privatliv**: Ansatte har rett til privatliv, også på arbeidsplassen. Dette betyr at overvåking og kontrolltiltak må være proporsjonale og nødvendige for å oppnå et legitimt formål.
- **Informasjon:** Ansatte skal informeres om hvilke personopplysninger som samles inn, hvordan de brukes, og hvem som har tilgang til dem.
- **Tilgang til egne data**: Ansatte har rett til å få tilgang til, rette og slette sine egne personopplysninger som virksomheten behandler.

Virksomhetens behov for sikkerhetstiltak

- **Informasjonssikkerhet**: Virksomheten må beskytte sensitive data mot uautorisert tilgang, tap eller skade. Dette inkluderer sikkerhetstiltak som f.eks. logging og sikkerhetsmonitorering, brannmurer, antivirusprogrammer, kryptering, samt organisatoriske tiltak som opplæring av ansatte og etablering av sikkerhetspolicyer.
- **Internkontroll**: For å sikre at personopplysninger behandles lovlig og sikkert, må virksomheten ha en systematisk tilnærming til internkontroll. Dette innebærer å etablere rutiner for oppfyllelse av virksomhetens plikter og de registrertes rettigheter.
- **Risikovurdering**: Virksomheten bør regelmessig gjennomføre risikovurderinger for å identifisere potensielle trusler og sårbarheter, og implementere passende sikkerhetstiltak basert på disse vurderingene.

sto

Personvern i arbeidslivet

- Alle arbeidsgivere behandler opplysninger om sine ansatte og konsulenter.
- Ansatte og konsulenter bruker telefon, pc, og mange og ulike IT-systemer som innebærer behandling av personopplysninger.
- Det er utfordrende å vite hvilke opplysninger som samles inn, hva som lagres og hvordan opplysningene blir brukt.

Personvernerklæringen for ansatte og konsulenter

(finnes nederst til høyre på Intranett)

- **Informasjon** om hvilke personopplysninger som behandles, og hvorfor.
- Selskapet er **behandlingsansvarlig** – og følger personvernprinsippene, (se Policy for personvern).
- **Formålet** er å administrere ditt ansattforhold, og din bruk av telefon, pc og IT-systemer; for drifts- og sikkerhetsmonitorering.
- **Behandlingsgrunnlagene** er avtale, berettiget interesse og rettslige forpliktelser.

Informasjonssikkerhet

- Alle virksomheter trenger å beskytte sine egne og kunders data, både mot interne og eksterne trusler.

- Sikkerhetshendelser kan få store konsekvenser:

  Det kan være tap av
  - verdier
  - forretningshemmeligheter
  - taushetsbelagt informasjon
  - omdømme

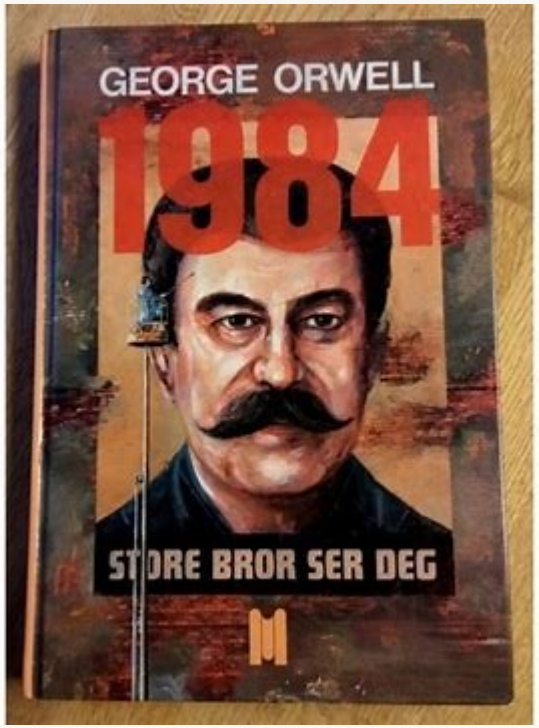
Krav til informasjonssikkerhet følger også av rettslige forpliktelser

- IKT-forskriften
- GDPR artikkel 32 (informasjonssikkerhet)
- Sikkerhetsloven
- NIS2 og DORA
- Lov om vern av forretningshemmeligheter

Noe treffer oss direkte, eller indirekte i avtaler med kunder.

Sikkerhetstiltak er helt nødvendig, men..

- Kan utfordre de ansattes personvern fordi noen tiltak innebærer at det samles inn store mengder opplysninger om de ansattes bruk av IT-systemer.
- Fare for ulovlig overvåkning av de ansatte.
- Fare for at opplysningene blir brukt til andre formål enn de var innhentet for.
- Spredning av informasjonen.
- At opplysningene ikke blir slettet.
- Ansatte er usikre på hva som faktisk gjøres.



Sikkerhetstiltak vs. ansattes personvern – dilemma?

Ikke enten eller, men begge deler.

- Personvernregler må følges når sikkerhetstiltaket innebærer behandling av personopplysninger:
  - GDPR
  - Arbeidsmiljølovens kapittel 9 om **kontrolltiltak**
    - Forskrift om innsyn i e-postkasse og annet elektronisk lagret materiale

- Krav i spesiallovgivning må følges for informasjonssikkerhet:
  - IKT-forskriften
  - Sikkerhetsloven
  - NIS2 og DORA
  - lov om vern av forretningshemmeligheter

Sentrale krav i GDPR som må vurderes

- **Oversikt** over hvilke opplysninger som behandles
- Definere **formål(ene)**
- Identifisere **behandlingsgrunnlag(ene),** som regel:
  - Nødvendig for å oppfylle ansettelsesavtalen (administrasjon)
  - Berettiget interesse (for sikkerhetstiltakene)
  - Rettslig forpliktelse (krav til informasjonssikkerhet)
- **Dataminimering** – kan man klare seg med mindre omfattende behandling, færre opplysninger, mindre inngripende tiltak?

Sentrale krav i GDPR forts.

- Hvordan skal det gis **informasjon?**
  - Ved iverksetting av tiltak
  - Informasjon til nyansatte
  - Personvernerklæring
- Hvem skal ha **tilgang** ?
- Rutine for **sletting** . **Lagringstid?**
- **Behandlingsprotokoll**
- **Risikovurdering, og vurdere behov for DPIA**
  (berettiget interesse krever en balansetest)

Lovkrav til kontrolltiltak, AML kap. 9

1) Krav om **saklig grunn i virksomhetens forhold** og ikke **uforholdsmessig belastning** .

2) Arbeidsgiver plikter å **drøfte** behov, utforming, gjennomføring og vesentlig endring av kontrolltiltak i virksomheten med arbeidstakernes tillitsvalgte (hos oss verneombud)

3) Plikt til å gi **informasjon** til de ansatte om formålet med kontrolltiltaket, konsekvenser av kontrolltiltaket og antatt varighet

4) Plikt til å **evaluere** tiltaket

Tiltaket må ikke innebære en «uforholdsmessig belastning for arbeidstakeren»

- Arbeidsgivers behov for tiltaket må vektes opp mot konsekvensene tiltaket har for de ansatte.
- Kravet til forholdsmessighet innebærer også en begrensning relatert til omfanget, utformingen og den konkrete praktiseringen av kontrolltiltaket.
- Tiltaket må ikke gå lenger enn det som er *nødvendig* for å oppnå formålet med tiltaket.

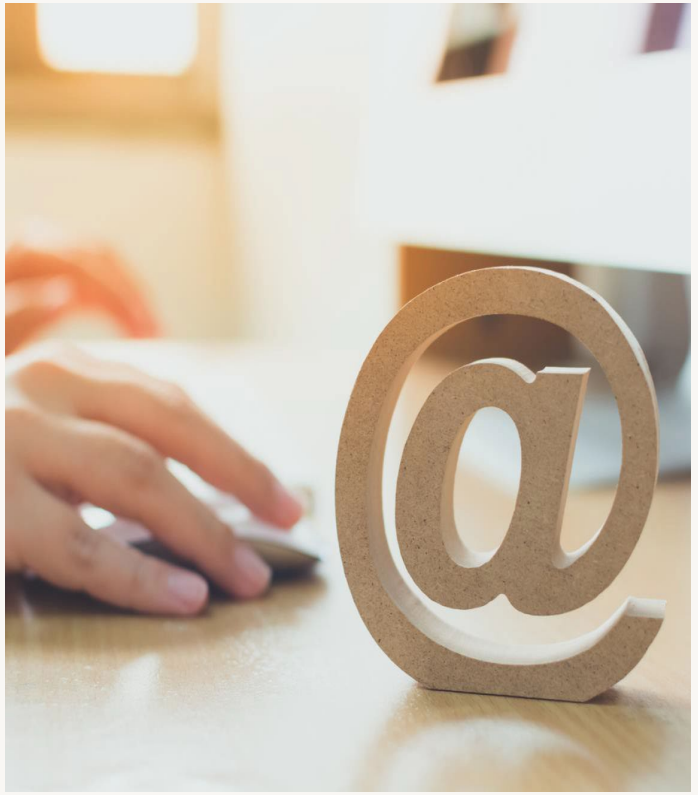
Arbeidsmiljølovens regler om kontrolltiltak

AML § 9-5 viser til e-postforskriften som **forbyr** arbeidsgiver innsyn i og overvåkning av ansattes epost og annet elektronisk lagret materiale (kontrolltiltak).

E-postforskriften – rett til innsyn på visse vilkår

- Gjelder for **arbeidsgivers rett**
  - **til innsyn** i opplysninger lagret i e-postkasse som arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet, og arbeidstakers personlige områder i virksomhetens datanettverk eller annet elektronisk utstyr som arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet.

- Adgang til innsyn på spesifikke vilkår:
  - ✓ **Nødvendig pga daglig drift eller andre berettigede interesser**
  - ✓ **Begrunnet mistanke** om bruk av epost eller elektronisk utstyr medfører grovt brudd på arbeidsrettslige forpliktelser



E-postforskriften - forbud mot overvåkning, med to unntak:

- E-postforskriften § 2 andre ledd:

«Arbeidsgiver har ikke rett til å ***overvåke*** *arbeidstakers bruk av elektronisk utstyr, herunder bruk av internett,* ***med mindre*** *formålet er:*

- ✓ *Å* ***administrere virksomhetens datanettverk*** *eller*
- ✓ *Å* ***avdekke eller oppklare sikkerhetsbrudd*** *i nettverket»*

Hva er «overvåking»?

- Ikke definert i forskriften, derfor kan vi anta at tiltaket
  - bør ha en viss varighet eller skje gjentatte ganger,
  - må være en form for innsamling av personopplysninger om den ansatte gjennom elektronisk utstyr stilt til rådighet av arbeidsgiver,
  - gir de ansatte en følelse av å bli overvåket, og en utrygghet for at den ansatte ikke vet og ikke har kontroll med hva opplysningene kan bli brukt til.

Om verktøy som planlegges tatt i bruk omfattes av forbudet i e-postforskriften eller om de oppfyller unntakene, må vurderes i tråd med ansvarlighetsprinsippet, dvs alltid vurdere om tiltaket er lovlig før det starter. Uavhengig av hensikten (formålet), f.eks. bruk av purview, slike tiltak kan innebære at opplysninger om arbeidstaker samles inn.

Hva betyr de to unntakene?

a) «**å administrere virksomhetens datanettverk**»

Hendelse(r) som medfører brudd på konfidensialitet, integritet, tilgjengelighet eller robusthet ved IT-systemene

b) «**å avdekke eller oppklare sikkerhetsbrudd i nettverket**»

Alle praktiske og tekniske tiltak som er nødvendige for at systemene, nettverk, utstyr og programvare skal fungere etter hensikten

Hvilke sikkerhetstiltak har vi?

(spesifisert i personvernerklæring)

- Epost; avsender, mottaker, dato, tid, tittel, navn på vedlegg – men ikke innhold i epost og vedlegg
- Kalender; tema for møte, møtedeltakere, tidspunkt, sted, varighet, men ikke innhold i møtebeskrivelsen
- Fildelingssystem
- Besøkte internettsider (dato, tid, domenenavn, og undersider dersom det ikke benyttes https). Hvis mistanke om misbruk kan mer detaljert informasjon innhentes.
- Logging og sikkerhetsmonitorering
  - sikkerhetsalarmer og endepunktslogger fra innrullerte enheter
  - annen nettverks- og klientaktivitet
- Sikkerhetskopi og gjenoppretting
- Sikkerhetstesting; penetrasjonstester og sikkerhetsanalyser
- Sikkerhetsrevisjoner
- Opplæring av de ansatte
- Adgangskontroll
- Tilgangsstyring
- Nettverksadministrasjon
- Kryptering
- Avvikshåndtering
- Rutiner og instrukser

Før gjennomføring av sikkerhetstiltak må sentrale krav i AML og GDPR vurderes og dokumenteres.

Full gjennomgang av personvernprinsippene

- Lovlig, rettferdig og gjennomsiktig
- Formålsbegrensning
- Dataminimering
- Riktighet
- Lagringsbegrensning
- Integritet og konfidensialitet
- Ansvarlighet

Policy for personvern

Formål

Formålet med denne policy er å beskrive prinsippene som legges til grunn for all behandling av personopplysninger i vårt selskap.

Bakgrunn

Lov om behandling av personopplysninger setter rammer for hvordan vi behandler personopplysninger. Se Lov om behandling av personopplysninger (personopplysningsloven) - Lovdata

Loven bygger på noen grunnleggende prinsipper i GDPR artikkel 5. **Alle som behandler personopplysninger må gjøre det i samsvar med disse prinsippene.**

Intern

Omfang

Policy for personvern omfatter hele selskapets virksomhet og gjelder for alle ansatte, konsulenter og andre som utfører arbeid for selskapet.

De detaljerte kravene som gjelder for oss finner du i Standard for behandling av personopplysninger.

Prinsipper

#1. Lovlig, rettferdig og gjennomsiktig

Hva logges ikke?

•SMS, WhatsApp, Messenger eller andre meldingsformer på mobil. Unntak er Slack, Teams og andre jobb-relaterte tjenester hvor dataen flyter gjennom selskapet.

•Nettverkstrafikk på mobil som ikke går over jobbnettverk.

•Mottaker, avsender eller innhold i privat epost som skjer i browser på PC. Dette er en av grunnene til at man ikke burde bruke privat epost i Outlook eller mail applikasjon på jobb-pc

Selskapet har kun tilgang til data/operasjoner som er lastet ned på selskaps-PC eller foregår på selskapets nettverk.