Tekna –
Teknisk-naturvitenskapelig forening
Postboks 2312 Solli
0201 Oslo

www.tekna.no
Org.nr 971 420 782
post@tekna.no
+47 22 94 75 00

Datatilsynet

Vår ref.:	Deres ref.:	Dato:
[Navn]	[Navn]	29. november 2023

Teknas innspill til Datatilsynets veileder - Overvåkning av ansattes bruk av elektronisk utstyr

Tekna – Teknisk naturvitenskapelig forening er den største masterforeningen i Norge, og den største fagforeningen i Akademikerne med over 105 000 medlemmer. Våre medlemmer har mastergrad eller mer fra tekniske og naturvitenskapelige fagområder.

Datatilsynet har bedt om innspill til veileder om overvåkning av ansattes bruk av elektronisk utstyr som allerede ligger tilgjengelig på Datatilsynets nettside.[1] Tekna har vurdert veilederen sammen med egne tillitsvalgte og internt i vårt sekretariat. Tekna har da konkludert med å utforme et forslag til en alternativ veileder.

Tekna ser det som positivt at Datatilsynet involverer andre når tilsynet utformer sine veiledere. Tekna håper slik samarbeid kun utvikles til glede for begge parter når det gjelder særlige utfordringer om personvern i arbeidslivet.

Kontroll- og overvåkning er et problem flere av Teknas medlemmer og tillitsvalgte opplever, særlig relatert til fenomenet bossware. Det vises i den sammenheng til FAFO-rapport nr 2023:12 Digitalisering, personvern og tillitsvalgtes medvirkning.

Den rettslige reguleringen av kontroll og overvåkning av ansatte
Temaet «Overvåkning av ansattes bruk av elektronisk utstyr» er forholdsvis bortgjemt i *Forskrift om arbeidsgivers innsyn i epostkasse og annet elektronisk lagret materiale*. Selve forskriftens tittel er et problem i seg selv. Plasseringen av overvåknings-bestemmelsen som eget avsnitt to under § 2 om *vilkår for innsyn* innebærer også at den rettslige reguleringen oppleves bortgjemt. Skillet mellom kontroll og overvåkning kommer heller ikke frem av forskriften. Av disse grunner er rettsområdet veilederen omhandler forholdsvis utilgjengelig. Og etter

[1] https://www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/overvaking-av-ansattes-bruk-av-elektronisk-utstyr/

Teknas vurdering er det ingen god begrunnelse for å skille mellom overvåking og kontroll.

Det foreslås derfor at forskriften får en annen betegnelse. Det foreslås da at alt benevnes «kontroll og overvåkning», eventuelt at alt benevnes «kontroll». Eventuelt må skillet mellom disse to begrepenes avklares på en konsis måte.

Med en felles regulering av kontroll og overvåkning, bør veilederen om overvåkning kunne inngå i «Veileder om kontroll og overvåkning i arbeidslivet» Datatilsynet har vært med å utforme. Sistnevnte veileder bør uansett oppdateres. Tekna kan gjerne involveres i dette.

Datatilsynets veileder – i tilfelle lov og forskrift på området ikke endres
Veilederen Datatilsynet selv har utformet har mange kvaliteter. Likevel fremstår veilederen for tung og omfattende juridisk sett til å kunne fungere som et best mulig oppslagsverk for hoved-målgruppen arbeidsgivere. De mange henvisningene til ulike rettskilder forvirrer mer enn å oppklare, og noen av eksemplene, definisjonene og bruken av «jungelspråket» for de uinnvidde er ikke så gode som de burde være. Blant annet kan dette føre til at man ikke har en felles forståelse av sentrale begreper, og Tekna mener det er behov for en klargjøring. Språkrådets definisjon av «overvåkning» er for eksempel en annen enn den Datatilsynet legger til grunn. Uten en klargjøring av begrepet "overvåkning", så kan dette både tolkes som overvåkning av datanettverk og/eller atferd og holdninger hos de ansatte.

Forslag til alternativ veileder:

Overvåkning av ansattes bruk av elektronisk utstyr

– veileder for arbeidsgivere

Veilederens formål

Denne veilederen regulerer hvordan arbeidsgiver lovlig skal kunne overvåke arbeidstakernes bruk av elektronisk utstyr. Veilederen gjelder ikke kontrolltiltak i virksomheten og kameraovervåking.

Hva er forbudt?
Overvåkning av arbeidstakerne i en virksomhet er ulovlig dersom overvåkningen skjer i strid med vilkårene i e-postforskriften (Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale) § 2, andre ledd. Denne bestemmelsen lyder:

Arbeidsgiver har ikke rett til å overvåke arbeidstakers bruk av elektronisk utstyr, herunder bruk av Internett, med mindre formålet med overvåkingen er

a. å administrere virksomhetens datanettverk eller

b. å avdekke eller oppklare sikkerhetsbrudd i nettverket.

Formålet med overvåkningen
Formålet med overvåkningen ligger implisitt i teksten i bestemmelsen i E-postforskriften, og skal ivareta at informasjon i alle former i virksomheten:

- Ikke blir kjent for uvedkommende (konfidensialitet)
- Ikke blir endret utilsiktet eller av uvedkommende (integritet)
- Er tilgjengelig ved behov (tilgjengelighet)

Hva innebærer vilkårene i epostforskriften som åpner for overvåkning?
Vilkårene i epostforskriften for lovlig overvåkning gjelder dersom tiltaket:

1. Behandler personopplysninger
2. Gjelder «overvåkning»
3. Gjelder arbeidstakerens «bruk av elektronisk utstyr»
4. Gir arbeidsgiver faktisk tilgang til opplysningene
5. «Administrerer virksomhetens datanettverk», eller;
6. «Avdekker eller oppklarer sikkerhetsbrudd i organisasjonen»

Nærmere om de enkelte vilkår

1. Behandler personopplysninger
«Behandling»: All bruk av personopplysninger, slik som innsamling, registrering, sammenstilling, lagring og utlevering, eller en kombinasjon av slike bruksmåter.

«Personopplysning»: Opplysning eller vurdering som kan knyttes til en enkeltperson. Dette kan være navn, adresse, telefonnummer, e-postadresse, bilnummer, bilder eller fødselsnummer.

Anonymisering av de registrerte dataene er ikke alltid nok for at det ikke dreier seg om personopplysningene. Dette fordi flere opplysninger satt opp mot hverandre kan avsløre personen som er anonymisert.

2. Overvåkning
«Overvåkning»: Det å ha oppsyn med eller holde vakt over et objekt.

En overvåkning forutsetter videre å vare *over en viss tid*. Dette i motsetning til kontrolltiltak i virksomheten som skjer sporadisk og som reguleres av arbeidsmiljøloven kap 9 (lenke til annen side hos Datatilsynet).

Overvåkning med kamera reguleres ikke i E-postforskriften og må tilfredsstille vilkårene i Forskrift om kameraovervåking i virksomhet som du kan lese mer om her (lenke til annen side hos Datatilsynet).

En teoretisk mulighet for at personopplysningene som overvåkes også kan brukes til å kontrollere de ansattes atferd eller holdninger, er ikke tilstrekkelig for å karakterisere tiltaket som overvåkning. Tiltaket må altså være av et visst omfang.

Eksempel
En vanlig funksjon i samhandlingsverktøy er en indikator (for eksempel farge eller ikon) som viser om arbeidstakeren er pålogget, borte eller frakoblet. I utgangspunktet er dette ikke overvåking.

Arbeidstakerens opplevelse av å bli overvåket kan innebære overvåkning, selv om tiltaket ikke er ment som overvåkning fra arbeidsgivers side.

Eksempel
De ansattes pulter utstyres med en sensor for å registrere tilstedeværelse på free seating-kontoret for å regne ut hvor store arealer en virksomhet har behov for i forbindelse med flytting. Sensorene registrer ikke den enkelte person, men kan av de ansatte likevel oppleves som en overvåkning av dem selv.

3. Bruk av elektronisk utstyr
Vilkåret er knyttet til "bruk av elektronisk utstyr, herunder bruk av internett". Dette henger sammen med e-postforskriftens virkeområde. «Elektronisk utstyr» skal her defineres vidt, er teknologinøytral og omfatter stort sett alt som arbeidstaker bruker på arbeidsplassen, så lenge det er verktøy som samler inn eller kan brukes til å utlede personopplysninger. Men lydopptak faller utenom, se Les mer om lydopptak i arbeidslivet (lenke til annen side hos Datatilsynet).

Elektronisk utstyr kan for eksempel være:

- Datamaskiner – Nettbrett – Mobiltelefoner – Printere

Arbeidsgiveren må ha gitt arbeidstakeren utstyret med det formålet at det skal benyttes i arbeidet for at forskriften skal gjelde.

Arbeidstakere som også bruker utstyret i privat sammenheng, er beskyttet av forskriften.

4. Gir arbeidsgiver faktisk tilgang til opplysningene
Vilkåret om at arbeidsgiver faktisk har tilgang til personopplysningene som behandles gjennom tiltaket må forstås implisitt i forskriften.

5. Administrere virksomhetens datanettverk
For at overvåkningen skal være lovlig, er det altså et vilkår at overvåkingen av de ansattes bruk av elektronisk utstyr iverksettes for å administrere virksomhetens datanettverk.

Ut fra en språklig forståelse må vilkåret antas å omfatte alle praktiske og tekniske tiltak som er nødvendige for at systemene, nettverk, utstyr og programvare skal fungere.

6. Avdekker eller oppklarer sikkerhetsbrudd i organisasjonen
Informasjonssikkerhet (tiltak for å verne konfidensialiteten, integriteten og tilgjengeligheten til opplysningene) omfatter mer enn

personopplysningssikkerhet som er regulert i artikkel 32 til 34 i personvernforordningen.

For å oppnå informasjonssikkerhet, må virksomheten identifisere risikoer informasjonsverdiene er utsatt for, og planlegge og gjennomføre egnede tiltak som skal redusere risikoene til et akseptabelt sikkerhetsnivå for virksomheten. Les mer om informasjonssikkerhet og personopplysningssikkerhet, slik det er regulert i personvernregelverket.

Begrepene å "avdekke" eller "oppklare" innebærer gjerne verktøy som motvirker sikkerhetsbrudd, og bruk av logger og lignende til etterarbeidet med å oppklare sikkerhetsbrudd eller annen mistenkelig aktivitet.

Spamfilter
Et spamfilter identifiserer både virus og andre typer skadelig programvare. E-post som blir identifisert som spam, blir lagt i karantene og er ikke synlig for arbeidstakeren.

Så lenge e-posten ligger i karantene er den synlig for "admin" hos arbeidsgiveren. Aktuelle virkemidler for å begrense inngrepet i personvernet ved bruk av spamfilter, er å begrense tilgangen til spamfilteret til så få administratorer som mulig, utarbeide tydelige rutiner for hvordan administratorene skal utføre arbeid med spamfilteret, og logge administratorenes innsyn i spamfilteret slik at virksomheten kan avdekke eventuell snoking.

Logging
Logging er å holde oversikt over både pågående og tidligere hendelser i virksomhetens systemer. Det innebærer for eksempel at et selskap følger med på inn- og utgående trafikk i nettverket sitt for å avdekke unormal trafikk og mulige angrep på nettverket.

Eksempler på logging kan være:

- *Brannmur.* Her logges trafikken i virksomhetens nettverk. Det vil si alle IP-adresser en arbeidstaker er inne på. Innsyn i denne loggen kan utgjøre overvåking, fordi innsynet gir oversikt over arbeidstakers bruk av elektronisk utstyr over tid.

- *Loggføring av aktivitet/tilgangsstyring*. Dette innebærer loggføring av hvem som går inn på tilgangsstyrte mapper i virksomhetens systemer, og når de har vært inne. For eksempel vil det være nødvendig i helsesektoren å overvåke når ansatte har vært inne i pasient-journaler. Les mer om logging på Nasjonal sikkerhetsmyndighet sine nettsider (nsm.no)

Sjekkliste for arbeidsgiver
Vi har laget en kort oppsummering / sjekkliste dere kan gå gjennom dersom dere er usikre på om tiltaket dere vurderer å innføre vil være omfattet av forbudet mot å overvåke arbeidstakeres elektroniske utstyr.

1. Innebærer tiltaket behandling av personopplysninger?
Hvis ja: Tiltaket må oppfylle de generelle kravene i personopplysningsloven og personvernforordningen. Gå videre til punkt 2.

Hvis nei: Reglene i personvernregelverket gjelder ikke.

2. Omfatter tiltaket:

- arbeidstakeres bruk av elektronisk utstyr, herunder internett?
- overvåking?
- at arbeidsgiveren får tilgang til opplysningene?

Hvis ja på alle disse: Gå videre til punkt 3.

Hvis nei på ett eller flere: Tiltaket omfattes ikke av forbudet mot overvåking i e-postforskriften, men må oppfylle de generelle kravene i personopplysningsloven med personvernforordningen.

3. Skjer overvåkingen for noen av disse formålene:
Administrere virksomhetens datanettverk?

Avdekke eller oppklare sikkerhetsbrudd i nettverket?

Hvis ja på et av disse: Unntaket er oppfylt. Tiltaket er lovlig, så lenge det oppfyller kravene i personvernforordningen.

Hvis nei: Tiltaket er ulovlig.

Med vennlig hilsen

Line Henriette Holten
generalsekretær