

Gjennomføring av sikring og analyse av elektronisk lagrede data som inneholder personopplysninger

Sikring og analyse av elektronisk lagrede data er et komplisert område både juridisk og teknisk. Personvernlovgivningen setter grenser for hvordan elektroniske data som inneholder personopplysninger kan sikres og behandles. For å sikre konfidensialitet, integritet og bevisverdi av dataene må sikringen og behandlingen gjennomføres av ekspertise innenfor området. Nedenfor er det beskrevet ulike momenter og utfordringer knyttet til sikring og behandling av elektronisk lagret informasjon.

Rettslige rammer for innsyn i e-post og elektroniske data

Grunnlag for behandling av elektronisk lagrede data. Behandlingsansvarlig etter personopplysningsloven og eventuelt annen lovgivning som regulerer behandling av elektronisk lagret informasjon er den som ønsker innsyn i dataene. Behandlingsansvarlig, dvs. den som ønsker innsyn i e-post eller andre elektroniske data, må foreta juridiske vurderinger om det foreligger grunnlag for innsyn og behandling av elektronisk lagret informasjon etter personopplysningsloven og -forskriften eller annet regelverk. Ibas vil på oppdrag fra behandlingsansvarlig være databehandler etter nevnte regelverk, og handler på oppdrag og instruks fra oppdragsgiveren og underlagt databehandleravtale som må inngås.

Spesielt om innsyn i ansattes e-post og elektronisk lagret informasjon. Innsyn i ansattes elektronisk lagret informasjon ble endret i personopplysningsforskriften og trådte i kraft 1. mars 2009. Etter de nye reglene har arbeidsgiver innsyn i ansattes e-post og elektroniske filer når det:

- er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten, eller
- foreligger begrunnet mistanke om at arbeidstakers bruk av e-postkassen medfører grovt brudd på de plikter som følger av arbeidsforholdet, eller kan gi grunnlag for oppsigelse eller avskjed.

Ett av disse grunnlagene må foreligge for at det skal være anledning til innsyn. Foruten e-post kan innsyn gjennomføres i personlige område i virksomhetens datanettverk og i andre elektroniske kommunikasjonsmedier eller elektronisk utstyr som er stilt til den ansattes bruk i arbeidet.

Er det grunnlag for innsyn, kan dataene sikres og den ansatte skal så langt som mulig varsles og få anledning til å uttale seg før innsyn foretas i de sikrede data. Varselet skal inneholde grunnlaget for innsynet og begrunnelse for dette, og det skal orienteres om den ansattes rettigheter etter regelverket. Arbeidstakeren skal også så langt mulig gis anledning til å være tilstede under innsynet, even-

tuelt sammen med tillitsvalgt eller annen representant. Er den ansatte ikke varslet, skal denne informeres snarest etter at innsynet er gjennomført. Det skal da gis samme informasjon som i det nevnte varselet, samt informasjon om hvilken metode for innsyn som ble benyttet, hvilke data som ble gjennomgått samt resultatet av innsynet (dvs. hva ble funnet av relevant informasjon). Dette gjelder ikke ved undersøkelse av straffbar handling mv. Nevnte gjelder både overfor nåværende og tidligere ansatte, samt andre som utfører eller har utført arbeid for den som ønsker innsynet. Dette gjelder også for innsyn i slettede data.

Speilkopiering/sikring. For å sikre integriteten og bevisverdien i data som skal gjennomgås, bør det tas speilkopi, dvs. en identisk kopi hvor integriteten til dataene opprettholdes ved spesielle kopieringsmetodikk. En slik kopiering gir trygghet både for arbeidsgiver og den ansatte ved at det kan dokumenteres at det ikke er skjedd endringer i dataene, det være seg endringer foretatt av arbeidstaker etter at denne ble informert om forestående innsyn, eller endringer foretatt ifm gjennomføring av selve innsynet. Se nedenfor om hvordan dette gjennomføres av Ibas.

Speilkopiering/sikring kan imidlertid kun gjøres dersom det foreligger grunnlag for innsyn som nevnes ovenfor. Foreligger det grunnlag for innsyn, kan alle data som er aktuelle for innsyn sikres, selv om det senere viser seg at kun deler av de sikrede data vil bli gjennomgått.

Gjennomføring av innsynet. Innsyn i e-post og andre elektroniske data skal etter personopplysningsforskriften gjennomføres på en slik måte at dataene så langt som mulig ikke endres og at frembrakte opplysninger og analyseresultater kan etterprøves. Det stilles krav til å sikre integriteten og bevisverdien av dataene, og Ibas benytter verktøy og metoder som sikrer nevnte både ved bevis-sikringen og under gjennomføring av innsyn, se nedenfor.

Ved gjennomgangen av den ansattes e-postkasse og andre data, danner grunnlaget for innsynet rammene for innsynes omfang. Avdekkes det informasjon som arbeidsgiver ikke har rett til innsyn i, skal e-post eller dokumenter straks lukkes, og

eventuelle kopier av det sikrede materialet skal slettes.

Gjennomføring av sikring, lagring og analyse

Ibas AS gjennomfører datasikring, lagring og analyse av datamaterialet på vegne av oppdragsgivere. Ibas er databehandler etter personopplysningsloven og Ibas følger personopplysningsloven med forskrift samt annet relevant regelverk i behandling av elektronisk lagret informasjon.

Metoder for sikring av datamateriale. Teknologi som benyttes til sikring av individuelle lagringsenheter og annet datamateriale er spesialutviklet og dedikert til formålet. Sikringen kan også gjennomføres ved bruk av oppdragsgivers infrastruktur der dette er påkrevet eller hensiktsmessig. Dette kan for eksempel gjelde sikring av kryptert informasjon, sikring av servere via nettverket eller bruk av oppdragsgivers system for sikkerhetskopiering (backup/restore). Ibas benytter både utstyr som anses å være det ledende innenfor elektronisk sikring og gransking, og egenutviklet spesialutstyr.

Speilkopiering. Ibas sikrer datamaterialet på dedikerte lagringsmedier. Forutsatt at original lagringsenhet er uten feil, vil speilkopien være en identisk kopi av original enhet. Verktøyet/programvaren som benyttes ved sikring genererer digital sjekksum (MD5 Hash) som verifiseres mot innholdet på original lagringsenhet for å bekrefte kopiens integritet. Denne digitale sjekksummen kan sammenlignes med et fingeravtrykk som vil være unikt for det sikrede datamaterialet. Ved speilkopiering benyttes skriveblokker som forhindrer skrivning/ending av innhold på original datalagringsenhet.

Sikring av informasjon fra systemer i bruk. Ibas kan også sikre informasjon fra aktive systemer som e-postservere, filservere, databaseservere, produksjonssystemer o.l. Verifisering med digital sjekksum kan benyttes, men har ikke samme anvendelse her som ved sikring av lagringsmedia som kan tas ut av drift.

Oppbevaring. Lagringsmedier som inneholder sikret informasjon krypteres når oppdragsgiver ønsker dette eller det er påkrevet. Datalagringsenhetene kan om ønskelig forsegles. Når kopiene ikke benyttes til innsyn/analyse, vil lagringsenhetene lagres i sikkert område iht. Ibas' rutiner. Lagringsmedia kan også lagres hos oppdragsgiver eller hos andre eksterne parter (escrow) etter avtale.

Kryptering. Ibas tilbyr kryptering av alle data for å sikre mot innsyn fra uvedkommende og at data kommer på avveie. Regime for håndtering av krypteringsnøkler avtales nærmere i det enkelte oppdrag.

Dokumentasjon. Det føres bevissikringslogg (chain of custody) som inneholder informasjon som identifiserer hvor informasjonen er sikret fra (original maskin og lagringsenhet), digital sjekksum, identifikasjon av lagringsmedia som inneholder speilkopi og kopiert data, samt logging av eventuelle hendelser under sikringen og hvem som håndterer informasjonen/lagringsenhetene.

Sletting av sikret informasjon. Lagringsenheter som inneholder sikrede data vil slettes ved overskriving da saken avsluttes, og etter nærmere avtale med oppdragsgiver/ databehandlingsansvarlig og iht. personopplysningsloven. Ibas vil utføre sikker sletting av data etter gjeldende standarder.

Analyse og gjennomgang av sikrede data. Analyse av sikrede data og premissene for dette gjennomføres etter nærmere avtale med oppdragsgiver/databehandlingsansvarlig. Ibas gjennomfører analysen i henhold til gitt mandat. Alternativt kan datamaterialet behandles og tilgjengeliggjøres slik at oppdragsgiver selv kan utføre innsyn, med dataverktøy spesielt tilpasset slik gjennomgang.

Ibas kan stille utstyr og programvare til rådighet for oppdragsgivere som selv ønsker å gjennomføre gjennomgang av data. Hvilken type verktøy som benyttes vil bl.a. avhenge av hvordan innsynet skal gjennomføres, og vil normalt innebære indeksering av det gjeldende materialet. Dette gir mulighet for raske og effektive søk. Ibas kan tilby løsninger for gjennomgang for alle prosjektstørrelser, fra mindre datamengder hvor en person forestår gjennomgang/innsyn til store og komplekse prosjekter hvor flere titalls personer er involvert i å foreta innsynet.

Rapportering. Ibas dokumenterer utført arbeid og resultater av eventuell analyse av sikrede data i en skriftlig rapport til databehandlingsansvarlig. Ibas' medarbeidere har også erfaring med å vitne i rettsaker for å redegjøre for hvordan data er sikret og analysert.

For mer informasjon kan du kontakte:

- **Thomas Dahl, dataetterforskningsjef**
IBAS AS
Tlf: 9166 0057/ thomas.dahl@ibas.no
www.ibas.no
 - **Jan Sandtrø, advokat/partner**
SIMONSEN Advokatfirma DA
Tlf: 9973 1934 / js@simonsenlaw.no
www.simonsenlaw.no
-