

Sammendrag:

Behandling av personopplysninger i norske virksomheter

Denne rapporten presenterer resultatene fra en utvalgsundersøkelse om norske virksomheters behandling av personopplysninger. Blant de 424 virksomhetene i utvalget, finner vi offentlige og private næringsvirksomheter, offentlig forvaltning og offentlig tjenesteprodusenter og andre (for eksempel frivillige organisasjoner). I rapporten bruker vi betegnelsen ”virksomheter” om alle disse.

Undersøkelsen tar sikte på å avdekke:

- Hvilke personopplysninger som behandles i virksomhetene.
- I hvilken grad virksomhetene etterlever kravene til behandling av personopplysninger som følger av personopplysningsloven eller forskriften til loven.
- Virksomhetens kunnskap om og holdninger til lovverket og til de sentrale offentlige organene for ivaretaking av personvernet.
- Virksomhetenes holdning til personvern veid opp mot enkelte andre interesser.

Hovedkonklusjoner

Undersøkelsen tyder på en grunnleggende positiv holdning til personvern blant virksomhetene. Kunnskapen om personopplysningsloven og de pliktene som følger av den, er imidlertid lav. Svært mange av virksomhetene mener at kravene ikke gjelder for dem, selv om de behandler personopplysninger og følgelig er omfattet av loven. En lav andel av virksomhetene sier seg helt enig i at de etterlever de konkrete kravene som følger av loven eller forskriften. Dette gjelder krav til informasjonssikkerhet, internkontroll og informasjon til den som opplysningene gjelder.

Virksomhetene behandler mange typer personopplysninger

Virksomhetene i utvalget behandler mange typer personopplysninger om egne ansatte og om kunder, klienter, brukere og andre eksterne personer. En stor del av dem behandler også opplysninger som i loven er definert som sensitive opplysninger. En av tre virksomheter behandler for eksempel helseopplysninger om egne ansatte og en av tre behandler opplysninger om ansattes medlemskap i fagforeninger. Dette er opplysninger som etter loven er sensitive. Behandling av dem krever konsesjon, med mindre opplysningene er avgitt uoppfordret.

77 prosent av virksomhetene sier at de behandler opplysninger om kunder, klienter, brukere eller andre eksterne personer, også opplysninger som etter loven er definert som sensitive. Det er flere virksomheter innen offentlig tjenesteyting og forvaltning som behandler opplysninger om eksterne personer enn blant øvrige virksomheter. Denne gruppen omfatter helse- og sosialtjenester og undervisning, noe som vil forklare at en stor andel behandler personopplysninger om eksterne personer.

Svak etterlevelse av personopplysningsloven

Utvalget består av virksomheter med fire eller flere ansatte. Alle virksomhetene i utvalget behandler følgelig personopplysninger og er dermed omfattet av personopplysningsloven.

Loven eller forskriften til loven stiller opp en rekke plikter som skal oppfylles når personopplysninger behandles. Dette gjelder krav til *informasjonssikkerhet* og *internkontroll* og en *informasjonsplikt* overfor den som personopplysningene gjelder for. Undersøkelsen avdekker at en svært stor andel av virksomhetene mener at tiltak som skal til for at disse pliktene er oppfylt, ikke er aktuelle for dem. Dette vitner om en dårlig kjennskap blant virksomhetene om hvilke plikter de har etter loven.

Vi har bedt representantene for virksomhetene om å si seg mer eller mindre enige i at de gjennomfører ulike tiltak som skal til for å hevde at de etterlever pliktene.

Internkontroll og informasjonssikkerhet

Med en tredeling av svarene i ”enig”, ”verken eller” og ”uenig”, sier om lag halvparten at de har etablert et system for internkontroll. Likevel er det en god del av disse igjen som ikke sier seg enig i at de har rutiner for sletting av opplysninger som ikke lengre er nødvendige for det opprinnelige formålet. Uten rutiner for sletting kan man vanskelig hevde at man gjennomfører tilfredsstillende internkontroll. Å ikke slette opplysninger som ikke lenger er nødvendige for det opprinnelige formålet, er også et direkte brudd med loven og ikke bare en indikasjon på manglende internkontroll. 40 prosent av alle virksomhetene sier de har slike rutiner.

Bare en av tre virksomheter sier at de fører en systematisk oversikt over hvilke personopplysninger som behandles i virksomheten. Det er strengt tatt ikke mulig å oppfylle de ulike kravene i personopplysningsloven uten en slik oversikt. 44 prosent av virksomhetene sier enten at en slik oversikt ikke er aktuell eller de sier seg *helt uenige* i at de har en slik oversikt.

Av de ulike kravene til informasjonssikkerhet og internkontroll som vi har spurt om, er det kun 4 prosent av virksomhetene som sier seg *helt enige* i at de har gjennomført de ulike tiltakene. 30 prosent kan ikke si seg helt enige i at de har gjennomført et eneste ett.

Det er ikke store forskjeller mellom private og offentlige næringsvirksomheter på den ene siden og offentlig forvaltning og tjenesteyting på den andre når det gjelder å gjennomføre ulike tiltak som skal til for å oppfylle kravene til informasjonssikkerhet og internkontroll. Størrelsen på virksomhetene (målt etter antall ansatte) har liten betydning for om kravene til informasjonssikkerhet og internkontroll etterleves.

Informasjonsplikten

Kun mellom en firedel og halvparten av virksomhetene gir alltid den typen informasjon som vi har spurt om, til den som opplysningene gjelder for. Hva opplysningene skal brukes til og retten til innsyn, er det virksomhetene oftest svarer at de alltid informerer om. Det er likevel bare 35 prosent som alltid informerer om dette. Kun en av fire informerer alltid om det er frivillig å gi fra seg opplysninger eller ikke, og kun 30 prosent informerer alltid om hvorvidt opplysningene vil bli gitt til andre eller ikke.

De virksomhetene som behandler opplysninger om eksterne personer, etterlever ikke i særlig større grad informasjonsplikten enn alle virksomhetene sett under ett. Blant disse virksomhetene er det bare 6 prosent som svarer at de alltid gir *alle* typer informasjon vi har spurt om. 33 prosent kan ikke svare ”ja, alltid” til en eneste en av dem.

Virksomheter innen offentlig forvaltning og tjenesteyting er flinkere enn de andre til å oppfylle de ulike sidene ved informasjonsplikten. Det er ikke særlig forskjell mellom store og små virksomheter.

Positiv holdning til personvern, lover og regler, men lite kunnskap

Det er stor oppslutning om behovet for et sterkt Datatilsyn. Det er imidlertid bare 16 prosent som sier at de har god kjennskap til Datatilsynets rolle og oppgaver og bare 4 prosent sier det samme om Personvernnemnda. Med en tredeling av svarene i ”enig”, ”nøytral” og ”uenig”, er det blant dem som sier de har noe kjennskap til personopplysningsloven, 70 prosent som mener at loven er nødvendig. Det er bare 6 prosent av dem som mener loven kun er nødvendig for noen spesielle sektorer og aktiviteter.

Positiv holdning, men lite kunnskap til personopplysningsloven

Hele en av tre sier at de har lite kjennskap til personopplysningsloven. Blant de som sier de *har* noe kjennskap til loven, er det hele 28 prosent som ikke kan svare på om loven er lett å forstå og 21 prosent *kan ikke svare* på om loven er lett å etterleve. Blant de virksomhetene som har et klart standpunkt til dette, er det flere som mener at loven både er lett å forstå og lett å etterleve enn som mener det motsatte.

Påstanden om at lover og regler som beskytter personvernet er for strenge, får heller ikke tilslutning blant virksomhetene. På spørsmål om hva som kan være den viktigste grunnen til at enkelte virksomheter ikke følger kravene i loven, svarer tre av fire *mangel på kunnskap* om lovgivningen. At lovgivningen er for lite fleksibel eller at det er for tidkrevende å tilpasse seg den, får lav tilslutning blant virksomhetene.

Personvern hensynene veier tungt

Når virksomhetene blir bedt om å vurdere personvern opp mot andre interesser, lar en overvekt av dem *personvernet veie tyngst*. Et stort flertall av virksomhetene er uenige i at arbeidsgiveren skal ha ubegrenset rett til innsyn i de ansattes e-post og i at arbeidsgiveren skal ha anledning til skjult kameraovervåking på arbeidsplassen for å avdekke mulige lovbrudd. Nesten halvparten av virksomhetene sier at de er *helt uenige* i dette. Det er noe høyere oppslutning om

at arbeidsgiveren uten varsel bør kunne se hvilke internettsider de ansatte har besøkt. Tre av fire virksomheter mener det bør være strenge regler for utveksling av opplysninger, selv om en friere utveksling kan gi bedre produkter og tjenester. En av tre sier seg *helt enig* i dette.