

VEDLEGG 3 GRUNPRINSIPPER FOR BEHANDLING AV PERSONOPPLYSNINGER

For å være i stand til å ivareta innbyggernes rettigheter etter personvernregelverket, er det nødvendig å ha en god forståelse av de grunnleggende prinsippene for lovlig behandling av personopplysninger, og ikke minst hva en personopplysning er.

Hva er en personopplysning?

Som ansvarlig for behandling av personopplysninger om innbyggere og ansatte i en kommune, er det vesentlig å være klar over grensene for hva som er en personopplysning og samtidig at verdien av informasjonen må sees fra perspektivet til den den gjelder. Generelt er det viktig å være klar over at terskelen er veldig lav for at en opplysning faller inn under definisjonen, og at regelverket dermed gjelder.

Definisjonen av begrepet «personopplysninger» består av to elementer:

- 1) Det må dreie seg om en «opplysning».
- 2) Opplysningen må handle «om» en identifisert eller identifiserbar fysisk person.

Når det gjelder det første elementet, hva som er en «opplysning», så skal dette skal forstås svært vidt, og ifølge juridisk litteratur er det ingen begrensninger knyttet til verken art, innhold eller form. Det stilles for eksempel ingen krav til at opplysningene skal være betydningsfulle, sanne, troverdige, objektive, subjektive eller typisk knyttet til privatlivets fred. Objektive fakta om en person, for eksempel informasjon om hvilken type bolig noen bor i, vil være en personopplysning. Subjektive opplysninger er også personopplysninger, for eksempel vurderinger og utsagn om at en elev «har en tendens til å havne i krangel». Hvorvidt opplysningene er offentliggjort og/eller allment kjente, betyr heller ikke noe. Det er nok at opplysningene befinner seg i kommunens systemer i en eller annen form.

Når det gjelder det andre elementet, at opplysningen må være knyttet til en «identifisert eller identifiserbar» fysisk person, er også denne terskelen svært lav. Det er ikke et krav at personen må være identifisert. Det er tilstrekkelig at det er mulig å identifisere vedkommende. For eksempel vil initialer være en identifikator som ikke alene kan identifisere en person i et lands befolkning, men som kan være tilstrekkelig til å identifisere en person i et klasserom eller på en arbeidsplass. Kjønn og alder vil kanskje ikke være tilstrekkelig for å identifisere en person i en hel kommune, men tilstrekkelig på f. eks en avdeling.

Det er viktig å være oppmerksom på at det heller ikke er et krav at kommunen selv har muligheten for å identifisere; det er tilstrekkelig at noen andre kan sammenkople tilstrekkelig med identifikatorer slik at en person blir identifisert.

Personvernprinsippene

Personopplysningsloven og personvernforordningen inneholder både rettigheter og plikter. Felles for alle reglene er at de bygger på noen grunnleggende prinsipper. Alle som behandler personopplysninger må opptre i samsvar med disse prinsippene.

Prinsippene gir på ulike måter uttrykk for at behandling av personopplysninger skal skje på en måte som i størst mulig grad sikrer forutsigbarhet og forholdsmessighet for enkeltmennesket.

Under er en gjennomgang av personvernprinsippene:

Lovlig, rettferdig og gjennomsiktig

At behandlingen av personopplysninger må være lovlig innebærer først og fremst at det må finnes et rettslig grunnlag for en planlagt behandling av personopplysninger. Personvernforordningen har en liste over rettslige grunnlag, og minst ett av disse må være oppfylt for at behandlingen skal være lovlig. Prinsippet om lovlighet kan også sies å inkludere alle de øvrige prinsippene og reglene for behandling av personopplysninger som en behandlingsansvarlig må oppfylle.

At behandlingen av personopplysninger må skje rettferdig betyr at den skal gjøres i respekt for de registrertes interesser og rimelige forventninger. Behandlingen skal være forståelig for de registrerte, og ikke foregå på skjulte eller manipulerende måter.

Gjennomsiktig betyr i denne sammenheng at bruken av personopplysninger skal være oversiktlig og forutsigbar for den som opplysningene gjelder for. Gjennomsiktighet bidrar til å skape tillit, og det setter enkeltpersonen i stand til å bruke sine rettigheter og ivareta sine interesser.

Formålsbegrensning

Personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål. Det betyr at ethvert formål som innebærer behandling av personopplysninger skal identifiseres og beskrives presist. Alle formål skal være forklart på en måte som gjør at alle berørte kan forstå hva personopplysningene skal brukes til. At formålet skal være legitimt, innebærer at det i tillegg til å ha et rettslig grunnlag, også skal være i samsvar med øvrige etiske og rettslige samfunnsnormer. Personopplysninger kan ikke gjenbrukes til formål som er uforenlige med det opprinnelige formålet.

Dataminimering

Prinsippet om dataminimering innebærer å begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere formålet med innsamlingen. Dersom personopplysninger ikke er nødvendige for å oppnå formålet, skal man heller ikke samle dem inn. Prinsippet er nyttig som ledetråd for valg av tiltak for å begrense risiko knyttet til personvern. F. eks ved at man ikke behandler direkte identifiserbar informasjon hvis dette ikke er nødvendig.

Riktighet

Personopplysninger som behandles skal være korrekte, og de skal om nødvendig oppdateres. Dette betyr at den behandlingsansvarlige må sørge for straks å slette eller rette personopplysninger som er uriktige ut i fra de formålene de er samlet inn for.

Lagringsbegrensning

Prinsippet om lagringsbegrensning innebærer at personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for.

Integritet og konfidensialitet

Personopplysninger skal behandles slik at opplysningenes integritet, konfidensialitet og tilgjengelighet

beskyttes. Det betyr at den behandlingsansvarlige må sørge for å iverksette tiltak mot utilsiktet og ulovlig ødeleggelse, tap og endringer av personopplysninger.

Ansvarlighet

Prinsippet om ansvarlighet understreker ansvaret for å opptre i samsvar med reglene for behandling av personopplysninger. Dette ansvaret ligger på alle virksomheter som behandler personopplysninger. Det er ikke nok å bare ha ansvar, man må vise at man tar ansvar. Det betyr at virksomheten må kunne dokumentere at den har gjennomført tiltak for å etterleve personvernforordningen. Virksomheten må opptre proaktivt og etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid.

[Datatilsynet har laget en utfyllende veiledning til personvernprinsippene der de går mer grundig gjennom hva prinsippene betyr.](#)

I tabellen under er det en oversikt over hvordan prinsippene kommer til uttrykk gjennom plikter for kommunen og eksempler på operasjonaliseringen av pliktene:

Prinsipp (artikkel 5)	Plikt	Referanse	Eksempel
Lovlighet	Personopplysninger skal behandles på grunnlag av et behandlingsgrunnlag	Artikkel 6	Særlovgivning for barnevern, skole, sosialtjenester, helse og omsorg
Rettferdighet og åpenhet	Kommuner skal gi innbyggerne informasjon om hvordan personopplysninger behandles	Artiklene 12-15	Overordnet informasjon i en personvernerklæring Spesifikk informasjon i vedtak, brev, møte, etc.
	Enkeltpersoner som er berørt av brudd på personopplysningssikkerheten kan ha rett til informasjon om hva som har skjedd	Artikkel 34	Spesifikk informasjon i vedtak, brev, møte, etc.
Formålsbestemthet	All bruk av personopplysninger skal ha et forhåndsbestemt formål	Artikkel 12, 24, 30	Formål med bruk av personopplysningene følger ofte av behandlingsgrunnlaget. Formålet skal beskrives i informasjon til innbyggere og av behandlingsprotokollen. Formål skal være forklart på

			en måte som gjør at alle berørte har samme entydige forståelse av hva personopplysningene skal brukes til.
Dataminimering	Begrense mengden og detaljeringsgraden av personopplysninger som hentes inn. Begrense til det som er nødvendig for å oppnå formålet.	Artikkel 24 og 25	Lage rutiner for hvilken informasjon som skal innhentes og jevnlig kontrollere at det følges opp
Riktighet	Personopplysninger som behandles skal være korrekte	Artikkel 24 og 25	Rutiner for å sjekke om opplysninger er korrekt og oppdatert
Lagringsbegrensning	Det skal være klart hvor lenge opplysningene skal lagres	Artikkel 24 og 25	Arkivloven, kassasjonsregler Samtykkets rekkevidde
Integritet og konfidensialitet	Kommuner skal gjennomføre risikovurderinger	Artikkel 32	Risiko- og sårbarhetsvurdering skal gjennomføres av IKT-systemer før anskaffelse
Ansvarlighet	Kommunen skal ha et internkontrollsystem som sikrer at pliktene i personvernregelverket etterleves	Artikkel 24	Dokumenterte rutiner og prosesser Dokumentert kontroll