



PERSONVERNPOLICY

BAKGRUNN

SiOs visjon er å skape en bedre hverdag for alle studenter. For at SiO skal kunne levere et best mulig tjenestetilbud til studentene, vil det være behov for å samle inn, bruke og oppbevare persondata om studentene. I tillegg er enkelte av SiOs tjenester åpne for andre enn studenter, og disse vil det på samme måte være nødvendig å ha registrerte personopplysninger om. SiOs ansatte er en tredje gruppe der personopplysninger vil være registrert hos SiO.

De overordnede føringer for hvordan SiO skal samle inn, bruke, oppbevare og sikre persondata er gitt i SiOs personvernpolicy

POLICY

SiO skal:

- Alltid opptre i tråd med lover og regler. SiOs virksomhet skal være i samsvar med GDPR-forordningen og norsk personvernlovgivning.
- Kun oppbevare og bruke persondata som er *nødvendig* for å levere et godt tjenestetilbud, ha en effektiv drift og god og lovmessig behandling av kunder og ansatte. Formålet med oppbevaring av persondata skal dokumenteres.
- Etablere innebygget personvern i alle prosesser og systemer. Dette innebærer at SiO skal kunne håndtere hendelser/avvik på en god og lovmessig korrekt måte, og at registrertes rettigheter til sletting, innsyn, endring og portabilitet skal ivaretas. Dette inkluderer også personopplysninger om SiOs kunder og ansatte registrert hos SiOs samarbeidspartnere og leverandører
- Ha tilgjengelige og tydelige kontaktpunkter for registrerte som har spørsmål eller ønsker innsyn/endring/sletting/flytting av data. Tilsvarende for varsling av avvik
- Ha en personvernombud som til enhver tid er oppdatert på lover og regler, har gjennomført nødvendige kurs og har en direkte rapporteringslinje til SiOs administrerende direktør
- Ha kontrakter og/eller samtykkeerklæringer hvor det tydelig fremkommer hvorfor og hvordan persondata registreres og oppbevares, dersom registrering og oppbevaring av persondata ikke er hjemlet i lov
- Benytte systemløsninger som har tilstrekkelig sikkerhetsnivå på lagrede persondata og muliggjør overføring og sletting av data. Der dagens systemer ikke gir slik mulighet, skal SiO ha en tidfestet plan for nødvendig systemendring, og i mellomtiden ha manuelle rutiner som på best mulig måte sikrer registrertes rettigheter
- Ha rutiner for tilgangskontroll som sikrer at kun autoriserte brukere får tilgang til persondata
- Ha tydelige roller og ansvarsforhold internt i organisasjonen. Dette gjelder særlig behandlingsansvarlige, sikkerhetsansvarlige og personvernombud. I tillegg skal generelt lederansvar og -forankring være tydelig.

- Ha et bevisst forhold til risiko for feil og avvik. Systematisk gjennomføre risikovurderinger og vurdere personvernkonsekvenser. Ha gode rutiner for feilretting og avvikshåndtering
- Sørg for nødvendig opplæring av ansatte som behandler persondata

