Personvernerklæring for Felles IAM

Om denne erklæringen

Felles IAM er en tjeneste som gir deg en brukerkonto og riktige tilganger til IT-systemer og ressurser ved institusjonen du er tilknyttet, og som fjerner tilgangen din når du ikke trenger den lenger. Tjenesten leveres av Sikt – Kunnskapssektorens tjenesteleverandør ("Sikt", "vi", "vår", "oss") til universiteter, høyskoler og andre virksomheter i kunnskapssektoren.

Sikt er ansvarlig for å sikre at personopplysningene vi behandler om deg, blir brukt i samsvar med personvernlovgivningen, herunder EUs personvernforordning (GDPR) og personopplysningsloven. Denne personvernerklæringen gir informasjon om hvordan vi behandler personopplysninger om deg når du er eller har vært registrert i Felles IAM.

Sikt har rolle både som behandlingsansvarlig og databehandler for Felles IAM, jf. GDPR art. 4 nr. 7 og 8. **Denne personvernerklæringen gjelder kun for den behandlingen Sikt er behandlingsansvarlig for**. Institusjonen du er tilknyttet er behandlingsansvarlig for hoveddelen av behandlingen av personopplysninger i Felles IAM, blant annet brukerkontoen din, tilganger, kontoaktivering og logger. For spørsmål om dette må du ta direkte kontakt med institusjonen din.

Kategorier av registrerte

Behandlingen omfatter opplysninger knyttet til studenter (inkludert søkere med studierett, privatister eller deltakere i etter- og videreutdanning), ansatte, innleide eller gjester ved en virksomhet som bruker Felles IAM.

Hvilke opplysninger vi behandler og formålet ved behandlingen

Institusjonen du er tilknyttet er behandlingsansvarlig for hoveddelen av personopplysningene som behandles i Felles IAM. Sikt er hovedsakelig databehandler, men har behandlingsansvar for enkelte behandlinger.

Hovedformålet med Sikts behandling av opplysningene er å sikre at du har én identitet i universitets- og høyskolesektoren. Det betyr at:

Når du blir tatt opp eller får tilknytning til en ny institusjon i universitets- og høyskolesektoren, sjekker vi om du allerede har en brukerprofil hos en annen institusjon. Vi gjør dette ved å slå opp i en katalog i systemet for å se om opplysningene dine finnes der fra før.

Hvis vi finner en match, beholder du den samme UHID og det samme UH-brukernavnet fra din tidligere institusjon, hos den nye institusjonen.

Etter at tilknytningen til din institusjon eller institusjoner har opphørt, slettes alle opplysninger om deg fra Felles IAM, med unntak av UHID og UH-brukernavn som forblir lagret i et eget navnerom.

Vi gjør dette for å sikre at UHID og UH-brukernavn aldri blir tildelt en annen person. Når en ny identitet eller et nytt brukernavn skal opprettes, slår vi derfor opp mot de som allerede er lagret. Grunnen til at det er viktig at UHID og UH-brukernavn ikke blir tildelt en annen person, er at dette kan gi en annen person tilgang til dine tidligere kontoer ved utdanningsinstitusjonen dersom disse ikke er slettet.

Sikt er behandlingsansvarlig for følgende opplysninger:

Opplysning	**Spesifisering av hva de brukes til**
Navn og fødselsdato; fødselsnummer, D-nummer eller S-nummer; passnummer hvis du ikke har noen av disse; e-post ved institusjonen, privat e-post og privat mobilnummer	Finne ut om du allerede har en identitet ved en annen institusjon
UHID og UH-brukernavn	Gi deg samme identitet og brukernavn ved den nye institusjonen, dersom du har UHID og UH-brukernavn fra før. Hindre at ID-en og brukernavnet gis til en annen person.

Hvor opplysningene kommer fra

Opplysningene hentes fra institusjonens egne kildesystemer: Felles studentsystem (FS) for studenter, DFØ eller Unit4 (UBW) for ansatte, og gjesteregisteret Greg for gjester. UHID og UH-brukernavn lages av Felles IAM første gang du registreres ved en institusjon.

Behandlingsgrunnlag

Behandlingsgrunnlaget for behandlingen som Sikt er behandlingsansvarlig for, er GDPR art. 6 nr. 1 bokstav f, berettiget interesse.

Sikts berettigede interesse er å gi hver person én identitet i sektoren. Det minimerer antall IDer per person, og bedrer personvernet overordnet i sektoren. Den andre berettigede interessen er å hindre at brukernavn gjenbrukes, slik at en ny person får tilgang til data som hørte til en tidligere bruker.

Sikt leverer en løsning med felles identitet på tvers av institusjoner i UH-sektoren, og har et ansvar for høy sikkerhet og godt personvern for alle brukere. Derfor deler vi UHID og UH-brukernavn mellom institusjonene i Felles IAM, slik at hver person har én felles identitet. For at dette skal være trygt, lagrer vi UHID og UH-brukernavn og slår dem opp hver gang en ny ID opprettes. Slik sikrer vi at en ID som er eller har vært i bruk, aldri tildeles en annen person, og at den samme personen kan gjenbruke sin ID fra en annen institusjon man er tilknyttet. Det hindrer at noen ved en feil får tilgang til en annen persons data eller kontoer.

Vi har vurdert at dette innebærer en svært liten ulempe for deg. UHID og UH-brukernavn er vanligvis ikke alene direkte identifiserende, men det kan oppleves uventet at Sikt, som ikke er arbeidsgiver eller studiested, behandler opplysningene som behandlingsansvarlig. Vi mener at behovet for å beskytte

personopplysningene dine veier tyngre enn denne ulempen, og at løsningen totalt sett styrker sikkerheten og personvernet i sektoren.

Du kan kontakte Sikt for å få tilsendt vår vurdering i sin helhet.

Deling av opplysninger med tredjeparter

Opplysningene deles ikke med andre enn Sikt, institusjonen din og leverandørene under. Leverandørene har avtale med Sikt eller med vår leverandør og kan bare bruke opplysningene til å levere tjenesten.

Dersom du allerede har en identitet ved en annen institusjon, får den nye institusjonen bare vite din UHID og UH-brukernavn. Andre opplysninger deles ikke mellom institusjonene, heller ikke hvilken annen institusjon du er tilknyttet.

Leverandør	**Hva de gjør**	**Hvor**	**Grunnlag for overføring**
Identity Automation (JAMF)	Leverer og drifter kjernen i tjenesten (RapidIdentity)	Lagring i AWS i Stockholm. Leverandøren har tilgang fra USA for drift og support	EUs standardavtaler (SCC)
Amazon Web Services Inc (AWS)	Datasenter for RapidIdentity	Datasenter for hosting av RapidIdentity ligger i Stockholm.	Lagring i EØS. For eventuell tilgang fra tredjeland ved support: EUs standardavtaler eller EU-USA Data Privacy Framework

Om tilgang fra USA

Identity Automation er et amerikansk selskap og har teknisk tilgang fra USA for å drifte løsningen. Slik tilgang regnes som en overføring av personopplysninger til et land utenfor EU/EØS. Overføringen skjer med grunnlag i EUs standardavtaler (SCC). Du kan be om en kopi av standardavtalene.

Både Identity Automation (JAMF) og AWS er underlagt amerikansk lov, og amerikanske myndigheter kan i visse tilfeller kreve opplysninger overlevert. Sikt har vurdert denne muligheten for utlevering i en egen overføringsvurdering, og kommet til at overføringen er lovlig.

Hvor lenge opplysningene lagres

Når tilknytningen din til institusjonen opphører, mister du tilgangene og kontoen deaktiveres etter en kort overgangsperiode som institusjonen bestemmer. Opplysningene i Felles IAM slettes deretter etter institusjonens frist. Kontakt institusjonen for nøyaktig frist.

Opplysning	Lagringstid
Opplysningene som brukes til matchingen	Slettes når institusjonen sletter personoppføringen din i Felles IAM, etter institusjonens frist
UHID og UH-brukernavn	Så lenge Felles IAM leveres, slik at de aldri gis til en annen person. Lagringen vurderes på nytt minst hvert femte år
Sikkerhetskopier	Daglige kopier i 35 dager og månedlige i 365 dager. Slettede opplysninger kan derfor finnes i sikkerhetskopier i inntil ett år.

Sikkerhetstiltak

Vi bruker tekniske og organisatoriske tiltak for å beskytte opplysningene dine inkludert:

- Kryptering av all trafikk til og fra tjenesten
- Kryptering av lagrede data i ro (encryption at rest)
- Administratorer og brukere må bruke tofaktorautentisering
- Hver institusjon ser bare opplysninger om egne brukere; bare Sikt og Identity Automation har tilgang på tvers av institusjonene (for drift og support).
- Leverandøren er uavhengig revidert (SOC 2 Type II), og Sikt har rett til å kontrollere at avtalene følges

Dine rettigheter

Etter personopplysningsloven og personvernforordningen (GDPR) har du blant annet disse rettighetene:

- **Innsyn:** Du kan få vite hvilke opplysninger vi har om deg, og få en kopi av dem.
- **Retting:** Du kan kreve at uriktige opplysninger om deg rettes. De fleste opplysningene kommer fra kildesystemer, for eksempel FS eller personalsystem, og må rettes der. Vi anbefaler at du tar kontakt med institusjonen din, så oppdateres opplysningene automatisk i Felles IAM.
- **Sletting:** Du kan kreve at opplysningene dine slettes når de ikke lenger er nødvendige, når en protest har ført frem, eller når behandlingen er ulovlig. UHID og UH-brukernavn blir normalt ikke slettet, fordi de må beholdes for å hindre gjenbruk. Du kan likevel be om sletting eller protestere (se «Protest» under), og vi vurderer da saken din konkret.
- **Begrensning:** Du kan kreve at behandlingen begrenses mens vi vurderer et krav om retting eller en protest. Hvis tilgangen din ikke kan opprettholdes uten de omstridte opplysningene, kan det bety at den stenges midlertidig, med mindre du samtykker til at vi bruker dem i perioden.
- **Protest:** Siden behandlingen bygger på berettiget interesse, kan du protestere hvis du har grunner knyttet til din særlige situasjon. Vi vurderer protesten, og kan bare fortsette behandlingen dersom vi kan påvise tvingende berettigede grunner som går foran dine interesser, rettigheter og friheter, eller hvis behandlingen er nødvendig for å fastsette, gjøre gjeldende eller forsvare rettskrav.

- **Klage:** Du kan klage til Datatilsynet hvis du mener vi behandler personopplysninger i strid med regelverket.

Hvis du har spørsmål eller ønsker å utøve dine rettigheter, finner du våre kontaktopplysninger nedenfor.

Spørsmål og klage

Vi oppfordrer deg til å kontakte oss hvis du har spørsmål, bekymringer eller klager angående vår behandling av dine personopplysninger. Du kan kontakte oss på kontakt@sikt.no eller kontakte vårt personvernombud direkte:

Marita Ådnanes Helleland
Postadresse: Professor Brochs gate 8A, NO-7030 Trondheim
Telefon: 73 98 40 40
E-post: **personvernombud@sikt.no** NB: E-posten er ikke sikker! Vennligst ikke send sensitive opplysninger.

For spørsmål om brukerkontoen din og tilgangene dine må du kontakte institusjonen du er tilknyttet.

Endringer

Erklæringen ble sist oppdatert 12.11.26. Vi oppdaterer den hvis det skjer endringer i tjenesten eller vår behandling av dine personopplysninger.