Delstrategi for personvernhåndtering

Dokumentinformasjon

Strategien omfatter:	Rammer og prinsipper for hvordan StInn kan ivareta personvernloven og GDPR ved behandling av persondata
Målgruppe:	Alle tillitsvalgte som behandler persondata
Mål i styrende dokumenter:	OM10
Tilknyttet:	*Prinsipper for internkontroll i StInn, Databehandleravtale mellom HINN og StInn*
Dokumenteier/godkjent av:	Sentralstyret/OU-arbeidsgruppa

Dokumenthistorikk

Versjonsnr:	Forfatter:	Dato:	Kommentar:	Godkjent av:
1	OU-arbeidsgruppa	01.07.2022		OU-arbeidsgruppa
2				
3				

1 Formål med delstrategien

Ved behandling av persondata er man pliktig til å følge personopplysningsloven (GDPR). Denne delstrategien tar for seg hvilke prinsipper som skal følges i StInn for at man i større grad skal ivareta kravene loven setter.

2 Definisjoner

«Personopplysninger» defineres slik loven definerer det. Per dags dato definerer loven dette som «opplysninger og vurderinger som kan knyttes til en enkeltperson» (Personopplysningsloven § 2 første punkt).

På samme måte defineres «behandling av personopplysninger» på samme måte som loven, per i dag «enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter…» (Personopplysningsloven § 2 andre punkt).

Personopplysninger deles videre inn i tre underkategorier:

- Generelle personopplysninger
- Sensitive personopplysninger
- Andre personopplysninger

Som generelle personopplysninger regnes:

- Navn
- Studiested
- Studieprogram, fakultetstilhørighet osv
- Alder
- Kjønn

«Sensitive personopplysninger» defineres slik av loven:

«…opplysninger om

a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,
b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,
c) helseforhold,
d) seksuelle forhold,
e) medlemskap i fagforeninger.»

«Andre personopplysninger» er de personopplysningene som ikke er gener elle eller sensitive.

3 Overordnede prinsipper

Den enkelte tillitsvalgt som behandler personopplysninger, er ansvarlig for at personopplysningene behandles i henhold til loven. Sentralstyret og organisasjonskonsulentene kan vedta og implementere rutiner for organisasjonen, som i nærmere detalj regulerer hvordan slike opplysninger skal behandles.

«Behandlingsansvarlig» av personopplysninger som behandles i StInn er Sentralstyret.
«Databehandler» er den enkelte tillitsvalgte eller ansatte som faktisk behandler opplysningene.

Det skal aldri under noen omstendigheter innhentes eller registreres informasjon som direkte eller indirekte kan regnes som sensitive personopplysninger uten at det foreligger godkjennelse fra Sentralstyret. Sentralstyret skal rådføre seg med organisasjonskonsulent før godkjennelse gis. Unntak gjelder ved matallergier (se kapittel 7).

4 Gradering av informasjon og tilgangsbegrensninger

Informasjonen deles inn i fem kategorier:

Grønn	Åpen	Informasjon som kan eller skal være tilgjengelig for alle uten særskilte tilgangsrettigheter.
Gul	Begrenset	Dette er i utgangspunktet informasjon som ikke er åpen for alle. I lover eller annet regelverk er det ingen krav om at informasjonen skal være åpen. Dette er altså all informasjon som ikke er klassifisert som åpen, fortrolig, eller strengt fortrolig. Informasjonen må ha en viss beskyttelse og kan være tilgjengelig for både eksterne og interne, med kontrollerte tilgangsrettigheter. Denne klassen benyttes dersom det vil kunne forårsake en viss skade for institusjonen, eller samarbeidspartner hvis informasjonen blir kjent for uvedkommende. Informasjonen har kun relevans for eller er innrettet mot en begrenset brukergruppe enten ved høgskolen eller ved institusjoner og organisasjoner høgskolen har samarbeid med.
Rød	Fortrolig	Dette er informasjon som man er pålagt å begrense tilgangen til i lov, forskrift, avtaler, reglementer og annet regelverk. Dette tilsvarer graden «fortrolig» i den offentlige Beskyttelsesinstruksen. «Fortrolig» benyttes hvis det vil forårsake skade for offentlige interesser, StInn, enkeltperson eller samarbeidspartner hvis informasjonen blir kjent for uvedkommende.

Sort	Strengt fortrolig	Denne kategorien omfatter samme type informasjon som Fortrolig (rød), men der spesielle hensyn gjør at man ønsker å beskytte dataene ytterligere. Pålegg om beskyttelse og sikring utover de lovbestemte skal være nedfelt i avtaler eller skriftlig dokumentert på annen måte. Dette tilsvarer graden «strengt fortrolig» i den offentlige Beskyttelsesinstruksen. «Strengt fortrolig» benyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, høgskolen, enkeltperson eller samarbeidspartner at informasjonen blir kjent for uvedkommende.

I de tilfeller der sensitive personopplysninger samles inn skal dette kategoriseres som sort. Se også §§ 4-2 og 4-3 i *Prinsipper for internkontroll i StInn*.

5 Plattformer personopplysninger kan behandles og registreres i

Sensitive personopplysninger skal kun innhentes gjennom Nettskjema. Slike opplysninger kan kun oppbevares i Nettskjema når de ikke er anonymiserte (dette inkludere at man ikke kan ha slike opplysninger på egen harddisk, selv om den ikke er synkronisert mot internett).

Personopplysninger som innhentes skal som hovedregel registreres i Rubic. Personopplysninger kan også forekomme i OTRS, OpaVote, GoPlenum, MS Teams eller andre lignende systemer StInn bruker som en del av saksbehandlingen. Organisasjonskonsulentene definerer videre hvilke IT-systemer StInn benytter.

Tillitsvalgte i StInn må forvente at generelle personopplysninger om dem kan gjøres offentlig. Tillitsvalgte i StInn må også forvente at de politiske holdninger og verdier som de uttrykker blir offentliggjort gjennom protokoll, artikler, nyhetsbrev osv.

Personopplysninger som ikke regnes som generelle skal ikke lagres/oppbevares i systemer, nettsider eller lignende som ikke organisasjonskonsulentene har godkjent.

Når informasjon innhentes, skal kun Nettskjema benyttes med mindre organisasjonskonsulentene har godkjent en annen metode.

6 Deling av personopplysninger

Personopplysninger kan deles med HINN, SINN eller andre samarbeidspartnere i de tilfeller hvor formålet er at partnerne kan komme i kontakt med tillitsvalgte i StInn.

7 Matallergier

Det kan som unntak til hovedregelen i kapittel 3 samles inn helseopplysninger uten godkjennelse fra Sentralstyret hvis helseopplysningene som samles inn er matallergier, og formålet er at deltagere ved felles bespisning skal få tilpasset mat. I disse tilfellene skal ikke opplysningene lagres lenger enn maksimum to dager etter at måltidet er gjennomført. Informasjonen skal så langt det lar seg gjøre

ikke deles med flere enn de som er involvert i serveringen av mat. Når opplysninger om allergier deles med restaurant, kantine etc. skal navn utelates.

Når det er behov for å innhente matallergier skal dette som hovedregel samles inn for hvert måltid, men man kan samle inn for alle måltider som finner sted under et arrangement, seminar eller lignende.