Retningslinje for

Personvern

Vedtatt av landsstyret 02.06.2018
Endret av landsstyret 06.06.2020, 05.06.2021

1. Formål

Denne retningslinjen skal sørge for god håndtering av personopplysninger i Natur og Ungdom, og at Natur og Ungdom oppfyller lovkrav om personvern.

2. Gyldighet

2.1. Disse retningslinjene gjelder for alle personopplysninger som behandles av Natur og Ungdom sentralt, i fylkeslagene og i lokallagene.

2.2. Personopplysninger er opplysninger som kan knyttes til en enkeltperson. Det kan for eksempel være navn, adresse, telefonnummer, IP-adresse og bilder. Matpreferanser og allergier er også personopplysninger.

2.3. Sensitive personopplysninger er opplysninger om etnisk bakgrunn, politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, allergier, seksuell legning eller medlemskap i fagforening

3. Prinsipper

3.1. Alle ansatte, sentralstyremedlemmer, fylkesledere og landsstyremedlemmer må kjenne til retningslinjene for personvern.

3.2. NU må få samtykke fra alle vi samler inn personopplysninger fra. Opplysningene kan ikke brukes til andre formål enn det som spesifiseres i samtykket, og hvert formål skal godkjennes for seg. Det skal komme tydelig fram hvordan opplysningene behandles, hvorfor og hvor lenge.

3.3. Innhenting og oppbevaring av personopplysninger må ha hensikt og kunne begrunnes. Vi innhenter og oppbevarer kun det vi trenger. Annet skal slettes.

3.4. Tilgang til personopplysninger skal kun gis til ansatte og tillitsvalgte som trenger det.

3.5. Personer vi har oppbevart personopplysninger om har rett til å bli glemt. Vi skal derfor ha muligheten til å slette alle personopplysninger om personer i organisasjonen, også bilder.

3.6. Natur og Ungdom sentralt skal konkretisere retningslinjene i tydelige og grundige rutiner for håndtering av personopplysninger. Det skal kunne dokumenteres at rutinene følges.

4. Informasjon

4.1. Ved innmelding i NU, som medlem eller NU-venn, skal det gis god informasjon om NUs rutiner for håndtering av personopplysninger på

innmeldingsskjemaet. Den som melder seg inn må akseptere disse. Det samme gjelder ved opprettelse av Putsj-abonnementer. Rutinene skal ligge lett tilgjengelige på nettsida.

4.2. Ved påmelding til sentrale og regionale arrangementer skal deltakeren akseptere en personvernerklæring for å melde seg på.

5. Oppbevaring og bruk av personopplysninger

5.1. Personopplysninger hentet inn i forbindelse med NU-seminar må håndteres forsiktig. Etter endt seminar må opplysningene fjernes fra internettlagring, og overflødig informasjon må slettes helt. Vi kan lagre den mest nødvendige informasjonen i låste mapper på serveren til Natur og Ungdom sentralt så lenge vi trenger dette til søknader om pengestøtte. Om man vil bruke e-postadresse eller telefonnummer til å informere om annet som skjer må man få bekreftelse fra deltakeren på at dette er i orden.

5.2. Sentralt ansatte og tillitsvalgte som håndterer personopplysninger må signere en taushetserklæring om dette.

5.3. Opplysninger i fysisk format, som registreringsskjemaer, ringelister, personaldokumenter og verveslipper, oppbevares i låsbare skap.

6. Bilder

6.1. Dersom bilder av en seminardeltaker skal publiseres i NUs kanaler eller oppbevares skal deltakeren ha gitt aktivt samtykke til dette i påmelding til seminaret.

6.2. Navn på identifiserbare avbildede personer blir lagret sammen med bildene både online og offline. Dette for å kunne fjerne alle bilder av bestemte personer ved forespørsel.

6.3. Unntak kan gjelde på offentlige steder, i demonstrasjoner og lignende. Hvis du er usikker, be om samtykke.

7. Avvik

7.1. Personopplysninger på avveie[1], eller andre brudd med våre rutiner og retningslinjer, skal meldes til Datatilsynet innen 72 timer. Den som oppdager slike feil melder fra til daglig leder. Daglig leder har ansvar for avviksmelding.

[1] Eksempler på avvik er:
- Mistede deltakerlister eller ringelister
- Mistet/stjålet PC, minnepenn eller mobiltelefon med opplysninger på
- E-post/brev sendt til feil mottaker
- E-post/brev eller publisering som inneholder feil eller for mye opplysninger
- Feil i tilgangsstyring på dokumenter
- Datainnbrudd eller fysisk innbrudd.