RUTINER
Oslo, 26. februar 2019
Arkivnummer: 070/2018/GDPR/S

Personvernrutiner i LNU

Internkontroll: Personopplysninger og informasjonssikkerhet

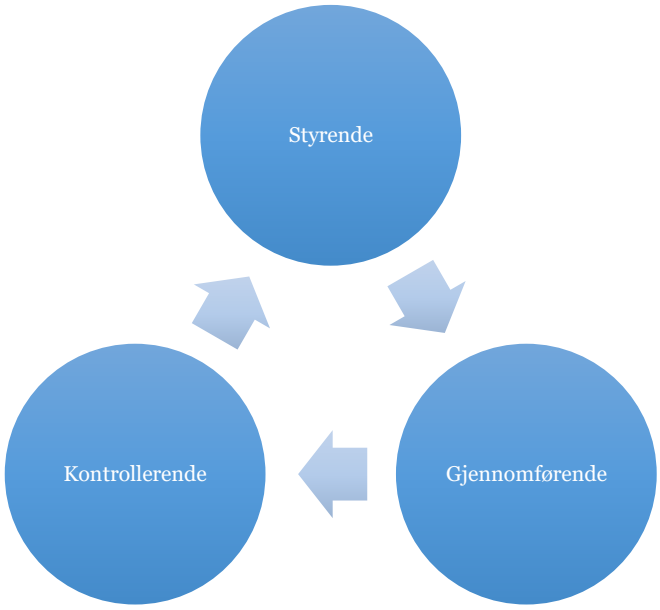
Innledning

Personopplysningsloven § 14 fastsetter følgende om internkontroll:

> *"Den behandlingsansvarlige skal etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet.*
>
> *Den behandlingsansvarlige skal dokumentere tiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda.*
>
> *Kongen kan gi forskrift med nærmere regler om internkontroll."*

LNUs løsning for å ivareta vårt ansvar etter personopplysningsloven er utfyllende beskrevet i dette dokumentet.

Løsningen er i hovedsak bygd opp etter Datatilsynets veileder, og består av følgende tre deler:



Styrende elementer, som i hovedsak retter seg mot ledelsen og hvilke beslutninger og føringer som legges for internkontroll. Disse beslutningene må ha allmenn tilslutning dersom systemet skal ha tilstrekkelig legitimitet.

Gjennomførende elementer, som i hovedsak retter seg mot ansatte. Her finner man beskrivelse av rutiner som det forutsettes at ansatte er kjent med og arbeider i samsvar med.

Kontrollerende elementer, som bidrar til å fange opp avvik fra systemet og til at det gjennomføres periodiske gjennomganger.

Beskrivelsene gjelder krav og plikter som LNU blir underlagt på grunn av personopplysninger, og eventuelle krav og plikter gjennom andre lover og forskrifter.

Styringsdokumenter og underliggende dokumenter er vedtatt av generalsekretær 03.09.2018, og forutsettes fulgt opp av alle som behandler fortrolig informasjon.

1. Styrende dokumentasjon

Personopplysningsloven stiller, som beskrevet innledningsvis, krav til internkontroll gjennom etablering og vedlikehold av systematiske tiltak. Tiltakene skal medvirke til at krav i lov og forskrift overholdes, og at vi dermed sikrer personopplysningenes kvalitet. Dette beskrives som:

- Rutiner for oppfyllelse av LNUs plikter, og dermed de registrertes rettigheter
- Rutiner og tekniske tiltak for informasjonssikkerhet

LNU behandler personopplysninger for å administrere forholdet til ansatte, tillitsvalgte, søkere på støtteordninger og brukere (les: deltagere på arrangementer, mottagere av nyhetsbrev, m.m.). Generalsekretær er *behandlingsansvarlig* og ansvarlig for at behandlingen av personopplysninger foregår etter personopplysningslovens krav og bestemmelser.

LNU behandler opplysninger om ansatte med hjemmel (behandlingsgrunnlag) i personopplysningslovens:

- Personopplysningslovens § 8 ved at det er fastsatt i lov.
- Personopplysningslovens § 8 ved at det innhentes samtykke fra den ansatte.
- Personopplysningslovens § 8 a) for å oppfylle avtale med den registrerte.
- Personopplysningslovens § 8 b) for å ivareta en rettslig forpliktelse.
- Personopplysningslovens § 8 f) for å ivareta tungtveiende interesser.
- Personopplysningslovens § 8 f) for å ivareta arbeidsrettslige plikter og rettigheter.

LNU behandler opplysninger om brukere med hjemmel i personopplysningslovens:

- § 8 a) for å oppfylle avtale med den registrerte (nødvendig administrasjon av forholdet).
- § 8 ved at det innhentes samtykke (utover det som dekkes av forrige punkt).
- § 8 ved at det er fastsatt i lov (regnskapsopplysninger).

Opplysninger om ansatte og (lønnede) tillitsvalgte håndteres i lønns- og personalsystemet Visma Business. Opplysningene om søkere på støtteordninger håndteres i LNUs søknadsportal. Opplysninger om brukere håndteres i SurveyMonkey, Mailchimp, Wufoo, Facebook og Google Analytics. Den daglige håndteringen av opplysninger om ansatte og lønnede tillitsvalgte utføres av assisterende generalsekretær, mens opplysninger om søkere på støtteordninger utføres av avdelingsleder for forvaltning. Informasjonsrådgiver sørger for at håndtering av opplysninger om brukere er i tråd med rutinene i dette dokumentet.

LNU skal kun behandle nødvendige opplysninger om ansatte, tillitsvalgte, søkere på støtteordninger og brukere. De som registreres hos oss skal alltid være klar over at det blir gjort, og om nødvendig skal vi be om samtykke for dette. Alle ansatte i LNU skal vite hvordan personopplysningene skal håndteres, og om nødvendig kan de søke hjelp hos sin nærmeste leder. LNU skal alltid kunne svare på spørsmål, både fra publikum og de som er registrert, om behandlingene av personopplysninger.

1.1 Sikkerhetsmål

Personopplysninger om ansatte, tillitsvalgte, søkere og brukere skal

- kun være tilgjengelige for ansatte som har behov for disse opplysningene i sitt arbeid
- være oppdatert i henhold til behov.

Personopplysninger må ikke komme på avveie, og LNU skal sørge for at det etableres rutiner for å minimere risiko for dette.

Personopplysningene skal sikres med hensyn til *konfidensialitet* (uvedkommende får ikke tilgang til opplysninger), *integritet* (opplysninger endres ikke uautorisert eller utilsiktet) og *tilgjengelighet* (opplysningene er tilgjengelige når det er nødvendig). Eksempler på hendelser vi ønsker å beskytte oss mot:

- Felles hendelser for brudd på konfidensialitet, integritet og tilgjengelighet:
  - innbrudd i LNUs lokaler eller nettverk
  - uvedkommendes bruk av ansattes brukerkontoer tilknyttet LNUs nettverk
  - angrep fra virus eller andre ondsinnede program
- Brudd på konfidensialitet (personopplysninger kommer på avveie):
  - tap av bærbart utstyr
  - tap av lagringsmedium
  - utskrift liggende på skriver
  - utilsiktet utlevering av ansattopplysninger via e-post
- Brudd på integritet (personopplysninger blir endret):
  - ulike versjoner av dokumenter
  - feilregistrering
- Brudd på tilgjengelighet (personopplysninger er utilgjengelige):
  - nettverk eller system ute av drift
  - brann, vannskade og strømsvikt
  - hærverk

1.2 Sikkerhetsstrategier

- Assisterende generalsekretær er sikkerhetsansvarlig i LNU
- Uvedkommende skal ikke kunne få fysisk tilgang til personopplysninger, enten disse er elektronisk lagret eller i papirversjon
- Tilgangskontroll skal sikre at tilgang til opplysninger om ansatte, tillitsvalgte, søkere og brukere skal begrenses til de som har behov for det
- LNUs elektroniske fellesarkiv og nettbaserte løsninger skal beskyttes mot uvedkommendes bruk, eksempelvis ved sikring av trådløst nettverk.

Se *Vedlegg 2 – Sikkerhetsinstruks for ansatte og tillitsvalgte* for mer inngående om sikkerhetstiltak i LNU og dokumentet *Personalarkiv* i PA\204.0 for beskrivelse av ekstra beskyttelsestiltak for personaldokumenter.

1.3 Organisering

Sikkerhetsansvarlig skal vedlikeholde en oversikt over behandlinger av personopplysninger med formål og behandlingsgrunnlag, og skal sørge for at LNU har de nødvendige rutiner for å gjøre behandlingen forsvarlig.

Sikkerhetsansvarlig skal en gang i året foreta en gjennomgang av internkontroll og informasjonssikkerhet.

Informasjonsrådgiver er ansvarlig for IT-infrastruktur og informasjonssystemene LNU benytter. Informasjonsrådgiver skal sørge for at IT-infrastruktur og informasjonssystemene ivaretar krav til sikkerhet basert på vedtatte rutiner og tekniske sikkerhetstiltak. Dette omfatter tiltak som:

- Sikre IKT-utstyr mot tyveri, hærverk, brann og strømutfall
- Holde oversikt over virksomhetens IT-utstyr
- Sikre at IT-utstyr kan behandle personopplysninger i henhold til dette rutinedokumentet
- Sørge for sikkerhetskopiering og sikker lagring av kopier

1.4 Andre parter

Parter som behandler personopplysninger på vegne av LNU er *databehandlere*. Behandlingsansvarlig skal inngå avtale med databehandlere. Avtalen skal regulere hvordan databehandleren skal håndtere og sikre personopplysningene.

- Amesto Accounting er databehandler for LNUs regnskapssystem. Avtalen ble signert 3. juni 2018 og er arkivert med referansenummer FA\160.
- Google er databehandler for all informasjon tilgjengeliggjort i LNUs e-postsystem (gjennom Gmail), skylagring (gjennom Google Disk), og andre tjenester tilknyttet G Suite. Forholdet er regulert gjennom G Suite Data Processing Amendment (versjon 2.0).
- SurveyMonkey er databehandler for respondentbesvarelser i spørreundersøkelser og påmeldingsskjemaer (Wufoo). Forholdet er regulert gjennom SurveyMonkeys personvernpolicy.
- Mailchimp er databehandler for kontaktinformasjon om abonnenter til LNUs nyhetsbrev. Forholdet er regulert i Mailchimps personvernpolicy.
- Backblaze er databehandler for sikkerhetskopien av LNUs fellesserver. Forholdet er regulert gjennom et Data Processing Addendum.
- Redpill Linpro er databehandler for informasjon om søkere i LNUs søknadssystem. Avtalen er signert den 17. desember 2012 og er arkivert med referansenummer FA\073.3.
- Frivillighetshuset/Unicornis (databehandleravtale er ikke inngått pr. juni 2018)

Parter som har tilgang til LNUs informasjonssystemer, skal signere taushetserklæring. Generalsekretær (behandlingsansvarlig) eller assisterende generalsekretær (sikkerhetsansvarlig) skal avtale forholdet med slike parter.

2 Gjennomførende dokumentasjon

2.1 Håndtering av personopplysninger

Ny behandling av personopplysninger

Ved oppstart av *ny behandling* av personopplysninger, skal assisterende generalsekretær (sikkerhetsansvarlig) bekrefte at det foreligger gyldig behandlingsgrunnlag. Ved nye behandlinger skal det vurderes behov for endring av internkontrollen.

Sletting av personopplysninger

Personopplysninger skal slettes når det ikke lenger er saklig behov for å oppbevare dem. Sikkerhetsansvarlig er ansvarlig for sletting dersom dette gjelder forhold knyttet til LNU som organisasjon.

Rutine for sletting:

1) Assisterende generalsekretær er ansvarlig for personopplysninger om ansatte i LNU. Assisterende generalsekretær skal:

- slette/makulere unødvendige opplysninger ved avslutning av arbeidsforholdet
- gjennomføre ny vurdering av behov for fortsatt lagring et år etter avslutning av arbeidsforholdet
- påse at det ikke lagres personopplysninger om ansatte som ikke er relevante for administrasjon av arbeidsforholdet

Rutinen gjelder ikke opplysninger i LNUs regnskap. Disse gjennomgås når oppbevaringsplikten utløper.

2) Assisterende generalsekretær er ansvarlig for personopplysninger om tillitsvalgte i LNU. Assisterende generalsekretær skal:

- slette/makulere unødvendige opplysninger når valgperioden til den tillitsvalgte er over
- påse at det ikke lagres personopplysninger om tillitsvalgte som ikke er relevante for administrasjon av tillitsvalgtforholdet

Rutinen gjelder ikke opplysninger i LNUs regnskap. Disse gjennomgås når oppbevaringsplikten utløper.

3) Informasjonsrådgiver er ansvarlig for LNUs bildearkiv. Informasjonsrådgiver skal:

- sørge for at bilder hvor enkeltpersoner som ikke er eller har vært ansatte eller tillitsvalgte i LNU utgjør hovedmotiv slettes innen fem år, med mindre oppdatert, skriftlig samtykke foreligger

4) Informasjonsrådgiver er ansvarlig for personopplysninger om brukere. Informasjonsrådgiver skal:

- sørge for at personopplysninger om brukere av LNUs tjenester slettes eller anonymiseres innen tidsfristen spesifisert i rutinedokumentet (referanse). Dette gjelder med mindre utvidet lagring er hjemlet i loven.

- påse at det ikke lagres flere personopplysninger om brukere enn nødvendig for formålet

5) Avdelingsleder for forvaltning er ansvarlig for personopplysninger om søkere på LNUs støtteordninger. Avdelingsleder for forvaltning skal:

- sørge for at personopplysninger om søkere slettes eller anonymiseres etter 3 års inaktivitet. Dette gjelder med mindre utvidet lagring er hjemlet i loven, eller hvis skriftlig samtykke til fortsatt lagring er innhentet fra søker
- påse at det ikke lagres flere personopplysninger om søker enn nødvendig for formålet

Rutinen gjelder ikke opplysninger i LNUs regnskap. Disse gjennomgås når oppbevaringsplikten utløper.

Rutine for utlevering av personopplysninger til andre

Utlevering betyr at personopplysninger overlates til annen behandlingsansvarlig. Dette er en ny behandling, og det kreves et eget behandlingsgrunnlag. Dersom ikke annet behandlingsgrunnlag finnes, må det innhentes samtykke fra den registrerte.

Utlevering av personopplysninger til tredjepart skal godkjennes av generalsekretær (behandlingsansvarlig). Selve utleveringsoppgaven gjennomføres av assisterende generalsekretær eller informasjonsrådgiver.

Sikring av kvalitet av personopplysninger

Generalsekretær er behandlingsansvarlig og har overordnet ansvar for at opplysningene er så korrekte og oppdaterte som mulig, med tanke på formålet med behandlingen. Avdelingslederne er ansvarlige for at personalopplysninger bekreftes korrekte av den ansatte årlig, i forbindelse med medarbeidersamtale. Avdelingsleder for forvaltning og informasjonsrådgiver er ansvarlig for at opplysninger om henholdsvis søkere og brukere er korrekte.

2.2 Rutiner – registrert person

Innhenting av samtykke

LNU skal kun behandle personopplysninger når organisasjonen har innhentet gyldig samtykke fra personen eller personene personopplysningen(e) gjelder. For at et samtykke skal være gyldig må det være

- frivillig
- spesifikt
- informert
- utvetydig
- gitt gjennom en aktiv handling
- dokumenterbart
- mulig å trekke tilbake like lett som det ble gitt.

Utfyllende informasjon om hva disse kriteriene innebærer finnes på Datatilsynets nettsider om behandlingsgrunnlag.

Oppfyllelse av informasjonsplikt

Søkere til stillinger i LNU orienteres under tilsettingsprosessen om våre retningslinjer, og om hvilke opplysninger som lagres under arbeidsforholdet, innsynsrett og rett til å få korrigert lagret informasjon. Tillitsvalgte, søkere på støtteordninger og brukere som blir bedt om å oppgi personopplysninger informeres om LNUs retningslinjer for lagring av dette, og har mulighet til å reservere seg mot slik lagring etter at oppgjør er gjennomført.

Innsyn

Henvendelser om innsyn skal formidles til sikkerhetsansvarlig (les: assisterende generalsekretær) som er ansvarlig for at henvendelser besvares uten ugrunnet opphold.

Rett til innsyn i personopplysninger er beskrevet i personopplysningsloven § 18:

> *"Enhver som ber om det, skal få vite hva slags behandling av personopplysninger en behandlingsansvarlig foretar, og kan kreve å få følgende informasjon om en bestemt type behandling:*
>
> *a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,*
>
> *b) hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter,*
>
> *c) formålet med behandlingen,*
>
> *d) beskrivelser av hvilke typer personopplysninger som behandles,*
>
> *e) hvor opplysningene er hentet fra, og*
>
> *f) om personopplysningene vil bli utlevert, og eventuelt hvem som er mottaker.*
>
> *Dersom den som ber om innsyn er registrert, skal den behandlingsansvarlige opplyse om*
>
> *a) hvilke opplysninger om den registrerte som behandles, og*
>
> *b) sikkerhetstiltakene ved behandlingen så langt innsyn ikke svekker sikkerheten.*
>
> *Den registrerte kan kreve at den behandlingsansvarlige utdyper informasjonen i første ledd bokstav a - f i den grad dette er nødvendig for at den registrerte skal kunne vareta egne interesser.*
>
> *Retten til informasjon etter annet og tredje ledd gjelder ikke dersom personopplysningene behandles utelukkende for historiske, statistiske eller vitenskapelige formål og behandlingen ikke får noen direkte betydning for den registrerte."*

LNU har og plikt til å informere når det samles inn opplysninger fra den registrerte. Dette er beskrevet i personopplysningsloven § 19:

> *"Når det samles inn personopplysninger fra den registrerte selv, skal den behandlingsansvarlige av eget tiltak først informere den registrerte om*
>
> *a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,*
>
> *b) formålet med behandlingen,*
>
> *c) opplysningene vil bli utlevert, og eventuelt hvem som er mottaker,*

d) det er frivillig å gi fra seg opplysningene, og

e) annet som gjør den registrerte i stand til å bruke sine rettigheter etter loven her på best mulig måte, som f.eks. informasjon om retten til å kreve innsyn, jf. § 18, og retten til å kreve retting, jf. § 27 og § 28.

Varsling er ikke påkrevd dersom det er på det rene at den registrerte allerede kjenner til informasjonen i første ledd."

Plikt til å informere når det samles inn opplysninger fra andre enn den registrerte, er beskrevet i personopplysningsloven § 20:

"En behandlingsansvarlig som samler inn personopplysninger fra andre enn den registrerte selv, skal av eget tiltak informere den registrerte om hvilke opplysninger som samles inn og gi informasjon som nevnt i § 19 første ledd så snart opplysningene er innhentet. Dersom formålet med innsamling av opplysningene er å gi dem videre til andre, kan den behandlingsansvarlige vente med å varsle den registrerte til utleveringen skjer.

Den registrerte har ikke krav på varsel etter første ledd dersom

a) innsamlingen eller formidlingen av opplysningene er uttrykkelig fastsatt i lov,

b) varsling er umulig eller uforholdsmessig vanskelig, eller

c) det er på det rene at den registrerte allerede kjenner til informasjonen varselet skal inneholde.

Når varsling unnlates med hjemmel i bokstav b, skal informasjonen likevel gis senest når det gjøres en henvendelse til den registrerte på grunnlag av opplysningene."

Innsyn i private e-poster og private filområder

Det vises til *Vedlegg 2 Sikkerhetsinstruks for ansatte og tillitsvalgte,* om den ansattes plikter i forbindelse med bruk av LNUs e-postsystem.

Arbeidsgiver skal som hovedregel ikke ha adgang til ansattes personlige e-postkasser. Arbeidsgiver kan likevel lese ansattes e-post når det enten er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten, eller ved begrunnet mistanke om at arbeidstakers bruk av e-postkassen medfører grovt brudd på de plikter som følger av arbeidsforholdet, eller kan gi grunnlag for oppsigelse eller avskjed.

Ved innsyn skal det så langt som mulig sendes varsel om innsyn til arbeidstakeren. Varselet skal inneholde en begrunnelse for hvorfor vilkårene anses oppfylt, og informasjon om arbeidstakerens rettigheter.

Ved innsyn skal verneombud eller tillitsvalgt være tilstede og helst også den ansatte. Privat e-post kan lagres i mapper kalt «privat». Slike mapper vil ikke bli rørt av LNU ved behov for innsyn av hensyn til den daglige driften. Innsynet skal loggføres i samarbeid av tillitsvalgt (eventuelt verneombud dersom den ansatte ikke har en tillitsvalgt) og nærmeste leder for den ansatte.

2.3 Informasjonssikkerhet

Tilgang til sikkerhetsdokumentasjon skal begrenses til de som har behov for det. Sikkerhetsdokumentasjon er derfor ført i vedlegg som ikke gis ut til enhver ansatt:

- Ansatte og tillitsvalgte i LNU benytter informasjonssystemet slik det fremgår av *Vedlegg 2 Sikkerhetsinstruks for ansatte og tillitsvalgte*
- Assisterende generalsekretær, som er sikkerhetsansvarlig i LNU, har gjennomført risikovurdering av informasjonssystemet og dokumentert denne i *Vedlegg 7 Risikovurdering*. Tilgang til vedlegget begrenses.

3 Kontrollerende dokumentasjon

Håndtering av uønskede hendelser

Ansatte som oppdager uønskede hendelser skal snarest rapportere om dette til nærmeste leder. Ledere som oppdager uønskede hendelser eller blir informert av underordnede, skal snarest rapportere dette til sikkerhetsansvarlig.

Meldinger om uønskede hendelser skal gjennomgås i fellesskap av LNUs ledergruppe, som består av generalsekretær, assisterende generalsekretær og de to avdelingslederne. Møtet skal konkludere om det skal gjennomføres tiltak for å hindre gjentakelse.

Avvikshåndtering

Ansatte som oppdager avvik fra rutiner, skal rapportere om dette i avviksskjema som sendes til sikkerhetsansvarlig, jf. *Vedlegg 6 Avviksskjema*. Avvik skal behandles på samme måte som uønskede hendelser.

Ledelsens gjennomgang

Ledelsen skal årlig gjennomgå sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssystemene. Ledelsen skal kontrollere at disse er i samsvar med virksomhetens behov og eventuelt oppdatere mål, strategi og organisering.

Ved ledelsens gjennomgang deltar generalsekretær, assisterende generalsekretær og de to avdelingslederne. Sikkerhetsansvarlig (assisterende generalsekretær) har ansvar for å utarbeide rapport fra gjennomgangen med aktuelle tiltak.

4 Vedlegg

Vedlegg 1 Definisjoner

Behandlingsansvarlig: Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Generalsekretær er behandlingsansvarlig i LNU.

Behandling av personopplysninger: Enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksområder (se personopplysningsloven § 2–2).

Beskyttelsesverdig informasjon: Informasjon som inneholder personopplysninger eller andre konfidensielle opplysninger.

Databehandler: Den som behandler personopplysninger på vegne av den behandlingsansvarlige (se personopplysningsloven § 2–5).

Informasjonssikkerhet: Personopplysningsloven, §13, stiller krav om at LNU «skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger».

Integritet: I forbindelse med informasjonssikkerhet: At det verken tilsiktet eller utilsiktet skal skje uautoriserte endringer av personopplysninger.

Internkontroll: Internkontroll er ledelsens verktøy for å styre aktiviteten i virksomheten slik at driften skjer i overensstemmelse med lover og regler. Samtidig er styringssystemet medarbeiderens verktøy for å utføre oppgaver på en forsvarlig og sikker måte.

Konfidensialitet: At uvedkommende ikke får tilgang på opplysninger.

Konfigurasjonsendring: Med konfigurasjon menes informasjonssystemets utforming inklusive både teknisk utstyr og programvare.

Personopplysning: Opplysninger og vurderinger som kan knyttes til enkeltperson.

Samtykke: En frivillig, spesifikk, informert, utvetydig og aktiv erklæring fra den registrerte om at hen godtar behandling av opplysninger om seg selv. Et samtykke kan trekkes tilbake når som helst uten negative konsekvenser.

Vedlegg 2 Sikkerhetsinstruks for ansatte og tillitsvalgte

Denne instruksen beskriver retningslinjer for bruk av informasjonsteknologi i LNU. Instruksen gjelder for alle ansatte og skal være lest og signert, og så leveres til assisterende generalsekretær, til oppbevaring i personalmappen.

Bruk av LNUs IKT-systemer

- Datamaskiner settes opp av informasjonsrådgiver med relevant programvare og tilgang til aktuelle IT-systemer. Før du får tilgang skal du gjennomgå grunnleggende opplæring i systemene.
- Dersom du har behov for ytterligere programvare, ta kontakt med informasjonsrådgiver.
- Du er selv ansvarlig for å følge de regler som gjelder for bruk av de forskjellige IKT-systemene og for behandling av beskyttelsesverdig informasjon i henhold til gjeldende regler.
- Utskrifter skal fjernes fra skriveren så snart utskriftsjobben er ferdig.
- Brukerkontoer deaktiveres 3 måneder etter oppsigelse eller vervslutt, med mindre annet er avtalt, og slettes senest etter ett år.

Brukernavn, passord og skjermsparer

- Du får tildelt brukernavn og førstegangspassord av informasjonsrådgiver.
- Passord er strengt personlig og skal ikke oppgis til eller lånes ut til andre.
- Passordet skal bestå av… *(fjernet)*
- Dersom du har mistanke om at passordet er blitt kjent av andre, skal passordet byttes og hendelsen rapporteres til assisterende generalsekretær (sikkerhetsansvarlig) snarest mulig som et avvik.
- Passordbeskyttet skjermsparer skal benyttes. Maskinen skal også være satt opp med automatisk skjermsparer med aktivering etter 15 minutters inaktivitet.
- Ved bruk av e-post på mobiltelefon eller annen portabel enhet skal enheten være sikret med mønster, kode eller tilsvarende låsemekanisme.

E-post

- All jobbrelatert epost (innkommende og utgående) skal gå gjennom LNUs e-postløsning.
- E-post sendt innad i LNUs e-postsystem er kryptert.
- LNU har i utgangspunktet ikke anledning til innsyn i privat e-post eller filer. Unntak gjelder hvis du er ikke-planlagt utilgjengelig i lengre tid, og virksomheten har behov for virksomhetsrelatert informasjon, ved begrunnet mistanke om straffbare forhold eller ved sikkerhetsmessige behov. Det er etablert en egen rutine for slikt innsyn (se kapittel 2.2).

Behandling av beskyttelsesverdig informasjon

- Beskyttelsesverdig informasjon skal som hovedregel ikke lagres lokalt på bærbare datamaskiner eller annet portabelt utstyr.
- Beskyttelsesverdig informasjon skal som hovedregel ikke behandles usikret på e-post. Selv om overføring og oppbevaring er sikret, er dette tiltaket ment å sikre.

- Ved mottak av beskyttelsesverdig informasjon på e-post fra en sender utenfor LNUs sekretariat skal denne slettes. Et unntak gjelder ved mottak av stillingssøknader til egen innboks. Andre unntak skal klareres med assisterende generalsekretær.
- Ved overføring av beskyttelsesverdig informasjon til andre personer med behandlingsgrunnlag, skal informasjonen krypteres med passord, eller sendes via lenke til fellesarkivet eller Google Disk. I Google Disk skal mappen filen ligger i indikere at den inneholder informasjon som slettes etter overføringen har skjedd.

Sikkerhetskopiering

- For å sikre at det blir tatt sikkerhetskopier, skal all jobbrelatert informasjon lagres på egen filserver i LNUs nettverk.
- Ansatte er selv ansvarlig for å vurdere hva som er arkivverdig. Ved tvil kontaktes LNUs administrasjonskonsulent.
- Filer på LNUs filserver sikkerhetskopieres i tre måneder på filserver og seks måneder i skyløsning. Det er kun informasjonsrådgiver som har tilgang til disse. Tilgangen til skyløsning er sikret med dobbelt autentisering.
- Ved behov for gjenoppretting av sikkerhetskopiert informasjon, kontakt informasjonsrådgiver.
- Informasjonsrådgiver skal legge til rette for at VPN er tilgjengelig for alle ansatte.

Nøkkelbrikker

- Dersom du mister nøkkelbrikken, meld umiddelbart fra til assisterende generalsekretær
- Ansatte som slutter skal levere nøkkelbrikken tilbake til assisterende generalsekretær for deaktivering

Sted/Dato:.....

Underskrift:.....

Navn i blokkbokstaver:.....

Vedlegg 3 Sikkerhetsinstruks for leder med personalansvar

Dette vedlegget inneholder sikkerhetsinstruks for ledere i LNU med personalansvar, det vil si assisterende generalsekretær, avdelingsleder for forvaltning og avdelingsleder for kompetanse og interessepolitikk.

Ansettelse

Sjekkliste for ansettelse av fast og midlertidig ansatte:

1) Taushetserklæring leses og underskrives av den ansatte
2) Sikkerhetsinstruks leses og underskrives av den ansatte
3) Utlevere nøkkelbrikke

Punktene 1 – 3 over skal gjennomføres før brukertilganger gis. Leder skal deretter informere informasjonsrådgiver om behov for brukertilganger. Vær spesielt oppmerksom på hvor lenge det er behov for tilgangen samt nivå på tilgang.

Assisterende generalsekretær er ansvarlig for å oppbevare en kopi av underskrevet erklæring og instruks.

Regelmessig verifikasjon av brukerkonti og brukertilganger

Informasjonsrådgiver skal sørge for regelmessig verifisering av brukertilganger til LNUs nettverk og IT-systemer. E-postkontoer til tidligere ansatte og tillitsvalgte skal være tilgjengelige 6 måneder etter at arbeidsforholdet/tillitsvalgtperioden utløp, og deretter stenges.

Leder skal så snart som praktisk mulig etter mottak, verifisere at oversikten er korrekt, dvs. reflekterer ansvar og organisasjonsmessig tilhørighet. Eventuelle feil og mangler skal formidles informasjonsrådgiver.

Hendelser med betydning for sikkerheten

Sikkerhetsrelaterte hendelser av alvorlig karakter skal rapporteres til sikkerhetsansvarlig.

Konsekvenser ved brudd på retningslinjene

Brudd på LNUs sikkerhetsregler er å betrakte som tjenesteforsømmelse, og skal vurderes i det enkelte tilfelle.

Permisjoner eller andre typer midlertidige arbeidsopphold

Leder skal vurdere innlevering av nøkkelbrikke/utlånt utstyr, samt påse at sensitiv informasjon er nedlåst.

Avslutning av arbeidsforhold

Leder skal verifisere at arbeidstaker har levert LNUs eiendeler:

- bærbar jobb-PC
- nøkkelbrikke

Leder skal:

- gi beskjed til informasjonsrådgiver om sperring av brukerkonti med brukertilganger.
- oppbevare kopi av beskjed til informasjonsrådgiver i den ansattes personalmappe.

Vedlegg 4 Sikkerhetsinstruks for sikkerhetsansvarlig

Sikkerhetsansvarlig (assisterende generalsekretær) rapporterer til behandlingsansvarlig (generalsekretær), og er nærmeste overordnede for følgende roller:

Sikkerhetsansvarlig har følgende ansvarsområder:

- Utarbeide og vedlikeholde regime for internkontroll.
- Ansvarlig for vedlikehold av dokumentet *Oversikt over personopplysninger*.
- Påse at de gjeldende sikkerhetsbestemmelsene, instrukser og rutiner blir fulgt.
- Påse at underlagte sikkerhetsledd har klart definerte oppgaver/forhold for å utøve sine funksjoner, og virkelig utøver disse.
- Ansvar for at administrasjonen utøver sitt ansvarlig for fysisk sikkerhet, personell og sikkerhet og dokumentsikkerhet.
- Påtale mislighold muntlig eller skriftlig, avhengig av misligholdets karakter.
- Sørge for at alle ansatte har kjennskap til regimet for internkontroll og tilhørende sikkerhetsbestemmelser, instrukser og rutiner.

Vedlegg 5 Taushetserklæring

Jeg forplikter meg herved til ikke å bruke, åpenbare, utlevere eller på annen måte gjøre tilgjengelig for uvedkommende informasjon om personopplysninger, data og organisasjonshemmeligheter som jeg har fått kjennskap til i mitt arbeid i Landsrådet for Norges barne- og ungdomsorganisasjoner.

Jeg vil også vise aktsomhet i omtale av andre forhold som jeg blir kjent med eller erfarer under mitt arbeid.

Jeg er dermed klar over straffelovens kapittel 21, og at brudd på bestemmelsene i denne loven kan medføre straffeansvar, oppsigelse eller avskjed.

Jeg er også klar over at denne taushetserklæringen gjelder etter opphør av ansettelsesforholdet eller oppdraget i henhold til lovene referert i avsnittet ovenfor.

Sted/Dato:.....

Underskrift:.....

Navn i blokkbokstaver:.....

Vedlegg 6 Avviksskjema

<table>
<tr><th colspan="3">Fylles ut av avviksmelder</th></tr>
<tr><td colspan="3">Sendes til: Sikkerhetsansvarlig</td></tr>
<tr><td colspan="3">Formål: Skjemaet skal sikre at alle brudd og antatte brudd på håndteringsrutiner eller sikkerhetsrutiner blir registret og behandlet på forsvarlig måte.</td></tr>
<tr><td colspan="3">Beskrivelse av avviket:

Vedlegg:</td></tr>
<tr><td colspan="3">Beskrivelse av midlertidig tiltak:

Vedlegg:</td></tr>
<tr><td colspan="2">Navn:</td><td>Dato/signatur:</td></tr>
<tr><th colspan="3">Fylles ut av sikkerhetsansvarlig</th></tr>
<tr><td colspan="3">Analyse av årsak:

Vedlegg:</td></tr>
<tr><td colspan="3">Beskrivelse av iverksatte tiltak:

Henvendes til:</td></tr>
<tr><td>Klassifikasjon:</td><td>Rapport sendes Datatilsynet:</td><td>Dato/signatur:</td></tr>
</table>

Vedlegg 7 Risikovurdering

Hendelse (vannskade, innbrudd, strømbrudd, osv.)	**Konsekvens**	**Sannsynlighet**	**Vurdering**

Vedlegg 8 Egenkontrollskjema

Egenkontrolltiltak	**Eier av aktivitet**	**Frekvens**	**Resultat**	**Kommentarer/ tiltak**