Veileder

for
behandling av personopplysninger og informasjonssikkerhet i idretten

Vedtatt av Generalsekretæren 20.12.2017

NORGES IDRETTSFORBUND

Bakgrunn

Digitalisering og bruk av IT-løsninger i idretten er økende. Frivillig sektor gjennomgår en profesjonalisering som en konsekvens av bl.a. krav som stilles fra offentlige myndigheter, de offentlige tilskudd som gis til idretten samt krav til innrapportering til offentlig sektor som f.eks. organisasjonsdata til Brønnøysundregistrene og innrapportering til skattemyndighetene osv. I tillegg søker idretten å utnytte elektroniske løsninger på en slik måte at disse kan bidra til å forenkle de oppgaver som idretten selv må løse, enten det er i det lokale idrettslaget eller i andre organisasjonsledd i idretten.

Utviklingen og bruken av sentrale registre i idretten har vært sterkt økende de senere år, og bidrar bl.a. til bedre datakvalitet, bedre kontroll og styring av tilgangen til persondata. Den økende elektroniske behandlingen av opplysninger gir muligheter, men skaper også utfordringer for informasjonssikkerheten. Det kan oppstå utilsiktede konsekvenser for opplysningenes konfidensialitet, og særskilte tiltak må iverksettes for å sikre at uvedkommende ikke får tilgang til opplysninger som er lagret elektronisk.

Idrettsstyret har 14.11.2017 vedtatt en ny *Norm for behandling av personopplysninger og informasjonssikkerhet* i idretten som erstatter den tidligere bransjenormen *Retningslinjer for databehandling i idretten*. Den nye normen gir idrettsorganisasjonen bedre grunnlag for å møte dagens og fremtidens lovpålagte krav knyttet til informasjonssikkerhet og personvern. Den nye normen gjør det også enklere å imøtekomme kravene ifm. innføring av ny lov for behandling av personopplysninger fra 25. mai 2018, hvor normen vil kreve en revisjon. Ny lov kommer som følge av EUs personvernforordning, GDPR (Global Data Protection Regulation).

Normen i sin helhet kan oppleves som omfattende for mindre organisasjonsledd, og denne veilederen er derfor etablert som en kortversjon med de mest sentrale punktene, samtidig som denne er mer praktisk rettet enn normen. Vi gjør likevel oppmerksom på at alle organisasjonsledd har et selvstendig ansvar for å etterleve gjeldende lovgivning om behandling av personopplysninger og informasjonssikkerhet, herunder særlig personopplysningsloven. Vi anbefaler derfor alle å sette seg inn i *Norm for behandling av personopplysninger og informasjonssikkerhet i idretten* for å sikre seg at lovens krav blir fulgt, herunder krav til meldeplikt, søknad om konsesjon mv.

Det er organisasjonsleddets ledelse som har ansvaret for å etablere og opprettholde tilfredsstillende informasjonssikkerhet. Brudd på lovverket kan straffes med svært store bøter fra ny lov trer i kraft i mai 2018, regnet ut fra organisasjonens brutto omsetning.

Norm for behandling av personopplysninger og informasjonssikkerhet i idretten finnes her.

Innhold

1. Personopplysninger

1.1. Om personopplysninger

Personopplysninger er opplysninger og vurderinger som kan knyttes til en enkeltperson. Norges Idrettsforbund og tilknyttede organisasjonsledd kan innhente og bruke slike opplysninger med hjemmel i «medlemsavtalen». Dvs. når en person blir medlem i idretten har idretten lovlig grunnlag for registrering og behandling (behandlingsgrunnlag) av nødvendige personopplysninger. Det gjøres særskilt oppmerksom på at regelverket omhandler all behandling av personopplysninger, og ikke bare de som lagres og behandles i IT-systemene.

1.2. Hvorfor registreres personopplysninger?

Formålet med all behandling av personopplysninger er ivaretagelsen av alle aktiviteter og medlemsavtalen, herunder gi god service til medlemmer og andre personer tilknyttet organisasjonen.

Medlemskap i idretten innebærer at idrettsorganisasjonen må behandle personopplysninger i ulike sammenhenger som ved administrasjon av aktivitet (idrett/konkurranser), medlemskap, roller og verv, forsikringer, kurs og kompetanse, rapportering til offentlige myndigheter med mer.

Personopplysninger skal

1. henføres til rett identifisert person
2. være riktige og ajourførte
3. ikke benyttes til formål som er uforenlig med behandlingsgrunnlaget.

Personer som registreres med e-postadresse varles pr. e-post og gis automatisk mulighet for å bli bruker til Min idrett hvor lagret informasjon vises og kan korrigeres av personen selv.

Personopplysninger for enkelte personer kan oppbevares for ivaretagelse av historiske data over tid bl.a. å ivareta historisk informasjon om aktivitet (resultater fra konkurranser m.v.) mens for andre personer må persondata slettes eller anonymiseres. Se mer om dette i punkt 1.6 i *Normen.*

Organisasjonsledd som har saklige behov for registrering av sensitive personopplysninger som f.eks. helseopplysninger, må søke konsesjon fra Datatilsynet for registrering og behandling av sensitive personopplysninger, med mindre dette utøves av legetjeneste dekket under Helseregisterloven. I slike tilfeller må organisasjonen forholde seg til *Norm for informasjonssikkerhet i idretten.*

Et organisasjonsledd håndterer i tillegg personopplysninger om egne ansatte.

1.3. Hva registreres?

Det registreres persondata som

1. fødselsnummer
2. folkeregistrert navn
3. adresse
4. andre kontaktopplysninger
5. ev. knytninger til andre familiemedlemmer (foresatte og søsken)
6. relevant informasjon knyttet til idretten og roller en har i idretten.

For personer som er tildelt hemmelig adresse av Folkeregisteret skal dette

forholdet ivaretas av idretten, og disse personene skal ikke lagres med adresse i idrettens systemer. Persondatabasen hos NIF vaskes mot Folkeregisteret og adressefeltene i fellesløsningene er ikke mulig å oppdatere for slike personer.

Personopplysninger som registreres skal være relevante og nødvendige, og registrering skal gjøres snarest mulig etter at informasjonen har fremkommet.

Persondata kontrolleres mot Det sentrale folkeregister. Idrettens systemer gjenbruker folkeregistrert navn, kjønn og fødselsdato, dvs. disse kan ikke endres.

1.4. Hvordan brukes personopplysningene?

Personopplysningene brukes av de som har et rettmessig behov for tilgang til disse, f.eks.

1. for å administrere medlemskap og betalinger
2. kursadministrasjon
3. administrasjon av påmelding/deltagelse i trening og konkurranser
4. lisenser og forsikringer mv.

Fødselsnummeret brukes ikke og vises ikke for brukere av idrettens løsninger. Dette registreres primært for å få en **entydig identifisering** av personen slik at data kan oppdateres basert på endringer som meldes til folkeregisteret. Fødselsnummeret brukes ellers kun i sammenhenger hvor idretten er pålagt å rapportere dette som en del av utveksling av informasjon med f.eks. offentlige etater eller forsikringsselskap.

Persondata er ikke søkbare på idrettens løsninger på internett med mindre en selv tillater dette ved å oppdatere sine personlige innstillinger på Min idrett. Dog, knyttet til det å la seg velge eller oppnevne til tillitsverv i en frivillig organisasjon, følger det at man også aksepterer at ens navn blir offentliggjort overfor allmennheten. Omfanget av annen informasjon som offentliggjøres har medlemmet anledning til å bestemme selv.

For informasjon om overføring av personopplysninger til internasjonale idrettsorganisasjoner, se *Normen* for ytterligere informasjon.

1.5. Informasjon og samtykke

Det skal innhentes samtykke fra personen i alle tilfeller hvor dette er nødvendig, herunder når tilgangen til den aktuelle behandlingen av personopplysninger ikke er fastsatt i lov eller har et annet gyldig behandlingsgrunnlag, dvs. når en skal behandle personopplysninger som går utover det som er rimelig som følge av «medlemsavtalen» og det ikke finnes annet lovhjemlet behandlingsgrunnlag. Samtykke skal innhentes fra foresatte når det kreves samtykke fra person er et barn under 15 år. Samtykke innhentes i tråd med alminnelige regler for samtykke.

Det kreves ikke særskilt samtykke for at et organisasjonsledd skal kunne distribuere markedsmateriell fra sine sponsorer direkte til personer tilknyttet organisasjonsleddet. Annen bruk av persondata for kommersielle hensyn er utenfor formålet og den registrerte har derfor rett til å reservere seg mot slik direkte markedsføring. Medlemsopplysninger skal **ikke** utleveres til tredjepart.

Dersom personen har oppgitt mobiltelefonnummer/e-postadresse, er dette å anse som et samtykke til at organisasjonsleddet kan kontakte vedkommende per e-post og SMS med bakgrunn i medlemsavtalen.

2. Konfidensialitet og taushetsplikt

Konfidensialitet skal ivareta taushetsplikten og for øvrig sikre mot at uvedkommende får kjennskap til opplysningene. Dette innebærer blant annet:

- ☐ Personer utenfor organisasjonsleddet uansett ressurser og kunnskap skal ikke kunne få uautorisert tilgang til personopplysninger.
- ☐ Personer i organisasjonsleddet skal gis tilgang i henhold til prinsippene for tilgangsstyring, jfr. pkt. 3 nedenfor.

For å sikre konfidensialitet for personopplysninger skal organisasjonsleddets leder sikre at alle som gis tilgang har taushetsplikt, og at de er bevisst taushetspliktens innhold og omfang.

Brudd på taushetsplikten og/eller ulovlig tilegnelse skal som konsekvens minimum medføre en advarsel for den som begår bruddet, og bruddet skal behandles iht. avviksprosedyre som beskrevet i normen. Brudd på taushetsplikten og/eller ulovlig tilegnelse er forbudt og varsling til tilsynsmyndighetene og anmeldelse må vurderes.

For å oppdage brudd eller forsøk på å bryte regelverket loggføres det følgende i de sentrale systemene:

- ☐ Sikkerhetsbarrierene registrerer sikkerhetsrelevante hendelser, bl.a. forsøk på uautorisert bruk av informasjonssystemet.
- ☐ Alle systemer som bruker Idrettens Sentrale Database registrerer alle forsøk på uautorisert bruk.

3. Tilgangsstyring

Tilgangsstyringen omfatter hvem som kan tildele rettigheter i idrettens systemer og dermed få tilgjengeliggjort personopplysninger.

Tildeling av rettigheter i idrettens systemer skal kun skje til personer som er underlagt eller arbeider under eget organisasjonsledds instruksjonsmyndighet (f.eks. egne ansatte, tillitsvalgte, osv.). Forhold knyttet til eksterne leverandører (utover konsulenter som ev. er under organisasjonsleddets instruksjons-myndighet) er regulert i *normen*, se punkt 4.6.

Autorisasjon kan bare gis i den grad det er nødvendig for personens rolle/arbeid, er begrunnet i tjenstlige behov og er i henhold til bestemmelser om taushetsplikt. Det er kun disse som kan gis tilgang til personopplysninger.

For idrettens fellessystemer er myndigheten for å tildele rettigheter delegert til det enkelte organisasjonsleddets ansvarlige ledelse, dvs. daglig leder, styreleder og styremedlemmer. Påloggingsinformasjon skal hemmeligholdes.

Gjennomgang og kontroll av tildelte rettigheter (roller/verv) skal foretas av den enkelte leder minimum en gang årlig, f.eks. etter avholdt årsmøte/ting og andre tidspunkter når det skjer endringer i ansettelsesforhold eller blant tillitsvalgte.

4. Avviksbehandling

Avvik skal behandles ved sikkerhetsbrudd, ved urettmessig tilgang til personopplysninger og/eller når behandling av personopplysninger er utført i strid med gjeldende regelverk, retningslinjer eller prosedyrer.

Hver enkelt person er ansvarlig for å rapportere oppdagede avvik på fastsatt elektronisk skjema på https://www.idrettsforbundet.no/varsle

Ved uautorisert utlevering av personopplysninger vil Datatilsynet bli varslet.

5. Ytterligere informasjon

Avslutningsvis henviser vi til *Normen* for de spesifikke kravene som stilles for å ha god informasjonssikkerhet i idretten. Vi viser også til gode, praktiske råd for å ivareta informasjonssikkerheten knyttet til personvern som finnes her: https://itinfo.nif.no/Personvern