Behandling av personopplysninger

Del I – Styrende aktiviteter i Persbråten Basketballklubb

Desember 2018

Innholdsfortegnelse

1. Innledning

1.1 Nærmere om idrettslaget

Idrettslagets formål er å drive idrett organisert i Norges idrettsforbund og olympiske og paralympiske komité (NIF). Persbråten Basketballklubb ble etablert i 1967og har 175 registrerte medlemmer.

Om medlemmer behandler idrettslaget følgende personopplysninger:

- navn, fødselsdato, statsborgerskap, kjønn, adresse, telefonnummer, epostadresse og personID;
- familietilknytninger;
- lisenser/forsikringer;
- overganger;
- kurs/kompetanse;
- roller og verv;
- dato for betaling av medlemskontingent og trenings-/aktivitetsavgift;
- dato for innmelding og avslutning av medlemskap;
- tilknytning til konkurranseaktivitet;

Idrettslaget kan også samle inn og behandle helseopplysninger om de medlemmene som gjennomfører fysiske tester eller av andre grunner knyttet til trening og/eller konkurranse. Ved arrangementer, turer o.l. i regi av idrettslaget vil det ofte være behov for å samle inn informasjon om deltakernes helsetilstand eller religiøse overbevisning eller andre sensitive personopplysninger for å legge til rette for inkludering av samtlige. Dette er særlig aktuelt der det vil bli servert mat (matallergier, matgrupper som strider med religion e.l.). Idrettslaget må ha samtykke for å behandle slike opplysninger.

Flere av medlemmene er under 15 år. For behandling av deres personopplysninger må de foresatte samtykke til registreringen. I forbindelse med registrering av barn under 15 år, registreres det er derfor også opplysninger om deres foresatte.

Opplysninger som behandles om frivillige kan omfatte opplysninger i samme utstrekning som medlemmer. «Frivillige» omfatter blant annet tillitsvalgte, trenere, oppmenn o.l. og andre frivillige som gjør arbeid for idrettslaget uten lønn eller annen form for kompensasjon.

For en nærmere angivelse av hvilke personopplysninger som behandles om de registrerte personene, se kartleggingsmatrisen, vedlegg 1.

2. Strategi personvern – Internkontroll behandling av personopplysninger

2.1 Strategi personvern

Personopplysninger skal hos idrettslaget behandles på en lovlig, rettferdig og transparent måte. idrettslaget har som mål å behandle så *få* opplysninger som mulig.

Personopplysningene idrettslaget behandler skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»).

Det overordnede formålet med idrettslagets behandling av personopplysninger er at personopplysninger kun skal innhentes og behandles i den grad dette er nødvendig for ivaretagelsen av organisasjonens aktivitet, medlemskapet i NIF/Særforbund og for å kunne gi god service til medlemmer, foresatte og andre personer tilknyttet organisasjonen. Disse formålene skal ivaretas av idrettslaget på lokalt nivå.

2.2 Personvern i idrettslaget

Idrettslagets håndtering av personopplysninger er basert på følgende personvernprinsipper:

- ✓ Behandling av personopplysninger skal baseres på at behandlingen er nødvendig for å håndtere medlemskapet eller vervet, idrettslagets berettiget interesse, samtykke eller annet rettslig grunnlag
- ✓ All behandling av personopplysninger må skje i overensstemmelse med det til enhver tid gjeldende personvernregelverk, og på en måte som er balansert med hensyn til den som er registrert.
- ✓ Personopplysninger skal bare samles inn for bestemte formål og disse må være legitime.
- ✓ Personopplysninger skal bare behandles i den grad det er nødvendig for å oppnå formålet.
- ✓ Personopplysninger må være relevante, korrekte og fullstendige ut fra det formål de skal benyttes til.
- ✓ Den registrerte skal ha rett til å bli informert om innsamling og bruk av sine opplysninger
- ✓ Databehandler skal sikre opplysningene mot uautorisert tilgang, endring, ødeleggelse og spredning
- ✓ Håndtering av sensitive personopplysninger skal være underlagt særlig strenge rutiner.
- ✓ All registrering av personopplysninger skal begrunnes. Hvis det ikke er nødvendig å registrere identifiserende opplysninger har enkeltindividet rett til å være anonymt.

2.3 Internkontrollsystem for behandlingen av personopplysninger

Personopplysningsloven sammen med generell personvernforordning (personvernforordningen), slik den er implementert i norsk rett, regulerer virksomheters behandling av personopplysninger i Norge. Internkontrollsystemet i idrettslaget er ment å ivareta prinsippene i personvernforordningen og sikre at det gjennomføres egnede tekniske og organisatoriske tiltak i tråd med personvernregelverket.

Internkontroll for behandling av personopplysninger deles gjerne i tre deler;

i. Styrende del
ii. Gjennomførende del
iii. Kontrollerende del

Ved siden av å være et styrende system skal idrettslagets internkontroll for behandling av personopplysninger også kunne legges frem for overordnede organisasjonsledd, Datatilsynet og Personvernnemnda ved behov, samt være tilgjengelig for idrettslagets medarbeidere, og medlemmer og mindreårige medlemmers foresatte.

2.3.1 Styrende dokumentasjon

Styrende del av internkontroll for behandling av personopplysninger, skal blant annet regulere idrettslagets mål og policy for behandling av personopplysninger. Videre skal den styrende del gi en

oversikt over hvilke personopplysninger som behandles og hvilke tiltak som er iverksatt for å møte personvernforordningens grunnkrav til behandling av personopplysninger, jf. personvernforordningen artikkel 5 og 30.

Styrende del er del I av internkontrollen i idrettslaget.

2.3.2 Gjennomførende dokumentasjon

Gjennomførende del av internkontrolldokumentet skal vise og adressere behandlingsansvarliges plikter. Den gjennomførende delen vil gi prosedyrer og arbeidsinstrukser for håndtering av personopplysninger i idrettslaget.

Gjennomførende del er del II av internkontrollen i idrettslaget.

2.3.3 Kontrollerende dokumentasjon

Kontrollerende del av internkontrollen har som formål å verifisere at behandlingene har foregått i samsvar med fastsatte prosedyrer og instrukser.

Eksempelvis skal den kontrollerende delen inkludere rapporter, sjekklister, logg mv. Den kontrollerende delen kan betraktes som et "sikkerhetsnett" som bidrar til at styringsdokumentene (under gjennomførende del) følges og at eventuelle avvik lettere oppdages.

Kontrollerende dokumentasjon omhandler sjekklister, skjema for avviksrapportering, rapporter og logg. Kontrollerende dokumentasjon består av to deler: En del som brukes under interne revisjoner og en del som brukes i det daglige arbeidet. Det er et klart skille mellom gjennomførende og kontrollerende dokumentasjon. Det første skal sikre at aktivitetene er i samsvar med mål og policy. Det siste skal bidra til at avvik fra mål og policy oppdages og rettes.

Kontrollerende del er del III av internkontrollen i idrettslaget.

2.4 Definisjoner

De mest sentrale personvernbegrepene er listet i vedlegg 7, hvor innholdet i begrepene er definert. Listen omfatter begreper som personopplysning, behandleransvar, databehandler, felles behandlingsansvar og behandlingsgrunnlag.

3. Behandling av personopplysninger i idrettslaget

3.1 Ansvarsplassering – flyt personopplysninger

3.1.1 Behandleransvar

Idrettslaget behandler en rekke personopplysninger om eksempelvis medlemmer og deres foresatte, trenere, dommere, tillitsvalgte og andre frivillige. Formålet med behandling av personopplysninger i idrettslaget er primært administrering av medlemskap, aktiviteter og verv.

Se vedlegg 1 for oversikt over de personopplysninger som behandles i idrettslaget.

Idrettslagets ledelse har det overordnede ansvaret for at behandlingen av personopplysninger skjer i tråd med til enhver tid gjeldende personvernregelverk, og har således behandleransvaret.

3.1.2 Nærmere om idrettslagets felles behandleransvar

Ved administrering av medlemsmassen, overordnet og på daglig basis, foreligger det et felles behandlingsansvar mellom idrettslaget, og øvrige organisasjonsledd i Norges idrettsforbund (NIF Dette omfatter alle personopplysninger som inngår i Idrettens sentrale database og som gjøres tilgjengelig via idrettens felles informasjonssystemer (KlubbAdmin, SportsAdmin). Ansvaret for å administrere Idrettens sentrale database har idretten lagt til NIF. Se vedlegg 6 for ytterligere informasjon om ordningen om felles behandleransvar.

Det er en forutsetning for å delta i organisert aktivitet, inneha tillitsverv, og/eller utføre oppgaver for idrettslaget at personopplysninger om den enkelte kan deles mellom alle NIFs organisasjonsledd. Dette innebærer at hver av partene i utgangspunktet har et selvstendig behandlingsansvar, men også et ansvar for de andres behandling av personopplysninger.

Opplysninger som idrettslaget har et felles behandlingsansvar for omfatter opplysninger om medlemmer, mindreårige medlemmers foresatte, tillitsvalgte og frivillige om blant annet;

- informasjon om personen, inkludert navn, fødselsdato, statsborgerskap, kjønn, adresse, telefonnummer, epostadresse og personID;
- familietilknytninger;
- lisenser/forsikringer;
- overganger;
- kurs/kompetanse;
- roller og verv;
- dato for betaling av medlemskontingent og trenings-/aktivitetsavgift;
- dato for innmelding og avslutning av medlemskap;
- tilknytning til konkurranseaktivitet.

For noen medlemmer eller frivillige kan idrettslaget være pålagt å få fremlagt politiattest fra vedkommende for at personen skal kunne utføre oppdrag på vegne av idrettslaget. Nødvendige opplysninger om fremvist politiattest vil fremgå i idrettslagets systemer, men det er kun opplysninger om at attesten er sett, av hvem og når, og at det ikke foreligger avgjørende anmerkninger, som vil lagres.

Det er etablert en ordning mellom NIF og NIFs organisasjonsledd som fastsetter formålene og midlene for behandlingen, hvor det respektive ansvaret for å overholde forpliktelsene i personvernregelverket er fastsatt, se vedlegg 6. Beskrivelsen er også tilgjengelig ved pålogging til idrettens felles informasjonssystem. NIF administrerer databehandlerforholdene knyttet til idrettens felles informasjonssystem. En nærmere oversikt over databehandlere knyttet til idrettens felles systemer, er tilgjengelig som en del av NIFs personvernerklæring.

Der idrettslaget tar i bruk eksterne løsninger (andre løsninger enn de NIF tilbyr) for innsamling av personopplysninger, vil det ikke foreligge felles behandlingsansvar mellom de tre organisasjonsleddene

for denne behandlingen. Slike eksterne løsninger som driftes ved hjelp av idrettslagets egne databehandlere er listet nedenfor under punkt 4.

3.2 Felles rutiner for behandling av personopplysninger - Personvernombud

Idrettslaget har utarbeidet, administrerer og vedlikeholder rutiner for behandling av personopplysninger om frivillige, medlemmer og andre. Rutinene er basert på strategien som fremkommer av dette dokumentet.

Det er utarbeidet to sett med rutiner:

a) For behandling av data om frivillige. Se Vedlegg 4.

b) For behandling av data om medlemmer og deres foresatte. Se Vedlegg 5.

3.3 Lokalt ansvar

Idretten behandler personopplysninger i stort omfang, og i flere organisasjonsledd. Organisasjonsleddene har, som behandlingsansvarlige, et selvstendig ansvar for å opprette og vedlikeholde et tilfredsstillende internkontrollsystem.

Policy for behandling av personopplysninger slik de er nedfelt i dette dokument (Styrende del) kommer i tillegg rutiner for sikring av informasjon og personopplysninger i idrettslaget (Gjennomførende del).

Nødvendig dokumentasjon for å oppfylle personvernforordningens krav til internkontroll utover dette dokumentet omfatter blant annet

- Ansvarsplassering i idrettslaget – ansvarlige avdelinger/roller for ulike hovedkategorier
- Overordnet og intern risikovurdering ved idrettslagets behandling av personopplysninger
- Sikkerhetsmål, sikkerhetsstrategi og akseptkriterier (utover kap 6)
- Sikkerhetsorganisasjon
- Fordeling av ansvar og roller internt i idrettslaget
- Rutiner for jevnlig ivaretagelse av idrettslagets tekniske og organisatoriske tiltak (kontrollerende del)
- Ivareta protokoller, retningslinjer og rutiner for behandling, jf. plikt til å føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar i personvernforordningen art. 30.
- Rutiner for bruk av databehandlere og eventuell overføring til utlandet
- Vedlikeholde informasjon utad, inkl. personvernerklæring
- Samarbeid med tilsynsmyndigheten
- Varsling av avvik til Datatilsynet, og til den registrerte
- Håndtering av henvendelser fra registrerte, utover det som følger av felles rutiner
- Vurdering av sikkerhetsmessige tiltak
- Overordnet kontrollrutine for behandlingen av personopplysninger

4. Databehandlersituasjoner

4.1 Innledning

Idrettslaget har tjenesteutsatt flere oppgaver til eksterne tjenestetilbydere og gjør dermed bruk av databehandler i sin behandling av personopplysninger.

4.2 Oversikt databehandlere

Se vedlegg 1 for oversikt over dataflyt m.m i løsningene.

Databehandler	System	Inngått databehandleravtale	Bruk av underleverandør
IA			

4.3 Oversikt – databehandlere for idrettens felles informasjonssystemer

For opplysningene som behandles under et felles behandlingsansvar mellom NIF og andre organisasjonsledd, er det NIF som er ansvarlig for å inngå databehandleravtaler med tredjeparter for den felles behandlingen. Idrettens felles informasjonssystem har blant annet en integrasjon med Buypass AS, hvorav Buypass AS opptrer som databehandler.

Uttømmende oversikt over tredjeparter som opptrer som databehandlere for idrettens felles informasjonssystemer kan finnes ved pålogging i idrettens felles informasjonssystemer og i personvernerklæringen på www.idrettsforbundet.no

5. Risikoanalyse – Vurdering av personvernkonsekvensene

5.1 Risikovurdering av idrettens systemer

Systemer idrettslaget bruker til behandling av personopplysninger skal ivareta følgende prinsipper om behandlingen av personopplysningene:

- Konfidensialitet – personopplysninger må være sikret mot at uvedkommende får tilgang til dem;
- Integritet– personopplysninger skal være sikret mot utilsiktet eller uautorisert endring eller sletting;
- Tilgjengelighet – personopplysninger skal være tilgjengelig for det formålet de er tiltenkt.

Dette betyr at den behandlingsansvarlige (idrettslaget) må sørge for å iverksette tiltak mot utilsiktet og ulovlig ødeleggelse, tap og endring av personopplysninger.

Idrettslaget skal ikke ta i bruk systemer som etter en vurdering i lys av disse kriteriene overstiger et akseptabelt risikonivå. NIF sentralt vil stå for gjennomføringen av risikovurderinger knyttet til idrettens felles informasjonssystemer. Veiledning til gjennomføring av risikovurderinger i det enkelte organisasjonsledd er gitt i «Håndbok for informasjonssikkerhet» utarbeidet av NIF.

Konklusjon: Persbråten Basketballklubb har konkludert med at risikonivået forbundet med sine informasjonssystemer er akseptabelt.

5.2 Vurdering av personvernkonsekvenser

I tillegg til risikovurdering, skal det dersom det er trolig at en type behandling vil medføre en høy risiko for fysiske personers rettigheter og friheter, foretas en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personvernet før behandlingen starter.

Det medfører at for enhver behandling som foretas internt i idrettslaget, bør det foretas en vurdering av behandlingens art, omfang, formål og sammenheng, for å avklare om det medfører en høy risiko ved behandlingen. Dette er for å avklare om det må foretas en ytterligere og konkret konsekvensvurdering av den aktuelle behandlingen som har høy risiko (Data Proteksjon Impasto Assement – DPIA).

5.3 Behandling i idrettslaget som krever vurdering av personvernkonsekvenser

Det er behandlingsansvarlig selv som må ta det avgjørende valget om det skal foretas en vurdering av personvernkonsekvenser.

For behandlingsaktiviteten som utføres under det felles behandlingsansvar som foreligger mellom NIF, særforbund og idrettslagene, er det besluttet at NIF skal gjennomføre risikovurderingene. NIF vil gjøre risikovurderingene tilgjengelig på forespørsel.

Konklusjon: Persbråten Basketballklubb har gjort en overordnet vurdering, jf. punktet over, og finner at det ikke foretas behandlinger av høy risiko.

6. Informasjonssikkerhet

6.1 Sikkerhetsmål

Det overordnede sikkerhetsmålet ved idrettslagets behandling av personopplysninger er at all bruk av personopplysninger skal være i samsvar medlemsavtalen, innhentet samtykke og-/ eller annet behandlingsgrunnlag, at opplysningene skal være fullstendige, oppdaterte og korrekte, og at omfanget av behandling av personopplysninger skal begrenses til det som er nødvendig.

Informasjonssikkerheten i idrettslaget skal videre ivaretas slik dette er beskrevet i sikkerhetsmålene nedfelt i «Håndbok for informasjonssikkerhet i idretten».

Målene skal understøtte og sikre idrettslagets og idrettens drift, allmenne tillit og omdømme i det offentlige rom, ved å forebygge og begrense forekomsten og konsekvensene av uønskede hendelser. Sikkerhetsmålene beskriver NIFs overordnete mål for beskyttelse av organisasjonens informasjonsbehandling mot interne og eksterne trusler av tilsiktet og utilsiktet art.

6.2 Sikkerhetsstrategi

Styreleder og frivillige som utfører enkelte organisatoriske eller administrative funksjoner på idrettslagets vegne har et medansvar for at informasjons- og personopplysningssikkerheten ivaretas i tråd med sikkerhetsmålene.

Styreleder skal sette seg inn i de målsetninger og retningslinjer som følger av dette dokumentet, samt de rutiner som gjelder for behandling av personopplysninger om frivillige og medlemmer i idrettslaget.

Idrettslagets ledelse har det overordnede ansvaret for å sørge for at andre som utfører oppgaver som innebærer behandling av personopplysninger på idrettslagets vegne har satt seg inn i de retningslinjer som gjelder for vedkommende ansvarsområde, slik disse følger av rutinene i internkontrollen Del II.

6.3 Sikkerhetsorganisasjon

Ethvert avvik fra kravene til behandling av personopplysninger skal varsles og følges opp. Alt etter alvorlighetsgrad, skal varsling skje til styreleder, Datatilsynet eller de registrerte selv.

Varslinger skal skje i henhold til rutinene for varsling i internkontrollsystemets Del II. Avvik skal følges opp, og det skal implementeres tiltak for å forhindre at de inntrer igjen.

6.4 Fysisk sikkerhet

Utstyr som benyttes av idrettslaget til behandling av personopplysninger skal sikres forsvarlig. Dører til lokaler hvor slikt utstyr befinner seg skal være låst når lokalene ikke er i bruk, og ellers utilgjengelig for uvedkommende.

6.5 Tilgang til informasjonssystem

Kun tillitsvalgte i idrettslaget som har tjenstlig behov for tilgang til idrettslagets systemer, skal gis tilgang, og kun i den utstrekningen som er nødvendig for at den enkelte kan gjennomføre sine oppgaver.

6.6 Overordnet konfigurasjonskontroll

Idrettslaget har gitt mulighet for at følgende roller og funksjoner kan gjøre endringer i personopplysninger i systemer som benyttes av idrettslaget:

- Styreleder med oppgaver knyttet til administrasjon av styremedlemmer, medlemmer og foresatte, trenere, oppmenn, dommere eller andre frivillige.
- Styremedlemmer med oppgaver knyttet til administrasjon av styremedlemmer, medlemmer og foresatte, trenere, oppmenn, dommere eller andre frivillige.
- Trenere og lagkontakter som håndterer opplysninger om utøvere og støttepersonell knytte til det enkelte lag/gruppe via lister i ecxel

I tillegg er det lagt opp til at det enkelte medlem og foresatte kan gjøre endringer i egne opplysninger via Min Idrett.

6.7 Ansvar for personer som gis tilgang til systemer og eller administrerer opplysninger på vegne av idrettslaget.

Det skal sikres at alle som gis tilgang til opplysninger i idrettslagets informasjonssystemer er gjort kjent med denne policyen og øvrige relevante retningslinjer, samt har undertegnet på taushetserklæring.

6.8 Tilgang til opplysningene

For idrettens felles informasjonssystemer, er påloggingen mot disse systemene basert på idrettens felles id og rettigheter er basert på roller. All tilgang til opplysninger skal som et minimum være sikret med brukernavn og passord.

7. Vedlegg