GDPR

FOR

SBK SKIOLD

Innholdsfortegnelse:

Behandling av personopplysninger

Del I – Styrende aktiviteter

Innholdsfortegnelse

1. Innledning

1.1 Nærmere om idrettslaget

Idrettslagets formål er å drive idrett organisert i Norges idrettsforbund og olympiske og paralympiske komité (NIF) i samsvar med idrettslagets lov og organisasjonsplan.

Dersom idrettslaget har ansatte, behandles personopplysninger om ansatte. Opplysningene omfatter eksempelvis navn, telefonnummer, adresse, bankkontonummer, fødsels- og personnummer, informasjon som arbeidsgiver er pålagt å registrere.

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;
- helseopplysninger på enkelte barn som deltar på klubbens IFO

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 andre sensitive personopplysninger for å legge til rette for samtlige. Dette er særlig aktuelt der det vil bli servert mat og det av hensyn til den enkelte registreres informasjon om f.eks. allergi eller religiøs overbevisning. Idrettslaget må ha samtykke for å samle inn og behandle slike opplysninger.

Flere av medlemmene er under 15 år. For behandling av deres personopplysninger må de foresatte samtykke til innmelding og registrering av personopplysninger. I forbindelse med registrering av barn under 15 år, registreres det er derfor også opplysninger om deres foresatte. Dette omfatter opplysninger i samme utstrekning som medlemmer.

Opplysninger som behandles om frivillige omfatter opplysninger i samme utstrekning som medlemmer. «Frivillige» omfatter blant annet tillitsvalgte, trenere, o.l. og andre 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.

2. Strategi personvern – Internkontroll behandling av personopplysninger

2.1 Strategi for personvern

Idrettslaget skal behandle personopplysninger 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).

De overordnede målene med idrettslagets behandling av personopplysninger er at disse kun skal innhentes og behandles i den grad dette er nødvendig for ivaretagelsen av idrettslagets aktivitet, medlemskapet i NIF og særforbund, og for å kunne gi god service til medlemmer og andre personer tilknyttet organisasjonen.

Målene skal understøtte og sikre idrettslagets drift, allmenne tillit, og omdømme i det offentlige rom, ved å forebygge og begrense uønskede hendelser.

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 personvernforordningen, slik den er implementert i norsk rett, regulerer virksomheters behandling av personopplysninger i Norge, jf. art. 1 i personvernforordningen.

Personvernforordningen art. 5 nr. 2 pålegger behandlingsansvarlige et ansvar for å kunne *påvise* at prinsipper for behandling av personopplysninger, oppstilt i personvernforordningen art. 5 nr. 1 overholdes («ansvar»).

Personvernforordningen art. 24 nr. 1 angir at den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og *påvise* at idrettslagets behandling av personopplysninger utføres i samsvar med personvernforordningen (internkontroll for behandling av personopplysninger). I dette ligger det også et krav til behandlingsansvarlig å dokumentere idrettslagets behandling av personopplysninger, herunder revisjons- og kontrollrutiner, og å ha en personvernstrategi.

Samlet sett betyr disse bestemmelsene at personvernforordningen skjerper kravene til virksomheters og offentlige organers behandling av personopplysninger. Personvernforordningen er per 2018 et helt nytt regelverk. Etterfølgende forståelse av regelverket, inkludert praksis, vil kunne påvirke og endre forståelsen av rettstilstanden innenfor personvern og dermed også påvirke idrettslagets internkontroll for behandling av personopplysninger.

Nye behandlinger og ny teknologi, bruk av nye plattformer m.m. vil kunne endre virksomheters behandling av personopplysninger. Idrettslagets internkontroll for behandling av personopplysninger skal derfor jevnlig revideres.

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 ansatte og medlemmer.

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 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.

Denne delen inkluderer rapporter, sjekklister, logg mv. Den kontrollerende delen kan betraktes som et sikkerhetsnett som bidrar til at styringsdokumentene 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

2.4.1 Personopplysning

Personopplysninger er enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»), som er lagret elektronisk eller er systematisert på papir, f.eks. medlemslister, lagslister og påmeldingslister. En identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator som f.eks. et navn, fødselsnummer, alder, adresse eller e-postadresse.

2.4.2 Særlige kategorier av personopplysninger / sensitive personopplysninger

Behandling av enkelte type personopplysninger defineres som «særlige kategorier av personopplysninger» eller «sensitive» personopplysninger. Dette omfatter opplysninger om:

- rasemessig eller etnisk opprinnelse,
- politisk, filosofisk eller religiøs oppfatning/overbevisning,
- fagforeningsmedlemskap,
- helseforhold,
- seksuell orientering, og
- genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person

Behandling av slike opplysninger er som hovedregel forbudt, med mindre et av vilkårene for slik behandling etter personvernforordningen art. 9 er innfridd. Et slikt vilkår er samtykke. Dette innebærer at idrettslaget kunne få samtykke til å f.eks. å behandle opplysninger om en utøves helsetilstand i forbindelse med kontroller, undersøkelser, tester i regi av idrettslaget. Tilsvarende vil et medlem gjennom samtykke kunne gi idrettslaget adgang til å behandle helseopplysninger om f.eks. allergier, eller opplysninger om religiøs overbevisning, til bruk for organisering av arrangementer og turer der det skal serveres mat og/eller drikke.

2.4.3 Behandling av personopplysninger

Med behandling av personopplysninger forstås enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

Definisjonen av behandling av personopplysninger er vid og dekker i prinsippet all bruk av personopplysninger uavhengig av hvilken teknologi som brukes.

2.4.4 Behandlingsansvarlig

Behandlingsansvarlig er den som bestemmer formålet med behandlingen og hvilke hjelpemidler som skal brukes. Det er idrettslaget som er behandlingsansvarlig for behandling av personopplysninger. Ansvaret skal ivaretas av den daglige ledelsen i idrettslaget. I idrettslag uten daglig ledelse er styret ansvarlig. Utføringen av behandlingen kan settes bort til for eksempel en ekstern part («databehandler»), men ansvaret kan ikke delegeres bort.

2.4.5 Databehandler

Med databehandler forstås en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige. Det kan for eksempel være et selskap idrettslaget benytter til en IT-løsning, HR- eller lagringstjeneste eller lignende.

Databehandler er undergitt behandlingsansvarliges instrukser, og kan ikke behandle opplysninger utenfor instruksen.

Det presiseres at en databehandler er en ekstern part eller et organisasjonsledd utenfor den behandlingsansvarliges organisasjonsledd. Det vil si at den behandlingsansvarliges egne medarbeidere ikke er dennes databehandlere. Det samme gjelder personer som utfører oppdrag og/eller utvikler løsninger på vegne av den behandlingsansvarlige, så fremt dette ikke omfatter behandling av personopplysninger.

2.4.6 Felles behandlingsansvar

Felles behandlingsansvar foreligger dersom to eller flere behandlingsansvarlige i fellesskap fastsetter formålene med (hvorfor) og midlene for (hvordan) behandlingen.

Forutsetningen for at det kan foreligge et felles behandlingsansvar, er at hver av partene i utgangspunktet har eller kan ha et selvstendig behandlingsansvar for den aktuelle behandlingen. Dersom behandlingens formål og midler fastsettes av en av de behandlingsansvarlige ved at den andre aktøren kun retter seg etter instruksjonen, vil det ikke foreligge et felles behandlingsansvar.

Formålet og midlene for behandlingen må være fastsatt i fellesskap. Hvilket formål den enkelte behandler personopplysninger for, og hvorvidt dette er det samme formålet som den/de andre er vurderingens kjerne. At flere behandlingsansvarlige hver for seg har tatt beslutninger som medfører at de behandler personopplysninger på en måte som helt eller delvis er sammenfallende, medfører ikke automatisk at det foreligger felles behandlingsansvar.

Der det foreligger et felles behandleransvar skal det utarbeides en avtale/ordning som regulerer ansvar og forpliktelser mellom aktørene som til sammen har et felles behandleransvar. Det felles behandleransvaret som idrettslaget er en del av, er beskrevet nærmere under punkt 3.1.3.

2.4.7 Behandlingsgrunnlag

Behandling av personopplysninger er som utgangpunkt ikke tillatt med mindre det foreligger et gyldig behandlingsgrunnlag, jf. personvernforordningen art. 6 - 9.

Behandlingsgrunnlag kan inndeles i tre hovedkategorier; et gyldig samtykke fra den enkelte, hjemmel i lov for behandlingen og oppfyllelse av et nødvendighetskriterium. Eksempel på nødvendighetskriterium kan være nødvendigheten av å oppfylle en kontrakt (ansettelseskontrakt) eller hvis den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse. Et annet eksempel kan være at behandlingen er nødvendig for at den behandlingsansvarlige eller tredjepersoner som opplysningene kan utleveres til kan ivareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen. Behandlingen kan også være nødvendig for å utføre en oppgave i allmennhetens interesse.

De fleste opplysninger om personer som er engasjert i idrettslag, kan sies å være opplysninger som er nødvendige for å oppfylle medlemskapet eller for at den enkelte skal kunne delta som utøver, eller å utføre oppgaver for idrettslaget som ansatt, oppdragstaker eller frivillig..

For barn under 15 år må i tillegg foresatte varsles om at den enkelte har meldt seg inn i idrettslaget og hvilke opplysninger som lagres om det enkelte barn.

2.4.8 Samtykke

Med samtykke fra den registrerte forstås enhver frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende. For barn under 15 år må slikt samtykke gis av foresatte.

Et samtykke skal kunne trekkes tilbake, like enkelt som det avgis. Hvis et samtykke trekkes tilbake skal behandling som ikke lenger er nødvendig opphøre, og registrerte opplysninger slettes i tråd med idrettslagets sletterutiner, med mindre idrettslaget har grunnlag for å fortsette behandlingen.

2.4.9 Tredjeland

Med tredjeland menes alle land utenfor EØS.

2.4.10 Overføring

I denne forstand menes overføring av personopplysninger all utlevering av personopplysninger, kopi eller overføring via et nettverk, eller all utlevering av personopplysninger, ut av idrettslagets virksomhet. Der slik overføring skjer ut av EU og EØS vil idrettslaget som overfører opplysningene vil være eksportør av personopplysningene. Dette kan typisk være tilfellet ved deltakelse i internasjonale konkurranser og/eller bruk av IT-løsninger som lagrer data utenfor EU og EØS.

3. Behandling av personopplysninger i idrettslaget

3.1 Ansvarsplassering – flyt personopplysninger

3.1.1 Behandleransvar

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

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, samt de retningslinjer og rutiner som følger av internkontrollsystemets del I-III.

3.1.2 Idrettslaget som Databehandler

~~[MERKNAD: Dette gjelder bare dersom idrettslaget behandler personopplysninger på vegne av f. eks. kommunen, f. eks. ved rapporteringer om deltakelse på arrangementer som kommunen arrangerer m.m.]~~

~~Selv om idrettslaget primært behandler personopplysninger som behandlingsansvarlig, kan idrettslaget utføre behandlingsaktiviteter der de opptrer som databehandler. Dette gjelder for eksempel i forbindelse med tilrettelegging av aktivitet i samarbeid med kommunen og eventuelt andre.~~

~~Der idrettslaget opptrer som databehandler er det inngått databehandleravtale med behandlingsansvarlig.~~

3.1.3 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 tilgjengeliggjøres via idrettens felles informasjonssystemer. Ansvaret for å administrere Idrettens sentrale database har idretten lagt til NIF.

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 ansatte og andre. Rutinene er basert på strategien som fremkommer av dette dokumentet.

Det er utarbeidet to sett med rutiner:

a) For behandling av ansattdata, og data om frivillige og oppdragstakere. 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

[**MERKNAD:** ~~Dette skjemaet fylles ut dersom idrettslaget eksempelvis bruker informasjonssystemer (utover de som er felles for idretten)~~]

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
MyKid	MyKid	Se betingelser	
Visma	Visma Net	Se betingelser	

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 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.

~~[**MERKNAD:** Her må idrettslaget konkludere med risikonivået forbundet med sine informasjonssystemer]~~

~~[Forslag til konklusjon:]~~ Idrettslaget 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. En vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer. Det kan tas høyde for bruk av ny teknologi og tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i.

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 Protection Impact Assessment – DPIA).

Det er derfor to steg i en vurdering av personvernkonsekvenser:

1. Om det må foretas en vurdering av personvernkonsekvensene ved en enkelt behandling
2. En faktisk vurdering av personvernkonsekvensene ved en behandling som har høy risiko for den registrerte

Disse to steg gjenfinnes i de to neste punkter i dokumentet.

5.3 Er behandlingen av en slik art som krever vurdering av personvernkonsekvensene

Personvernforordningen oppstiller i art. 35 typer behandling som alltid bør anses som høy risiko:

- en systematisk og omfattende vurdering av personlige aspekter ved fysiske personer som er basert på automatisert behandling, herunder profilering, og som danner grunnlag for avgjørelser som har rettsvirkning for den fysiske personen eller på lignende måte i betydelig grad påvirker den fysiske personen,
- behandling i stor skala av særlige kategorier av opplysninger som nevnt i artikkel 9 nr. 1 («sensitive personopplysninger»), eller av personopplysninger om straffedommer og straffbare forhold som nevnt i artikkel 10,
- eller er en systematisk overvåking i stor skala av et offentlig tilgjengelig område.

Idrettslaget skal selv vurdere i hvilket omfang de foretar behandlinger som omfattes av disse vilkårene, og som derfor bør anses å være av høy risiko.

Momenter utover kategoriene som direkte er oppstilt over vil være for eksempel:

- Flyt av data mellom systemer
- Tilgangsrutiner
- Om det er større mengder av personopplysninger med høy beskyttelsesverdig
- Sikkerhetstiltak

Det kan, selv om behandlingen isolert sett ikke oppfyller kriteriene for høy risiko, være anbefalt å foreta en vurdering av IT-løsninger av sentral viktighet for behandlingen.

5.4 Behandling i idrettslaget som krever vurdering av personvernkonsekvenser

~~[Dersom en etter idrettslagets vurdering kommer til at det foreligger høy risiko, og at DPIA derfor er påkrevet. Det er behandlingsansvarlig selv som må ta det avgjørende valget om det skal foretas en vurdering av personvernkonsekvenser. Dersom det konkluderes med at dette ikke er nødvendig bør dette påpekes her.]~~

~~[Forslag-Etter idrettslagets vurdering foreligger det ikke risiko som gjør DPIA påkrevet.]~~

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.

Idrettslaget har gjort en overordnet vurdering, jf. punktet over, og finner at det foretas følgende behandlinger av høy risiko:

~~[fyll inn aktuelle behandlinger]~~

5.4.1 MyKid og Visma

~~5.4.2 [behandling]~~

~~[Oppsummering av konsekvensvurdering (DPIA) og berørte systemer]~~

~~5.5 Overordnet risikoanalyse over behandlingen av personopplysninger idrettslaget~~

~~[**MERKNAD:** Når dokumentasjon er på plass og man ser helheten, er det aktuelt å innta en overordnet risikoanalyse av behandlingen som foretas samlet.]~~

~~[Forslag - risikoen anses lav for idrettslaget overordnet og samlet sett]~~

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

Ansatte i idrettslaget, herunder oppdragstakere, 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.

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

Idrettslagets ledelse har det overordnede ansvaret for å sørge for at andre enn ansatte som utfører oppgaver som innebærer behandling av personopplysninger på deres vegne har satt seg inn i de retningslinjer som gjelder for vedkommendes 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 nærmeste leder, idrettslagets ledelse, 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 ansatte og 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

~~[Redegjørelse for den fysiske og funksjonelle sammensetningen av informasjonssystemene, hvem som kan gjøre endringer i dette, og hvordan. Forslag nedenfor]~~

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

- Daglig leder, sportslig leder, leder IFO, nestleder av klubben og leder klubben
- ~~eller andre ansatte 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 oppmenn som håndterer opplysninger om utøvere og støttepersonell knytte til det enkelte lag/gruppe.]~~

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 dette dokumentet 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

7.1 Vedlegg 1; Kartlegging av behandling av personopplysninger i idrettslaget
7.2 Vedlegg 2; Databehandleravtale
7.3 Vedlegg 3; Risikovurdering av aktuelle systemer
7.4 Vedlegg 4; Rutiner og mal for behandling av opplysninger om ansatte, frivillige og andre oppdragstakere
7.5 Vedlegg 5; Rutiner og mal for behandling av medlemsdata
7.6 Vedlegg 6; Ordning for felles behandlingsansvar

Behandling av personopplysninger

Del III – kontrollerende aktiviteter

November 2019

Innholdsfortegnelse

8. Innledning

I den kontrollerende delen av idrettslagets internkontroll for behandling av personopplysninger skal det dokumenteres hvordan idrettslaget faktisk etterlever utarbeidede rutiner for behandling av personopplysninger.

Det er arbeidsutvalget (AU) v/styreleder som har ansvaret for gjennomføring av årlig revisjon og oppdatering.

9. Håndtering av uønskede hendelser (avvik)

9.1 Avvikshåndtering

Ansatte, tillitsvalgte, frivillige og eventuelt andre tilknyttet idrettslaget som oppdager uønskede hendelser (avvik) på personvern og informasjonssikkerhet hos idrettslaget skal umiddelbart rapportere om dette til styreleder/ ev. daglig leder (Sikkerhetsansvarlig).

Sikkerhetsansvarlig / behandlingsansvarlig skal umiddelbart vurdere om hendelsen må meldes til Datatilsynet innen 72 timer iht. personvernregelverkets bestemmelser, og eventuelt iverksette lovpålagt melding innen fristen. Dersom hendelsen gjelder personopplysninger omfattet av det felles behandlingsansvaret med øvrige organisasjonsledd i NIF (ref. internkontrollsystemets Del I – policy) skal varslingen koordineres med NIF.

Håndtering av uønskede hendelser skal gjennomgås i møte mellom sikkerhetsansvarlig og behandlingsansvarlig ved behov. I møtet skal det besluttes eventuelle rutinemessige eller tekniske tiltak for å forhindre at uønskede hendelser gjentar seg. Dersom det skulle være behov, kan idrettslaget henvende seg til NIF- IT for anbefalinger.

9.2 Når skal avvik meldes?

Det er behandlingsansvarlig, idrettslagets administrative leder, som har ansvaret for å melde et avvik til Datatilsynet. Meldingen skal være skriftlig, men Datatilsynet kan varsles først på telefon dersom det er viktig at Datatilsynet blir raskt kjent med avviket. Eksempelvis dersom avviket kan medføre at Datatilsynet blir varslet av andre aktører om det samme. Informasjonen kan også gis lagvis.

Det er en *uautorisert utlevering* som skal meldes til Datatilsynet innen 72 timer. En uautorisert utlevering av personopplysninger er når personopplysninger idrettslaget har behandlingsansvaret for befinner seg utenfor idrettslagets kontroll. Utleveringen kan være tilsiktet eller utilsiktet.
Merk; det har skjedd en utlevering selv om det er uklart om noen har fått opplysningene i hende.

9.2.1 Eksempler på uautorisert utlevering

- <u>Forsendelsesfeil</u>

a) Personopplysninger er sendt til feil mottaker per post eller per e-post.
b) Digitale forsendelser som avslører andres e-postadresser i en kontekst hvor mottakeren skal beskyttes.
c) Forsendelser til riktig mottaker, men som ved en feil også inneholder personopplysninger om andre.
d) Postforsendelse hvor innholdet mangler eller innholdet er der, men hvor konvolutten er revet opp.

- <u>Hacking eller datainnbrudd</u>

Hacking eller datainnbrudd har resultert i at personopplysninger er hentet ut av idrettslagets datasystem, eller det er *sannsynlig* at dette har skjedd. Eksempelvis at en tredjepart har fått tilgang til idrettslagets ansatt- eller medlemsregister.

- Snoking gjennomført av egne ansatte/tillitsvalgte

Snoking i personopplysninger gjennomført av egne ansatte/tillitsvalgte betraktes å være en uautorisert utlevering dersom vedkommende har ervervet opplysninger til egne private formål. Det samme gjelder der handlingen er utført av andre som utfører oppgaver for idrettslaget.

- Mangler ved tilgangsstyring

Mangelfull tilgangsstyring har resultert i at uvedkommende har fått tilgang til beskyttelsesverdig informasjon.

- Feilpublisering på internett

Publisering av feil personer på internett, eksempelvis manglende anonymisering av personer.

- Fysisk innbrudd

Digitale og/eller papirdokumenter med personopplysninger kommet på avveie.

9.3 Hva skal en avviksmelding inneholde?

En avviksmelding til Datatilsynet skal inneholde;

- Beskrivelse av avviket

a) Hva har skjedd?
b) Hvor skjedde det?
c) Hvordan oppstod avviket?

- Konsekvenser

Utredning av mulige konsekvenser for de som har fått sine personopplysninger utlevert.

- Tiltak

Gi en beskrivelse av iverksatte og planlagte tiltak for å forhindre at avviket skal skje igjen og hva som er gjort for å redusere avvikets potensielle skadevirkning.

- Informasjon

Gi en forklaring på hvorvidt de berørte har blitt informert om den uautoriserte utleveringen, eventuelt hvorfor de ikke har blitt informert.

9.4 Hvordan melde avvik?

De som oppdager avvik fra rutiner, skal rapportere om dette i avviksskjema (se vedlegg 1) som sendes til sikkerhetsansvarlig umiddelbart. Avviket skal umiddelbart drøftes i møte mellom relevant personell slik at frist for melding av avvik på 72 timer overholdes.

Det er sikkerhetsansvarlig, etter samråd med behandlingsansvarlig (administrativ leder), som beslutter om avviket skal meldes Datatilsynet.

Se under for mer informasjon om melding av avvik;

https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/melde-avvik-til-datatilsynet/

10. Egenkontroll

En gang pr. år, i løpet av 4. kvartal, skal rutiner og tekniske tiltak beskrevet i idrettslagets internkontroll for behandling av personopplysninger gjennomgås for å bekrefte at de fungerer etter hensikten.

Følgende punkter vil danne grunnlag for årlige revisjon og oppdatering:

- Er idrettslagets mål og strategi for behandling av personopplysninger den samme, og blir disse målene nådd?
- Er det endringer i relevant regelverket eller andre rammefaktorer som gjør at idrettslagets behandlinger av personopplysninger må endres?
- Har risikobildet endret seg?
- Er utarbeidede rutiner for behandling av personopplysninger kjent og funksjonelle for bruker?
- Blir rutinene fulgt?
- Har idrettslaget endret behandlingen av personopplysninger siden forrige kontroll?
- Gjør idrettslaget bruk av nye databehandlere og har vi sørget for at databehandleravtale er på plass?

Eventuelle endringer vil normalt kreve endringer i tidligere utarbeidet dokumentasjon. Det er sikkerhetsansvarlig som har ansvaret for gjennomføring av egenkontroll, herunder gjennomføring av stikkprøver, og skrive rapport. Se vedlegg 2 for mal rapport.

Det bør gjennomføres årlige stikkprøver av at rutinene følges internt. Det skal sjekkes at underleverandører følger databehandleravtalene. Sikkerhetsansvarlig er ansvarlig for å gjennomføre egenkontrollen og dokumentere resultatet.

Idrettslaget må selv finne en egnet måte å gjennomføre stikkprøver dette på. En metode som passer til type organisasjon og mengde/type opplysninger som behandles.

11. Ledelsens gjennomgang - informasjonssikkerhet

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

Ved ledelsens gjennomgang deltar behandlingsansvarlig, sikkerhetsansvarlig og eventuelt andre i idrettslaget ledelsen måtte utpeke.

Praktisk organisering av gjennomgangen, utarbeidelse av rapport samt iverksetting av eventuelle tiltak, er sikkerhetsansvarliges ansvar.

Ved gjennomgang av informasjonssystemet skal bl.a. følgende vurderes:

a) Resultater fra sikkerhetsrevisjoner og kontroller utført av offentlig myndighet.

b) Endringer med betydning for drift av informasjonssystemet eller for informasjonssikkerheten, herunder:

    - Endringer i offentlige sikkerhetskrav.
    - Endringer i de personopplysninger virksomheten skal behandle.
    - Endringer i trusselbildet som bl.a. beskrevet i rapport fra utførte risikovurderinger.

c) Om informasjonssystemet bør endres, eksempelvis som følge av ønske om ny funksjonalitet.

d) Overordnet behandling av alvorlige hendelser og avvik.

12. Vedlegg

12.1 Vedlegg 1; Avviksrapport
12.2 Vedlegg 2; Mal rapport egenerklæring
5.3 Vedlegg 3; Taushetserklæring

Taushetserklæring

Jeg forplikter meg herved til ikke å bruke, åpenbare, utlevere eller på annen måte gjøre tilgjengelig for uvedkommende informasjon om data og skjermingsverdig informasjon, personopplysninger, eller annen informasjon som uvedkommende ikke skal få kjennskap, til som jeg har fått kunnskap om i mitt arbeid ved Skiold.

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

Jeg har lest de lovbestemmelser som er anført på de neste sidene av denne erklæring. Jeg er dermed klar over straffelovens kapittel 21 samt markedsføringslovens § 28 og § 29. Brudd på disse bestemmelsene kan medføre straffeansvar, oppsigelse eller avskjed.

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

Drammen ..../....-2019

Sted Dato

.....

Underskrift

.....

Navn i blokkbokstaver

Ordning for felles behandleransvar

Samarbeidsordning for felles behandleransvar

13. Parter i ordningen om felles behandleransvar

Norges idrettsforbund (NIF) og organisasjonsledd i NIF (samlet benevnt som Partene) skal samarbeide ved behandlingen av personopplysninger knyttet til administreringen av medlemmer.

Partene forplikter seg til å etterleve det til enhver tid gjeldende «Personvernregelverket», herunder blant annet Personopplysningsloven av 2018, Generell Personvernsforordning; Europaparlaments- og rådsforordning (EU) 2016/679 («personvernforordningen»), kommunikasjonsvernforordningen og all annen gjeldende norsk lov og forskrift som regulerer behandling av personopplysninger, herunder lov som implementerer og gjennomfører GDPR, samt sektorlovgivning og forskrifter.

Hver av Partene har selvstendig ansvar for å oppfylle sin rolle og sine plikter som behandlingsansvarlig i henhold til Personvernregelverket.

Samarbeidet inngår som en del av Partenes internkontrollsystem for behandling av personopplysninger og følger som en del av idrettens organisasjonsstruktur ved behandling av opplysninger om medlemmer og frivillige.

14. Roller og personell i samarbeidet

14.1 Representanter

Partenes representanter er

- for idrettslagene: daglig leder for de som har det og styreleder for de som ikke har dette
- for særforbundene: generalsekretær
- for NIF: generalsekretær

Ansvaret kan delegeres innad i organisasjonsleddet. Organisasjonsleddets utpekte ansvarlige vil fungere som kontaktpersoner ved henvendelser vedrøvende denne ordningen. Dersom ansvaret er delegert skal dette fremgå i dokumentasjonen til organisasjonsleddets internkontrollsystem.

14.2 Roller og behandlingsgrunnlag etter GDPR

Behandlingen av personopplysninger i forbindelse med administrering av den organiserte idretten medfører at Partene vil ha et felles behandlingsansvar i henhold til Personvernregelverket for personopplysninger som deles mellom Partene. Personopplysningene som omfattes av det felles behandleransvaret er opplysningene som fremkommer av Idrettens sentrale database (ISD), og som tilgjengeliggjøres i systemene Klubbadmin og Sportsadmin (heretter i fellesskap «idrettens felles informasjonssystemer»). ISD inneholder informasjon om alle som er medlem i norsk idrett. Denne databasen administreres og driftes av NIF på vegne alle organisasjonsleddene i norsk idrett.

Personopplysningene som fremkommer av databasen, omfatter:

- informasjon om den registrerte 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;

Organisasjonsspesifikke opplysninger som et særforbund eller et idrettslag registrerer om medlemmer, frivillige eller oppdragstakere som går utover listede opplysninger, inngår ikke i Partenes felles behandlingsansvar.

Partene vil hver for seg og samlet sørge for samsvar og etterlevelse av Personvernregelverket.

Partene skal ha tilstrekkelig behandlingsgrunnlag for egen behandling av Personopplysninger. Dersom Personopplysninger skal overføres til ISD for felles behandling skal Partenes behandlingsgrunnlag så langt som mulig gi grunnlag for at også øvrige Parter kan tre inn som behandlingsansvarlig for den felles behandlingen.

14.3 Ansvar for oppfyllelse av informasjonsplikten

NIF påtar seg på vegne av partene hovedansvaret for å gi tilstrekkelig informasjon til de registrerte, herunder informasjon om overføring av Personopplysninger til ISD og formålet med dette, samt hvorvidt det vil foreligge et felles behandlingsgrunnlag og hovedtrekkene i denne ordningen. Informasjonen skal gis i henhold til kravene som er oppstilt i Personvernregelverket, herunder artikkel 13 og 14, slik at de Registrerte blir i stand til å ivareta sine rettigheter. Særforbund og idrettslag vil på sin side bidra til å oppfyllelse av disse kravene ved å gjøre tilgjengelig informasjon om hovedtrekkene i denne ordningen, og henvise til NIF for fullstendig oppfyllelse av informasjonsplikten.

14.4 Ansvar for tekniske og organisatoriske sikkerhetstiltak

Partene bekrefter ved å ta i bruk idrettens felles informasjonssystemer, herunder ISD, å ha iverksatt tekniske og organisatoriske sikkerhetstiltak for å beskytte Personopplysninger mot tap, misbruk og uautorisert endring for den delen av behandlingen av Personopplysningene de har et særskilt ansvar for.

For NIFs organisasjonsledd gjelder dette behandlingen av personopplysninger om egne registrerte frem til disse opplysningene overføres til ISD. NIF har hovedansvaret for at tekniske og organisatoriske sikkerhetstiltak er på plass for Personopplysningene når disse er registrert i ISD. Slike tiltak er iverksatt for å oppnå et sikkerhetsnivå som er egnet ut i fra risikoen ved behandlingen av Personopplysningene, hensyntatt kostnadene ved gjennomføringen. For organisatoriske tiltak er partene ansvarlige for å påse at tilgangen til opplysningene i ISD er begrenset til personer med tjenstlig behov i sin organisasjon.

14.5 Bruk av databehandler

Partene har i fellesskap besluttet at det administrative og praktiske ansvaret for drift og administrering av idrettens felles informasjonssystemer skal ligge hos NIF. NIF er med dette gitt ansvaret for å engasjere de nødvendige databehandlere for at informasjonssystemene skal fungere for alle partene.

NIF forvalter databehandleravtalene for idrettens informasjonssystemer, og skal påse at alle databehandlere som tas i bruk har påtatt seg de samme forpliktelsene de har for NIF overfor de andre partene. Det skal fremgå av Databehandleravtalen hvilke(n) person(er) i NIF som forvalter den felles instruksjonsretten. En oversikt over databehandlere som benyttes for idrettens felles informasjonssystemer skal til enhver tid være tilgjengelig på NIFs hjemmesider, i ISD eller i NIFs personvernerklæring. Databehandleravtalene skal gjøres tilgjengelig for organisasjonsleddene på forespørsel.

For å ivareta personvernforordningens krav skal partenes kontroll med, og instruksrett overfor, databehandlerne utøves gjennom et felles kontaktpunkt lagt til NIF. Håndteringen av slik kommunikasjon er i NIF lagt til leder for forretningsutvikling og fornying.

Generelt: Bruk av databehandlere
Partene står, utenfor den behandlingen som er omfattet av det felles behandlingsansvaret, fritt til å benytte andre databehandlere. For øvrig gjelder idrettens generelle regler og retningslinjer ved valg av databehandler.

14.6 Ansvar overfor den registrerte

Partene har et felles ansvar overfor de registrerte.

I det daglige har NIF ansvaret for å oppfylle den registrertes rettigheter, herunder rettighetene til innsyn, retting og sletting. Der en registrert velger å forholde seg til idrettslag eller særforbund skal det aktuelle organisasjonsleddet forestå håndteringen av den registrertes henvendelse i samarbeid med NIF.

14.7 Tvisteløsningsmekanismer

Uenighet om forståelsen eller gjennomføringen av denne ordningen, skal primært søkes løst gjennom forhandlinger mellom Partenes kontaktpersoner.

I konfliktsituasjoner skal Partene kalle inn til et samarbeidsmøte, der Partene skal søke å finne omforente løsninger så langt det er mulig. Partene er enige om at samarbeidsmøte skal avholdes minimum to ganger før eventuell 3. part involveres.

14.8 Solidaransvaret

De registrerte kan, i henhold til personvernforordningen artikkel 26 (3), forholde seg til hvilken som helst av partene uavhengig av denne ordningen. Dette gjelder blant annet retten til å klage inn for tilsynsmyndighetene og benytte rettsmidler mot hvilken som helst av partene. Partene er for slike forhold solidarisk ansvarlige, herunder i tilfeller der erstatning til den registrerte blir tilkjent jf. artikkel 82 (4).

I det tilfellet at det er mulig å spore bruddet på personvernregelverket til en av Partene, kan erstatning for brudd på personvernregelverket kreves dekket av den av Partene som er skyld i bruddet. En Part vil alltid være ansvarlig for brudd som begås ved bruk av en Databehandler som organisasjonsleddet selv har utpekt.

14.9 Ordningens varighet

Denne ordningen gjelder så lenge partene er tilknyttet NIF og benytter idrettens felles informasjonssystemer.

14.10 Lovvalg og verneting

Ordningen er underlagt norsk rett og Partene vedtar Oslo tingrett som verneting. Dette gjelder også etter opphør av avtalen.

Melding om avvik – Datatilsynet

1. Innledning

Behandlingsansvarlig (idrettslagets øverste leder) har ansvaret for at Datatilsynet varsles dersom det har skjedd brudd på personopplysningssikkerheten. Avviket skal meldes Datatilsynet uten ugrunnet opphold når det er mulig, og senest 72 timer etter å ha fått kjennskap til avviket. Se GDPR art 33.

Et avvik kan meldes via Altinn.no, se link under. Datatilsynet har også plikt (per september 2018) til å motta melding om avvik uten bruk av Altinn.no. Eksempelvis per e-post, eller ordinær post. Merk at e-post kan være en sårbar kommunikasjonskanal.

Dersom avviket gjelder bruk av idrettens fellessystemer sendes kopi av avviksmeldingen til varslinger@idrettsforbundet.no.

Kontaktpunkter Datatilsynet;

https://www.datatilsynet.no/om-datatilsynet/kontakt-oss/

Merk også at informasjon kan gis i flere omganger dersom idrettslaget ikke har full oversikt over hendelsen.

Datatilsynet er underlagt offentlighetsloven, slik all kommunikasjon er i utgangspunktet offentlig tilgjengelig. Dersom man ønsker unntak fra offentlighetsloven må dette anføres.

https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/melde-avvik-til-datatilsynet/

2. Innsender

Organisasjonsnummer	983885144
Navn (Idrettslag)	SBK Skiol
Adresse	Schwartzgate 2
Postnummer og sted	3043 Drammen
Er innsender behandlingsansvarlig eller databehandler?	????????????????

3. Beskrivelse av avviket

Forklar årsaken til avviket	Eksempelvis hackerangrep
Tidsrommet for avviket	
Når bla avviket oppdaget?	
Hvor mange personvern kan være berørt av avviket?	
Gi en kort forklar av hva som har skjedd	
Beskriv hva slags opplysninger som har blitt berørt av avviket	
Hvilken relasjon har idrettslaget til de personer som har blitt berørt?	Eksempelvis medlemsopplysninger? Eller i administrasjonen?
Hvor befinner opplysningene seg etter avviket?	

4. Konsekvenser

Beskriv mulige konsekvenser avviket har medført for de berørte personene?	

5. Tiltak

Hvilke tiltak er gjort og planlagt for å forhindre at hendelsen skal skje igjen	
Beskriv hva som er gjort for å redusere eventuelle skadevirkninger	

6. Informasjon

Har de berørte personene blitt informert om avviket?	Ja / Nei
Forklar hvordan de har blitt informert	

7. Kontaktinformasjon

Hvem kan kontaktes for å få mer informasjon?	
Oppgi idrettslagets generelle postadresse dersom det ikke skal kommuniseres med en direkte person	

8. Alternativ kontaktperson

Hvis tredjepart (rådgiver) skal kontaktes	

DATABEHANDLERAVTALER

Denne databehandleravtalen «**Databehandleravtalen**» gjelder der Databehandler behandler Personopplysninger på vegne av Behandlingsansvarlig (Idrettslaget). Databehandleravtalen er inngått mellom:

SBK Skiold	og	MyKid
org.nr. 983885144		org.nr. 997780973
omtales som «**Behandlingsansvarlig**»		omtales som «**Databehandler**»;

Behandlingsansvarlig og Databehandler omtales samlet som «**Partene**», og hver for seg som **«Part»**.

Databehandleravtalen gjelder fra signering og er på vegne av Partene signert av:

_____	_____
Sted/Dato	Sted/Dato
For SBK Skiold	For MyKid
_____	_____
[Navn]	[Navn]

Partene har blitt enige om følgende for å oppnå tilstrekkelige garantier med hensyn til beskyttelse av personvern og andre grunnleggende rettigheter for de som får sine personopplysninger, som spesifisert i denne Avtalen, overført fra Behandlingsansvarlig til Databehandler. Se vedlegg for personvernerklæring

Se vedlegg for personvernerklæring fra MyKid, **HER**

Denne databehandleravtalen «**Databehandleravtalen**» gjelder der Databehandler behandler Personopplysninger på vegne av Behandlingsansvarlig (Idrettslaget). Databehandleravtalen er inngått mellom:

SBK Skiold	og	Visma
org.nr. 983885144		
omtales som «**Behandlingsansvarlig**»		omtales som «**Databehandler**»;

Behandlingsansvarlig og Databehandler omtales samlet som «**Partene**», og hver for seg som **«Part»**.

Databehandleravtalen gjelder fra signering og er på vegne av Partene signert av:

_____	_____
Sted/Dato	Sted/Dato
For SBK Skiold	For Visma
_____	_____
[Navn]	[Navn]

Partene har blitt enige om følgende for å oppnå tilstrekkelige garantier med hensyn til beskyttelse av personvern og andre grunnleggende rettigheter for de som får sine personopplysninger, som spesifisert i denne Avtalen, overført fra Behandlingsansvarlig til Databehandler. Se vedlegg for personvernerklæring

Se vedlegg for personvernerklæring fra Visma, **HER**

15. Definisjoner

Databehandleravtalen skal forstås på bakgrunn av følgende definisjoner:

Personvernregelverket:	Med Personvernregelverket forstås: a) Personopplysningsloven av 2000; Gjennomføring og implementering av EUs personverndirektiv (95/46/EF) og kommunikasjonsverndirektiv (2002/58/EF) i norsk lov; b) GDPR (Generell Personvernsforordning); Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016. Med mindre annet er særskilt angitt skal enhver henvisning til GDPR forstås som en henvisning til gjennomføring og implementering av GDPR i norsk lov; c) Kommunikasjonsvernforordningen; forslag til Europaparlaments- og rådsforordning 2017/0003 (forordning om personvern og elektronisk kommunikasjon), dersom og fra den tid forordningen vedtas og gjennomføres i norsk lov; d) All annen gjeldende norsk lov og forskrift som regulerer Databehandlers Behandling av Personopplysninger, herunder lov som implementerer og gjennomfører GDPR, samt sektorlovgivning.
Personopplysning:	Enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»), jf. GDPR art. 4 (1).
Behandling:	Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring, jf. GDPR art. 4 (2).
Brudd på Personopplysningssikkerheten:	Et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte Behandlet. Slikt Brudd på Personopplysningssikkerheten er ikke avhengig av at det har skjedd et brudd på Personvernregelverket, jf. GDPR art. 4 (12).
Behandlingsansvarlig:	Fysisk eller juridisk person som alene eller sammen med andre bestemmer formålet med Behandlingen av personopplysninger og hvilke midler som skal benyttes, jf. GDPR art. 4 (7).

Databehandler:	Fysisk eller juridisk person som Behandler personopplysninger på vegne av den behandlingsansvarlige, jf. GDPR art. 4 (8).
Underleverandør:	Fysisk eller juridisk person som Databehandler engasjerer, intensjonelt eller ikke, for å utføre behandlingsaktiviteter på vegne av Behandlingsansvarlig.
Tredjestat eller internasjonal organisasjon:	Overføring av personopplysninger som Behandles eller skal Behandles etter overføring til en tredjestat eller til en internasjonal organisasjon som ikke sikrer et tilstrekkelig beskyttelsesnivå uten at det foreligger et overføringsgrunnlag, for eksempel land utenfor EØS-området.

16. Formål

Denne Databehandleravtalen har som formål å regulere Databehandlers Behandling av Personopplysninger på vegne av Behandlingsansvarlig i forbindelse med avtalen om tjenesten Databehandleravtalen gjelder for Hovedavtalen. Databehandleravtalen skal sikre at Personopplysninger behandles i samsvar med kravene i den til enhver tid gjeldende personvernlovgivning (Personvernregelverket, som definert ovenfor) og at Personopplysninger kun behandles i henhold til denne Databehandleravtalen og ved dokumenterte instruksjoner fra Behandlingsansvarlige.

Databehandlers behandling av Personopplysninger skal kun omfatte den Behandling som er nødvendig for at Databehandler skal kunne gjennomføre Hovedavtalen med den Behandlingsansvarlige.

Databehandleravtalen kan revideres ved behov for tilpasninger til preseptorisk lovgivning, tolkninger av GDPR og Personvernregelverket (slik dette er definert over). Alle endringer i denne Databehandleravtalen skal avtales og nedfelles skriftlig.

17. Databehandlers Behandling av Personopplysninger

17.1 Behandlingens art

Databehandler vil Behandle og ha tilgang til Personopplysninger i forbindelse med MyKid og Visma av MyKid og Visma i henhold til Hovedavtalen for den Behandlingsansvarlige.

I forbindelse med oppfyllelsen av Hovedavtalen vil Databehandler kunne foreta Behandlinger i form av tilgang, organisering, strukturering, tilpasning, gjenfinning, konvertering, lagring, flytting, konsultering og tilintetgjøring. Slik Behandling vil kun foregå i henhold til bestemmelsene i Databehandleravtalen og Hovedavtalen og kun etter instruksjoner fra Behandlingsansvarlig.

Behandlingen vil hovedsakelig foregå i gjennom support i leverandørs systemer etc.

Databehandler skal ikke Behandle Personopplysninger i større omfang enn det som er nødvendig for å oppfylle Hovedavtalen med den Behandlingsansvarlige. Annen Behandling kan kun skje unntaksvis og ved kortvarige tilfeller, og kun under instruksjon fra Behandlingsansvarlig.

Dersom Databehandler er i tvil om Behandlingen av enkelte Personopplysninger er nødvendig, eller innenfor Hovedavtalens omfang, skal det straks, og før Personopplysninger behandles, konsulteres med Behandlingsansvarlig.

Under ingen omstendigheter er Databehandler berettiget til å Behandle Personopplysninger eller andre data som tilhører Behandlingsansvarlig for egne formål, og utover de formål som fremkommer av Databehandleravtalen eller Hovedavtalen.

Dersom Databehandler er pålagt videre Behandling gjennom lov eller tilsvarende pålegg fra offentlig myndighet forplikter Databehandler seg til å varsle Behandlingsansvarlig, samt sikre videre konfidensialitet og sikkerhet som ilegges gjennom Databehandleravtalen.

17.2 Kategorier av Personopplysninger og datasubjekter

I forbindelse med oppfyllelse av Hovedavtalen, og avhengig av Databehandlers leveranse, kan Databehandler komme i kontakt med Personopplysninger under den Behandlingsansvarliges ansvar.

Dette omfatter blant annet opplysninger om navn, telefonnummer, epost-adresse, kommunikasjonsdata, dokumenter og tekst, finansiell informasjon, sensitive opplysninger, adferdsdata, bilder.

Disse personopplysningene vil gjelde ansatte hos den Behandlingsansvarlige.

17.3 Geografisk området for Behandlingen

Databehandler skal kun Behandle personopplysninger innenfor EØS-området. Databehandler har ikke rett til å overføre Personopplysninger til et tredjeland eller internasjonal organisasjon, herunder ut av EØS-området, uten at det er nødvendig for å oppfylle Hovedavtalen, kun etter spesifikt skriftlig samtykke fra Behandlingsansvarlig og under forsikring om at det foreligger tilstrekkelig overføringsgrunnlag i henhold til GDPR art. 44-49.

All slik eventuell overførsel skal møte de krav til sikkerhet og vern av de registrertes rettigheter som følger av Databehandleravtale og i henhold til Personvernregelverket.

17.4 Bruk av Underleverandører

Bruk av Underleverandører for Behandling av Personopplysninger skal forhåndsgodkjennes av Behandlingsansvarlig. Dersom Databehandler ønsker å benytte seg av en Underleverandør som ikke på forhånd er godkjent av Behandlingsansvarlig, eller ønsker å bytte ut en godkjent Underleverandør, skal Behandlingsansvarlig varsles og gis anledning til å motsette seg dette. Under ingen omstendighet skal Databehandler ta i bruk Underleverandører uten å på forhånd ha innhentet skriftlig samtykke fra Behandlingsansvarlig.

Behandlingsansvarlig har rett til 3 (tre) måneders varsel dersom Databehandler ønsker å bytte en Underleverandør. Behandlingsansvarlig har rett til å motsette seg Databehandlers bruk eller bytte av Underleverandør der det foreligger saklig grunn, og skal gi Databehandler skriftlig beskjed innen 30 dager etter informasjon om slikt bytte av Underleverandør er gitt.

Dersom Databehandler ikke godtgjør at Behandlingsansvarliges motsettelse er ubegrunnet, og i tillegg fastholder sitt bytte av Underleverandør, har Behandlingsansvarlig rett til å heve Hovedavtalen med Databehandler med umiddelbar virkning.

Databehandlers Underleverandører for Behandling av Personopplysninger skal være bundet av de samme avtalemessige og lovmessige forpliktelser som Databehandler er underlagt i henhold til denne Databehandleravtalen, gjennom egne databehandleravtaler. Det er Databehandlers ansvar å påse at databehandleravtalene med Underleverandører er utarbeidet i henhold til de til enhver tid gjeldende regler i Personvernsregelverket, samt underlagt Databehandlers rettigheter og plikter etter Hovedavtalen og denne Databehandleravtalen.

Databehandler skal ha en skriftlig avtale med alle Underleverandører som engasjeres i forbindelse med Behandling av Personopplysninger.

Behandlingsansvarlig har rett til å få tilgang til opplysninger om Underleverandører til enhver tid, herunder innhold i databehandleravtale og informasjon om tekniske og organisatoriske tiltak Underleverandør har iverksatt for å etterleve Personvernregelverket.

18. Forpliktelser som Databehandler

18.1 Bistand til Behandlingsansvarlig

Databehandler forplikter seg, uten kompensasjon eller annet vederlag, til å:

a. Behandle Personopplysninger kun etter instrukser fra Behandlingsansvarlig og kun i henhold til det som er formålet med Hovedavtalen;
b. Treffe alle tiltak som er nødvendig for å ivareta sikkerheten tatt i betraktning den Behandlingen som utføres på vegne av Behandlingsansvarlig, samt regelmessig og på eget tiltak foreta analyse og testing av slike forholdsmessige sikkerhetstiltak, herunder vurdere deres effektivitet;
c. Bistå Behandlingsansvarlig med å sikre overholdelse av dennes forpliktelser til å ivareta Personopplysningssikkerhet og vurdere personvernkonsekvenser, idet det tas hensyn til Behandlingens art og den informasjonen som er tilgjengelig for Databehandleren;
d. Bistå Behandlingsansvarlig, idet det tas hensyn til Behandlingens art og i den grad det er mulig, med å oppfylle dennes plikt til å oppfylle anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter og som eventuelt er nærmere spesifisert i Hovedavtalen. Kommer slik anmodning fra den registrerte direkte til Databehandler skal denne oversendes Behandlingsansvarlig som regulert i Databehandleravtalens varslingsbestemmelse;
e. Bistå Behandlingsansvarlig med å løse avvikssituasjoner i samarbeid med Behandlingsansvarlig, såfremt avviket nødvendiggjør dette og i henhold til avvikshåndtering som regulert i Databehandleravtalen;
f. Etter Behandlingsansvarliges instruks, slette eller tilbakelevere alle Personopplysninger og slette eventuelle eksisterende kopier, med mindre det foreligger en lovpålagt plikt til å fortsette lagringen;
g. Umiddelbart varsle Behandlingsansvarlig hvis en instruksjon er i strid med Personvernregelverket;
h. Sikre at alle som Behandler Personopplysninger har forpliktet seg til fortrolighet eller er underlagt en egnet lovfestet taushetsplikt, samt at kun slike autoriserte personer som har et nødvendig behov for å oppfylle Hovedavtalen har eller får tilgang til Personopplysninger.

18.2 Tekniske og organisatoriske tiltak

~~[MERKNAD: Idrettslaget må stille krav til sikkerhetsnivå hos databehandler. Sikkerhetsnivået kan ikke være svakere enn hos idrettslaget. Merk at behandlingsansvarlig har ansvaret også når dataene ligger hos databehandler.]~~

Databehandler skal sørge for at det foreligger tekniske og organisatoriske tiltak for å sikre og påvise at Behandlingen utføres i samsvar med Personvernregelverket, denne Databehandleravtalen og for å sikre bistand til oppfyllelsen av rettighetene til den registrerte.

Databehandler skal før oppstart, og deretter årlig, fremlegge dokumentasjon på Behandlingen som skjer på vegne av Behandlingsansvarlig. Denne dokumentasjonen skal inneholde:

i. Kategorier av behandlingsaktiviteter;
ii. Bruken av Underleverandører;
iii. Overføringer ut av EØS-området;
iv. En generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene;

Databehandler skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen ved Behandlingen. Disse egnede tekniske og organisatoriske tiltakene skal også sikre og påvise at Behandlingen utføres i samsvar med denne Databehandleravtalen. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov. Databehandler kan ta hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, men vurderingen skal gjøres i tråd med den vurderingen som skal gjennomføres etter GDPR art. 32.

Slike tekniske og organisatoriske tiltak skal som et minimum inkludere, men er ikke begrenset til, tiltak for å:

a) pseudonymisere og kryptere personopplysninger der det er relevant;

b) Sikre evnen til vedvarende fortrolighet, integritet, tilgjengelighet og robusthet i behandlingssystemene og –tjenestene;

c) Sikre evnen til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse;

d) Ivareta en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er;

e) Forhindre at datasystemer som Behandler Personopplysninger blir brukt eller gir tilgang til Personopplysninger til personer som ikke er autorisert, inkludert tilgang til å lese, kopiere, endre eller slette Personopplysninger uten autorisasjon.

Databehandler er forpliktet til å iverksette ovennevnte tiltak, og om nødvendig oppdatere tiltak, slik at de tekniske og organisatoriske tiltakene til enhver tid er i henhold til Personvernregelverket, herunder slik de er oppstilt i GDRP artikler 28 og 32.

18.3 Varsling

Databehandler skal varsle Behandlingsansvarlig uten ugrunnet opphold om:

i. En instruksjon fra Behandlingsansvarlig strider mot Personvernregelverket;
ii. Et pålegg om utlevering av Personopplysninger fra offentlig myndighet, med unntak av der slik varsling er forbudt;
iii. Et brudd eller mulig brudd på sikkerheten som kan føre til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte Behandlet, herunder som et minimum der det foreligger Brudd på Personopplysningssikkerheten;
iv. Henvendelser fra en registrert slik at Behandlingsansvarlig kan respondere, og uten at Databehandler selv responderer uten å ha fått eksplisitt tillatelse til å håndtere henvendelsen selv.

Databehandler plikter å gi tilstrekkelig bistand til Behandlingsansvarlig i etterkant av eventuelt varsel til Datatilsynet om Brudd på Personopplysningssikkerheten eller til den registrerte ved henvendelser. Enhver varsling eller henvendelse til Datatilsynet skal skje gjennom Behandlingsansvarlig. Dersom det er nødvendig for å avklare omfanget av Brudd på Personopplysningssikkerheten, skal Databehandler bistå Behandlingsansvarlig i samarbeidet med Datatilsynet.

Umiddelbart etter å ha gitt varsel om et Brudd på Personopplysningssikkerheten skal Databehandler gi ytterligere beskrivelse til Behandlingsansvarlig om:

i. Alle relevante forhold knyttet til bruddet som Databehandler har kjennskap til, herunder hva bruddet består av, kategorier og volum på Personopplysninger. Forhold knyttet til avviket som Databehandler først får kjennskap til etter slik varsling skal meddeles Behandlingsansvarlig straks Databehandler får slik kjennskap;
ii. Hvilke tiltak som er iverksatt eller foreslått iverksatt for å hindre konsekvenser og begrense omfanget av Bruddet på Personopplysningssikkerheten.

Videre skal Databehandler bistå Behandlingsansvarlig med å vurdere personvernkonsekvenser ved slikt Brudd på Personopplysningssikkerheten.

Databehandler plikter å varsle Behandlingsansvarlig dersom det avdekkes at Databehandler ikke etterlever, eller ser at det blir vanskelig å etterleve, kravene som følger av Personvernregelverket og denne Databehandleravtalen, uavhengig av årsak. I et slikt tilfelle kan Behandlingsansvarlig suspendere overføring og videre Behandling av Personopplysninger hos Databehandler.

19. Ansvar for Behandlingen

Databehandler er ansvarlig for et hvert Brudd på Personopplysningssikkerheten, samt enhver skade som forårsakes som følge av Behandlingen, og som er oppstått som følge av manglende etterlevelse av forpliktelsene etter Personvernregelverket, Databehandleravtalen eller som følge av at Databehandler har opptrådt utenfor eller i strid med lovlige instrukser fra Behandlingsansvarlig.

Databehandler skal være unntatt fra ansvar dersom de kan godtgjøre at de på ingen måte er ansvarlig for hendelsen som førte til skaden.

Ansvar for materiell eller ikke-materiell skade på en eller flere registrerte skal reguleres i henhold til vilkår og føringer gitt i GDPR art. 82. Behandlingsansvarlig skal ha rett til å kontrollere prosessen ovenfor den registrerte dersom den registrerte aksepterer dette.

Ingen ansvarsbegrensning skal gjelde dersom skadevoldende handling er foretatt ved forsettlig eller grov uaktsomhet av noen av Partene.

Hvis Databehandler bryter Personvernregelverket ved å fastsette formålene med og midlene for behandlingen, skal Databehandleren anses for å være en Behandlingsansvarlig med hensyn til nevnte Behandling.

Dersom Underleverandør ikke oppfyller sine forpliktelser med hensyn til Personvernregelverket og denne Databehandleravtalen, skal Databehandler ha fullt ansvar for Underleverandørs oppfyllelse eller manglende oppfyllelse av forpliktelser.

20. Sikkerhetsrevisjon

Databehandler er forpliktet til å gi Behandlingsansvarlig tilstrekkelig tilgang og dokumentasjon til all informasjon som er nødvendig for å påvise etterlevelse av forpliktelsene fastsatt i Databehandleravtalen, og for å kunne gjennomføre sikkerhetsrevisjoner. Slike sikkerhetsrevisjoner omfatter, men er ikke begrenset til, stedlig inspeksjon og evaluering av systemer, organisering og sikkerhetstiltak, samt bruk av Underleverandører.

Behandlingsansvarlig er berettiget til å oppnevne en uavhengig inspektør til å gjennomføre sikkerhetsrevisjoner av Databehandlers etterlevelse av denne Databehandleravtalen, Hovedavtalen og Personregelverket. Inspektøren skal være underlagt konfidensialitetsforpliktelser og Databehandler kan ikke motsette seg Behandlingsansvarliges valg av inspektør uten rimelig grunn. Databehandler har, dersom mulig, krav på en (1) ukes varsel for slik sikkerhetsrevisjon.

Behandlingsansvarlig er ikke ansvarlig for Databehandlers kostnader i forbindelse med sikkerhetsrevisjoner.

21. Taushetsplikt

Informasjon som Partene blir kjent med i forbindelse med denne Databehandleravtalen og gjennomføringen av den skal behandles konfidensielt, og ikke gjøres tilgjengelig for utenforstående uten samtykke fra den annen Part. Taushetsplikten er ikke til hinder for at opplysningene brukes når de er alminnelig kjent eller alminnelig tilgjengelig andre steder.

Partene skal ta nødvendige forholdsregler for å sikre at uvedkommende ikke får innsyn i eller kan bli kjent med konfidensiell informasjon.

Taushetsplikten gjelder Partenes ansatte, Underleverandører som handler på Partenes vegne i forbindelse med gjennomføring av denne Databehandleravtalen og Hovedavtalen. Partene kan bare overføre taushetsbelagt informasjon til slike Underleverandører og tredjeparter i den utstrekning dette er nødvendig for gjennomføring av denne Databehandleravtalen og Hovedavtalen, forutsatt at disse pålegges plikt om konfidensialitet tilsvarende dette punkt.

Taushetsplikten gjelder også etter at denne Databehandleravtalen og Hovedavtalen er opphørt. Ansatte eller andre som fratrer sin tjeneste hos en av Partene, skal pålegges taushetsplikt også etter fratredelsen om forhold som nevnt ovenfor. Taushetsplikten opphører 10 (ti) år etter opphøret av denne Databehandleravtalen og Hovedavtalen, med mindre annet følger av lov eller forskrift.

22. Varighet og avslutning av Behandlingen

Databehandleravtalen gjelder så lenge Databehandler Behandler eller har tilgang til Personopplysninger på vegne av Behandlingsansvarlig, og Behandlingsansvarlig er å anse som Behandlingsansvarlig for Personopplysningene.

Databehandlerens Behandling av Personopplysninger for Behandlingsansvarlig skal avsluttes ved opphør av Hovedavtalen. Ved avslutning av Behandlingen av Personopplysninger skal Databehandler enten tilbakelevere eller slette alle eventuelle Personopplysninger, etter den Behandlingsansvarliges instruks, så fremt videre Behandling ikke er lovpålagt. Slik lovpålagt videre Behandling må varsles om til Behandlingsansvarlig.

Databehandler har ikke krav på vederlag for kostnader knyttet til sletting, oppbevaring eller lovpålagt videre Behandling av Personopplysninger.

All tilgang til Behandlingsansvarliges systemer skal ved avslutning av Behandlingen stenges for Databehandler og dennes personell. Databehandler er forpliktet til å bistå Behandlingsansvarlig med gjennomføringen av dette.

Databehandler skal skriftlig dokumentere at sletting og/eller destruksjon er foretatt innen rimelig tid etter avtalens opphør.

Databehandler er ikke berettiget til vederlag for Behandling som nevnt under dette punkt.

23. Lovvalg og verneting

Denne Databehandleravtalen er underlagt norsk rett og Partene aksepterer Behandlingsansvarliges hjemting som verneting. Dette gjelder også etter avslutning av Hovedavtalen.

* * *

PERSONVERNERKLÆRING FOR SBK SKIOLD

Siste versjon: 08-11-2019

Denne personvernerklæringen er ment å gi informasjon om hvordan og hvorfor SBK Skiold, heretter «idrettslaget», samler inn og behandler dine personopplysninger. Denne personvernerklæringen retter seg mot medlemmer, herunder mindreårige medlemmers foresatte og frivillige (herunder tillitsvalgte, trenere, oppmenn og andre frivillige).

Idrettslaget ved øverste leder er behandlingsansvarlig for opplysninger som samles inn og behandles av idrettslaget. Det daglige ansvaret er delegert til Daglig leder. Personvernerklæringen som følger under inneholder informasjon du har krav på når det samles inn personopplysninger gjennom idrettslaget og generell informasjon om hvordan vi behandler dine personopplysninger.

Dine personopplysninger behandles i overensstemmelse med det til enhver tid gjeldende personvernregelverk.

1. Vår bruk av personopplysninger

Idrettslaget samler inn og behandler personopplysninger for å kunne oppfylle våre plikter overfor medlemmer og frivillige, for å administrere idretten, og oppfylle de krav som stilles til oss som ansvarlig for behandling av personopplysninger.

Personopplysninger vi behandler hentes i all hovedsak fra den registrerte selv, men i noen tilfeller henter vi også opplysninger fra tredjepart. Det kan være kilder fra offentlige registre eller myndigheter. Vi vil alltid varsle om slik innhenting i forkant, med mindre innsamling av opplysningene er lovpålagt, varsling er umulig eller svært vanskelig, eller det er opplagt at den registrerte allerede har informasjon om innhentingen.

2. Utlevering av personopplysninger - Overføring av personopplysninger til tredjepart

Dine personopplysninger behandles konfidensielt og det er bare de i idrettslaget som har et tjenstlig behov for å behandle personopplysningene som vil ha tilgang til dem. Som hovedregel vil dine personopplysninger ikke deles med noen utenfor idrettslaget.

Opplysninger om deg vil lagres i Idrettens sentrale database, hvor Norges idrettsforbund og dets organisasjonsledd har tilgang. Du kan selv administrere hvilke opplysninger som er tilgjengelig i databasen ved å logge deg inn på «Min Idrett». For behandlingen av personopplysningene som inngår i idrettens sentrale database foreligger det et felles behandlingsansvar mellom NIF og dets organisasjonsledd. For å sikre en trygg behandling av personopplysningene, har organene opprettet en ordning for å sikre etterlevelse av personvernregelverket. Denne ordningen er nærmere beskrevet i NIFs personvernerklæring.

Personopplysninger kan bli gjort tilgjengelig for tredjepart som hjelper oss med å drifte idrettslaget, eksempelvis den tekniske driften av våre IT- og regnskapssystemer.

Når tredjeparter gis tilgang til personopplysninger på denne måten inngås databehandleravtaler slik at vi sikrer at tredjepartene overholder våre krav til behandling av personopplysninger og gjeldende lovgivning.

Det kan også være at vi deler dine personopplysninger med våre samarbeidspartnere dersom du har gitt ditt samtykke til dette, eller vi er forpliktet til dette etter lov (eksempelvis Skatteetaten og NAV).

Du kan alltid føle deg trygg når du oppgir dine personopplysninger til oss.

3. Hvilke personopplysninger behandler vi?

Vi behandler kun personopplysninger som er nødvendige for å administrere medlemskap eller frivillighet i idrettslaget. Opplysninger vi registrerer er i hovedsak begrenset til navn, fødselsdato, telefonnummer, epostadresse, postadresse, statsborgerskap, kjønn, idrettens personID, familietilknytninger, lisenser/forsikringer, overganger, kurs/kompetanse, roller og verv, om politiattest er fremvist, at medlems- og treningsavgift er betalt og tilknytning til konkurranseaktivitet. Vi kan også behandle personopplysninger som ditt bilde. Dersom det er nødvendig vil også andre personopplysninger kunne registreres, og vi vil i slike tilfeller informere om dette.

I forbindelse med deltakelse i arrangementer der det vil bli servert mat, kan vi samle inn informasjon om allergier og matpreferanser. På trening eller under arrangementer vil det også kunne behandles opplysninger om treningsresultater, prestasjon og progresjon. I noen tilfeller vil slike opplysninger være å regne som særlige kategorier av opplysninger og vi vil kun behandle slike opplysninger i den utstrekning vi har tillatelse til det.

Informasjonskapsler

Vi benytter informasjonskapsler (cookies) på vår hjemmeside. En informasjonskapsel er en liten tekstfil og vår nettside vil alltid spørre din nettleser om å få lagre kapselen på din maskin. Vi gjør dette for at vi skal huske dine handlinger, preferanser og hvor ofte du har vært på vår hjemmeside. Dette gjør det igjen mulig for oss å gi deg som bruker bedre tilgang til ulike funksjoner. Videre bruker vi også informasjonskapsler på sidene våre for at vi skal kunne føre statistikk over hvor ofte vårt nettsted generelt brukes.

Du kan administrere innstillingene for informasjonskapsler i din nettleser.

4. Grunnlag for behandlingen

Det rettslige grunnlaget for behandlingen av personopplysningene i idrettslaget er først og fremst medlemsavtalen, men vi henter også inn ditt samtykke for noen av våre behandlinger. Hjemmel i lov kan også være et grunnlag, eksempelvis ved rapportering til Skatteetaten.

For enkelte organisatoriske og administrative oppgaver, utover det som er strengt nødvendig for administrering av medlemskap, kan vi behandle dine personopplysninger på bakgrunn av vår berettigede interesse og for statistiske formål. Vi fører blant annet statistikk for å ha oversikt over aktivitet i de enkelte idrettene, noe vi også rapporterer videre til særforbund og NIF. Når vi behandler personopplysninger på andre grunnlag enn medlemsavtalen eller ditt samtykke har vi foretatt en vurdering av om formålet med bruken av dine personopplysninger er forholdsmessig sammenlignet med ditt personvern. Våre berettigede interesser omfatter muligheten til å allokere ressurser etter behov, utvikle tilbud til medlemmene og en god administrering av idretten innenfor idrettslaget.

Ved bruk av samtykke som behandlingsgrunnlag vil vi gjøre bruk av vårt eget samtykkeformular slik at vi får innhentet et gyldig samtykke. Dette gjelder blant annet for de spesielle kategoriene av personopplysninger som vi i noen tilfeller behandler.

5. Lagring av personopplysningene og sletting

~~[**MERKNAD:** Det følgende avsnittet må benyttes der idrettslaget benytter andre tjenester enn idrettens felles informasjonssystemer:~~

~~Personopplysningene du registrerer lagres på en server hos [sett inn navn på leverandører] som er lokalisert [sett inn land], og som i dag anses for å være en trygg og tilfredsstillende lagring av dine opplysninger. Grunnen til dette er at alle EU stater er forpliktet til å møte kravene i personvernforordningen (GDPR) og dermed sikrer den registrerte et minimum av personvern [NB: forutsatt at alle serverne er lokalisert i EU].~~

Lagring av opplysninger som idretten har et felles ansvar for (se punkt 2 ovenfor) håndteres av NIF på vegne av idretten. Ytterligere informasjon om dette finnes i personvernerklæringen på www.nif.no.

Idrettslaget sletter dine personopplysninger uten ugrunnet opphold når de ikke lenger er nødvendige for formålet de ble samlet inn for. Dette betyr at vi eksempelvis sletter opplysninger samlet inn for å administrere ditt medlemskap i det du ikke lenger er medlem i Idrettslaget. Opplysninger om medlemmets foresatt vil slettes på samme tidspunkt, med mindre den foresatte er registrert i tilknytning til et annet medlem eller dersom vedkommende har en rolle som frivillig.

Dersom du trekker tilbake samtykket som ligger til grunn for behandlingen av opplysninger, eller du gjør en innsigelse mot behandlingen og det ikke finnes mer tungtveiende berettigede grunner for behandlingen, vil vi slette dine opplysninger.

Merk at det kan være lovkrav som gjør at vi likevel er forpliktet til å oppbevare dine personopplysninger i en viss periode. Andre opplysninger vil og være nødvendig å beholde av hensyn til forsikringsavtaler. Vi har egne konkrete sletterutiner per behandlingsaktivitet.

6. Dine rettigheter som registrert

Som registrert har du flere rettigheter knyttet til vår behandling av dine personopplysninger. Her får du informasjon om hvilke disse er, og hvordan du kan utøve disse rettighetene overfor idrettslaget i forbindelse med behandling av dine personopplysninger. Dersom du anmoder oss om å benytte deg av en eller flere av disse rettighetene vil vi innrette oss etter anmodningen innen en måned fra den ble avgitt. Anmodningene kan rettes til Daglig leder.

Innsyn: Du kan sende oss en forespørsel om innsyn i vår behandling av dine personopplysninger. I de fleste tilfeller vil opplysningene vi har lagret om deg vises ved innlogging på MinIdrett.

Retting: Dersom du mener opplysningene vi har lagret om deg ikke er riktige (f. eks. epostadresse eller verv) kan du når som helst be om at vi retter dette. Du kan også foreta rettinger ved innlogging på MinIdrett.

Protestere: Dersom du ikke ønsker at vi skal behandle dine personopplysninger, kan du protestere mot behandlingen.

Trekke ditt samtykke: Du kan når som helst trekke tilbake ditt samtykke om at vi kan lagre og behandle dine personopplysninger, der slikt samtykke er avgitt. Dette gjelder eksempelvis for behandlingen av helseopplysninger eller publisering av bilder.

Sletting: Dersom du protesterer mot behandlingen av dine personopplysninger, eller du trekker tilbake ditt samtykke, vil informasjon som vi har lagret om deg vil bli slettet under den forutsetning at vi ikke har annet grunnlag for å beholde disse. Dersom du ønsker dine personopplysninger slettet under andre omstendigheter, kan du enkelt rette en henvendelse til oss om dette.

Dataportabilitet: Du har rett til å kreve dataportabilitet for opplysninger om deg selv som du har gitt til idrettslaget, og som har behandlingsgrunnlag i samtykke eller avtale. Dette omfatter eksempelvis opplysninger som administreres under ditt medlemskap eller bilder. Dersom du ønsker å utøve din rett til portabilitet vil de aktuelle opplysningene om deg bli sendt deg, eller en tredjepart som du utpeker så fremt dette er teknisk mulig.

Rett til å begrense behandlingen: Dersom du ønsker at vi skal begrense behandlingen av dine personopplysninger, kan du be om dette.

Rett til å klage til en tilsynsmyndighet: Dersom du mener vår behandling av dine personopplysninger skulle være i strid med personvernforordningen, eller personvernregelverket for øvrig, har du rett til å klage på dette til Datatilsynet. Klager kan leveres på deres nettsider; www.datatilsynet.no.

Dersom det er ønskelig med mer informasjon om vår behandling av personopplysninger, kan vi kontaktes på tlf 32836433, e-post leder@skiold.net eller morten@skiold.net.

7. Endringer i vår personvernerklæringen

Vi kan endre på personvernerklæringen fra tid til annen etter eget skjønn. Når vi gjør endringer i denne erklæringen vil vi endre revisjonsdato øverst på denne siden, og en modifisert personvernerklæring har virkning fra revisjonsdatoen. Vi oppfordrer deg til å lese gjennom denne personvernerklæringen for å være informert om hvordan vi beskytter din informasjon.