Behandling av personopplysninger

Del I – Styrende aktiviteter

Innholdsfortegnelse

1. Innledning

1.1 Nærmere om Norges studentidrettsforbund

Norges studentidrettsforbunds formål er å fremme studentenes idretts- og friluftsliv i Norge, og representere idretten internasjonalt.

Norges studentidrettsforbund behandler personopplysninger om ansatte. Opplysningene omfatter eksempelvis navn, telefonnummer, adresse, bankkontonummer, fødsels- og personnummer, informasjon som arbeidsgiver er pålagt å registrere.

Generelt sett behandler Norges studentidrettsforbund følgende personopplysninger:

- Navn, fødselsdato, statsborgerskap, kjønn, bilde, adresse, telefonnummer, epostadresse og personID;
- kurs/kompetanse;
- roller og verv;
- Klubbtilhørighet
- tilknytning til konkurranseaktivitet;

Norges studentidrettsforbund kan også samle inn og behandle helseopplysninger relatert til aktiviteter som forbundet arrangerer. Ved kurs, arrangementer, turer o.l. i regi av Norges studentidrettsforbund 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. Norges studentidrettsforbund må ha samtykke for å samle inn og behandle slike opplysninger.

Norges studentidrettsforbund har få eller ingen medlemmer eller deltagere under 15 år. For behandling av deres personopplysninger må de foresatte samtykke til registrering av personopplysninger. I forbindelse med registrering av barn under 15 år, registreres det derfor også opplysninger om deres foresatte. Dette omfatter opplysninger i samme utstrekning som medlemmer.

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

Norges studentidrettsforbund skal behandle personopplysninger på en lovlig, rettferdig og transparent måte. Norges studentidrettsforbund har som mål å behandle så *få* opplysninger som mulig.

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

De overordnede målene med Norges studentidrettsforbunds behandling av personopplysninger er at disse kun skal innhentes og behandles i den grad dette er nødvendig for ivaretagelsen av Norges studentidrettsforbunds 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 Norges studentidrettsforbunds drift, allmenne tillit, og omdømme i det offentlige rom, ved å forebygge og begrense uønskede hendelser.

2.2 Personvern i Norges studentidrettsforbund

Norges studentidrettsforbunds håndtering av personopplysninger er basert på følgende personvernprinsipper:

- ✓ Behandling av personopplysninger skal baseres på at behandlingen er nødvendig for å håndtere medlemskapet eller vervet, Norges studentidrettsforbunds 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 Norges studentidrettsforbunds behandling av personopplysninger utføres i samsvar med personvernforordningen (internkontroll for behandling av personopplysninger). I dette ligger det også et krav til behandlingsansvarlig å dokumentere Norges studentidrettsforbunds 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 Norges studentidrettsforbunds internkontroll for behandling av personopplysninger.

Nye behandlinger og ny teknologi, bruk av nye plattformer m.m. vil kunne endre virksomheters behandling av personopplysninger. Norges studentidrettsforbunds 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 Norges studentidrettsforbunds internkontroll for behandling av personopplysninger også kunne legges frem for overordnede organisasjonsledd, Datatilsynet og Personvernnemnda ved behov, samt være tilgjengelig for Norges studentidrettsforbunds ansatte og medlemmer.

2.3.1 Styrende dokumentasjon

Styrende del av internkontroll for behandling av personopplysninger skal blant annet regulere Norges studentidrettsforbunds 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 Norges studentidrettsforbund.

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 Norges studentidrettsforbund.

Gjennomførende del er del II av internkontrollen i Norges studentidrettsforbund.

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 Norges studentidrettsforbund.

2.3.4 Informasjonskapsler

På vår sin nettside finnes ulike digitale annonser. Annonseplattformen leveres av Dynamic Elements Markets AS og deres underleverandør Adnuntius AS. Informasjon om bruken av annonser, lagres i informasjonskapsler på tilsvarende måte som ved bruk av våre nettsider. Informasjonskapselen slettes automatisk etter 30 dager og formålet er å kunne generere statistikk over besøk på annonseplattformen. Lagring og bruk av informasjonskapslene krever at den besøkende er informert og har akseptert dette. Du kan enkelt gå inn å godta/avslå bruk av informasjonskapsler på annonseplattformen her:

- *http://delivery.adnuntius.com/consent?noCookies=YES*
- *http://delivery.adnuntius.com/consent?noCookies=NO*

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 Norges studentidrettsforbund kunne få samtykke til å f.eks. å behandle opplysninger om en utøves helsetilstand i forbindelse med kontroller, undersøkelser, tester i regi av Norges studentidrettsforbund. Tilsvarende vil et medlem gjennom samtykke kunne gi Norges studentidrettsforbund 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 Norges studentidrettsforbund som er behandlingsansvarlig for behandling av personopplysninger. Ansvaret skal ivaretas av den daglige ledelsen i Norges studentidrettsforbund. 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 Norges studentidrettsforbund 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 Norges studentidrettsforbund 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 Norges studentidrettsforbund som ansatt, oppdragstaker eller frivillig..

For barn under 15 år må i tillegg foresatte varsles om at den enkelte har meldt seg inn i Norges studentidrettsforbund 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 Norges studentidrettsforbunds sletterutiner, med mindre Norges studentidrettsforbund 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 Norges studentidrettsforbunds virksomhet. Der slik overføring skjer ut av EU og EØS vil Norges studentidrettsforbund 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 Norges studentidrettsforbund

3.1 Ansvarsplassering – flyt personopplysninger

3.1.1 Behandleransvar

Norges studentidrettsforbund behandler en rekke personopplysninger om eksempelvis egne ansatte, styre og komiteer, medlemmer, deltagere på mesterskap, deltagere på kurs og konferanser etc. Formålet med behandling av personopplysninger i Norges studentidrettsforbund er primært administrering av medlemskap, aktiviteter, verv og ansettelsesforhold.

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

Norges studentidrettsforbunds 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 Norges studentidrettsforbund som Databehandler

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

Selv om Norges studentidrettsforbund primært behandler personopplysninger som behandlingsansvarlig, kan Norges studentidrettsforbund 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 Norges studentidrettsforbund opptrer som databehandler er det inngått databehandleravtale med behandlingsansvarlig.

3.1.3 Nærmere om Norges studentidrettsforbunds felles behandleransvar

Ved administrering av medlemsmassen, overordnet og på daglig basis, foreligger det et felles behandlingsansvar mellom Norges studentidrettsforbund, 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 Norges studentidrettsforbund 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 Norges studentidrettsforbund har et felles behandlingsansvar for omfatter opplysninger om medlemmer, tillitsvalgte og frivillige om blant annet;

- informasjon om personen, inkludert navn, fødselsdato, statsborgerskap, kjønn, adresse, telefonnummer, epostadresse og personID;
- kurs/kompetanse;
- roller og verv;
- Klubbtilhørighet
- tilknytning til konkurranseaktivitet.

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 Norges studentidrettsforbund 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 Norges studentidrettsforbunds egne databehandlere er listet nedenfor under punkt 4.

3.2 Felles rutiner for behandling av personopplysninger - Personvernombud

Norges studentidrettsforbund 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 deltakere på arrangement. 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 til rutiner for sikring av informasjon og personopplysninger i Norges studentidrettsforbund (Gjennomførende del).

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

- Ansvarsplassering i Norges studentidrettsforbund – ansvarlige avdelinger/roller for ulike hovedkategorier
- Overordnet og intern risikovurdering ved Norges studentidrettsforbunds behandling av personopplysninger
- Sikkerhetsmål, sikkerhetsstrategi og akseptkriterier (utover kap. 6)
- Sikkerhetsorganisasjon
- Fordeling av ansvar og roller internt i Norges studentidrettsforbund
- Rutiner for jevnlig ivaretagelse av Norges studentidrettsforbunds 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

Norges studentidrettsforbund 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
Erik Froseth	Thea	22.03.2019	
Sara Habberstad	Questback	01.05.2018	
Rune Sagør	MIND	02.08.2018	Microsoft(365) NORGE

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 Norges studentidrettsforbund 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. Norges studentidrettsforbund 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.

Norges studentidrettsforbund har konkludert med at risikonivået forbundet med sine informasjonssystemer er akseptabelt. Videre utredning rundt behandling av data på hjemmesiden bør allikevel vurderes

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 Norges studentidrettsforbund, 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.

Norges studentidrettsforbund 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 Norges studentidrettsforbund som krever vurdering av personvernkonsekvenser

Etter Norges studentidrettsforbunds 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.

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

5.5 Overordnet risikoanalyse over behandlingen av personopplysninger Norges studentidrettsforbund

Risikoen anses lav for Norges studentidrettsforbund overordnet og samlet sett.

6. Informasjonssikkerhet

6.1 Sikkerhetsmål

Det overordnede sikkerhetsmålet ved Norges studentidrettsforbunds behandling av personopplysninger er at all bruk av personopplysninger skal være i samsvar med innhentet samtykke og-/ eller annet legitimt 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 Norges studentidrettsforbund skal videre ivaretas slik dette er beskrevet i sikkerhetsmålene nedfelt i Håndbok for informasjonssikkerhet i idretten.

Målene skal understøtte og sikre Norges studentidrettsforbunds 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 Norges studentidrettsforbund, herunder oppdragstakere, og frivillige som utfører enkelte organisatoriske eller administrative funksjoner på Norges studentidrettsforbunds vegne har et medansvar for at informasjons- og personopplysningssikkerheten ivaretas i tråd med sikkerhetsmålene.

De ansatte i Norges studentidrettsforbund 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 Norges studentidrettsforbund.

Norges studentidrettsforbunds 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 vedkommende sitt 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, Norges studentidrettsforbunds 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 Norges studentidrettsforbund 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 Norges studentidrettsforbund som har tjenstlig behov for tilgang til Norges studentidrettsforbunds systemer, skal gis tilgang, og kun i den utstrekningen som er nødvendig for at den enkelte kan gjennomføre sine oppgaver.

6.6 Overordnet konfigurasjonskontroll

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

- Generalsekretær og andre ansatte med oppgaver knyttet til administrasjon av styremedlemmer, deltagere på arrangement og andre frivillige.

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

Det skal sikres at alle som gis tilgang til opplysninger i Norges studentidrettsforbunds 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