*Nedenfor finner du mal til bruk for utarbeidelse av IT-instruks til deres klubb. IT-instruksen skal utleveres (og leses!) av alle som gis tilgang til personopplysninger i klubben. Det betyr, at IT-instruksen skal utleveres til alle styremedlemmer, ansatte og frivillige. I henhold til personvern-reglene må alle som behandler personopplysninger sikre seg at slike opplysninger behandles sikkert og korrekt, slik at personopplysninger ikke misbrukes, kommer på avveie eller behandles feilaktig. For å sikre dette, er det et krav at man utdanner og instruerer sitt personale og relevante personer som får tilgang til personopplysninger om hvordan man skal behandle slike data. Det er også at krav om regelmessig oppfølging for å sikre at instruksen er kjent/overholdes. Derfor er det FIFs anbefaling, at klubben én gang i året sender IT-instruksen til ansatte, styremedlemmer og frivillige med beskjed om å gå gjennom instruksen, slik at de kjenner og følger reglene vedr. behandling av personopplysninger. De årlige utsendte e-postene må lagres, slik at klubben har dokumentasjon på at man faktisk har fulgt opp sin forpliktelse om regelmessig oppfølging. FIF vil også anbefale å inkludere signaturbekreftelsen til slutt i dette dokumentet. På denne måten kan dere dokumentere at styremedlemmer, ansatte og frivillige har mottatt og lest instruksen. Dette vil gi klubben ytterligere dokumentasjon for at man har gjort sitt beste for å overholde lovens krav om utdannelse og instruering.*

*En særlig utfordring for klubber, som i stor grad bruker frivillige til å utføre diverse oppgaver, er at personopplysninger i større eller mindre grad sendes ut av «klubbens IT-systemer», hvor klubben ikke lengre kan styre hva som skjer med dataene. Instruksen nedenfor forsøker å ta høyde for denne utfordringen, ved å instruere om hvordan data skal behandles utenfor klubbens IT-systemer. FIF vil imidlertid sterkt anbefale at klubber som bruker eller har mulighet til å anskaffe dokument-/samhandlingsløsninger, som f. eks. SharePoint, OneDrive eller liknende, deler dokumenter via slike løsninger. På den måten vil dere ha større kontroll på klubbens behandling av medlemmers, samarbeidspartneres og ansattes personopplysninger.*

*Malen nedenfor skal brukes slik at all tekst må gjennomleses for å sjekke at den passer i deres klubb. Hvis den ikke passer, retter dere teksten slik at den passer med forholdene hos dere. Alle tekster i firkantede parenteser og med kursiv [xxx] skal utfylles/endres av dere. Hvis den foreslåtte tekst passer i deres klubb, fjerner dere kun parentesene og kursiveringen av teksten. Hvis det er forhold som er relevante i deres klubb og som ikke er inkludert i malen, tilføyer dere nødvendig informasjon.* ***Toppteksten er kun til info og skal slettes.***

*----------------------------------------------------------------------------------------------*

**IT-instruks og instruks om behandling av personopplysninger for [sett inn klubbens navn]**

Gjeldende fra [sett inn dato]

**Generelt**

I denne IT-instruks finner du de regler som gjelder for bruken av [sett inn klubbens navn]s IT-systemer, samt bruken av de personopplysninger som klubben gir deg adgang til for utførelse av én eller flere oppgaver for klubben. Personopplysninger er all informasjon som sier noe om en gitt person. Begrepet er altså meget bredt og omfatter eksempelvis: navn, adresse, e-post, telefonnumre, medlemsnumre, men også ting som f.eks. klesstørrelse og resultater i en turnering.

[Sett inn klubbens navn] skal beskytte og verne om de personopplysninger vi får fra medlemmer, gjester, ansatte og samarbeidspartnere, slik at vi overholder de til enhver tid gjeldene personvern-regler. Derfor pålegger vi også alle som har adgang til personopplysninger i eller fra [sett inn klubbens navn] å følge de reglene som er angitt i denne instruks. Informasjon, inkludert personopplysninger, må ikke kopieres eller utleveres til personer som ikke har legitim adgang til disse.

**Datamaskiner, telefoner og annet som benyttes til å få tilgang til data**

Enhver enhet som gir tilgang til [sett inn klubbens navn]s data, skal være beskyttet av passord og/eller biometrisk sikring (fingeravtrykksløsning). Se mere om kravene til passord nedenfor. Du skal låse enheten når du forlater den. Enheten skal være beskyttet, slik at fornyet adgang skal etableres hvis enheten har vært inaktiv lengere enn 15 minutter (f. eks. via innstillinger for hvilemodus, skjermsparer ol.). Dette omfatter også private enheter som datamaskiner, telefoner og andre enheter som benyttes til å lese eller oppbevare informasjon fra klubben som inneholder personopplysninger.

**Oppbevaring av data/arkivering**

Fysiske data

Fysiske personopplysninger er opplysninger om personer i notatbøker, protokoller, papirutskrifter mv.

Generelt sett skal du når du behandler personopplysninger huske å rydde opp etter deg, hente utskrifter i skriveren ol., slik at uvedkommende ikke får tilgang til personopplysningene.

Sensitive personopplysninger skal beskyttes med en høyere grad av sikkerhet enn ikke sensitive personopplysninger, ettersom det kan få langt større konsekvenser for personen opplysningene gjelder hvis opplysningene kommer på avveie.

Har du sensitive personopplysninger, opplysninger om lovovertredelser eller straffedommer på trykte medier, skal disse være låst inne når du ikke benytter dem og når du forlater kontoret. I golfklubber vil dere normalt kun inneha sensitive personopplysninger om de ansatte i klubben, og disse skal kun deles med personer i klubben som har et tjenstlig behov for å se disse. Om dere innehar sensitive personopplysninger om andre enn ansatte, skal disse også håndteres som beskrevet ovenfor.

Elektroniske data

Elektroniske personopplysninger er opplysninger om personer i IT-systemer, på telefoner, på minnepinner og i annen elektronisk form.

Alle data skal lagres i programmer som er installert eller godkjent av [sett inn klubbens navn]. Du skal ikke selv, uten godkjenning, installere ny programvare eller laste ned programmer fra internett til bruk for å behandle, vise eller lagre [sett inn klubbens navn]s data. Dette betyr også at du ikke skal laste ned eller benytte andre fildelingstjenester, enn de [sett inn klubbens navn] har instruert deg om å benytte.

Datalagring lokalt

Personopplysninger, som oppbevares lokalt (i klubbens lokaler), skal oppbevares på enheter (server, NAS osv.), som er beskyttet med passord. Enhetene skal oppbevares i avlåst lokale. Det anbefales at lokalet er innbruddssikret.

Hvis det inngås serviceavtaler, så skal det inngås avtale med leverandøren om beskyttelse av data. Ved innbrudd/tyveri skal reglene for sikkerhetsbrudd følges, og styret/daglig leder skal varsles.

Datalagring på nett

Alle personopplysninger, som lagres på nett (f. eks. i skyløsninger), skal aksesseres via en sikker forbindelse. Dette skjer typisk via en nettleser som støtter https eller lignende kryptert adgang. Kan du ikke se om det er https som benyttes, ta kontakt leverandøren for å sikre at adgangen er kryptert.

Digitale data skal være beskyttet av samme grad av sikkerhet som fysiske data, og sensitive personopplysninger skal beskyttes i høyere grad enn ikke sensitive personopplysninger. Se ovenfor.Alle data skal oppbevares på en måte, slik at de kun deles med personer som har et tjenstlig behov for tilgang til dataene. Arkivering av data skal behandles på samme måte.

Ved arbeidsforholdets opphør skal dine arkiver gjøres tilgjengelige for ledelsen.

Du skal ikke oppbevare personopplysninger lokalt på din datamaskin, minnepinner eller lignende, hvor filer og personopplysninger utilsiktet kan bli slettet permanent, mistes eller komme uvedkommende i hende.

**Utlevering av personopplysninger**

Utlevering av personopplysninger er en behandling omfattet av personvernreglene. Medlems-opplysninger kan utleveres til andre medlemmer i klubben, når det har et saklig formål. Medlemsopplysninger kan publiseres på lukkede hjemmesider, men de må ikke offentliggjøres på offentlige tilgjengelige hjemmesider uten samtykke fra de aktuelle medlemmene. Når du utleverer personopplysninger innenfor klubben, skal du kun utlevere opplysninger som er relevante for oppgaven/personen du deler opplysningene med. Hvis du blir bedt om å utlevere telefonnumre på noen medlemmer, skal du ikke utlevere en liste som også inneholder e-post adresser.

Du skal vise varsomhet slik at du ikke distribuerer personopplysninger uberettiget, f.eks. ved ukritisk å videresende e-poster, som i seg selv eller i vedlagte filer inneholder personopplysninger som ikke skal komme uvedkommende i hende. Husk at kollegaer, styremedlemmer mfl. også kan være uvedkommende, særlig når du behandler sensitive personopplysninger.

Vær oppmerksom på at sponsorer/samarbeidspartnere er selvstendige juridiske enheter, slik at medlemsopplysninger ikke kan utleveres til disse uten samtykke.

**Brukernavn og passord**

Brukerkontoer og passord skal ikke deles.

Passord du benytter til klubbens IT-løsninger skal være forskjellige fra de passord du bruker privat. Passordene skal være på minst 8 tegn, og de skal inneholde store og små bokstaver, tall og spesialtegn. Du må ikke gi dine passord til andre, og du skal endre dine passord hvis du mistenker at de har kommet på avveie.

Passord til systemer som inneholder sensitive personopplysninger skal endres minimum hver 90. dag. I klubber vil det normalt kun være opplysninger om de ansatte i klubben som kan inneholde sensitive personopplysninger, i form av opplysninger om helseforhold og/eller fagforeningsmessig tilhørighet.

Når ansatte slutter, eller frivilliges funksjonsperiode avsluttes, skal alle deres tilganger til klubbens IT-systemer fjernes omgående.

**Sikkerhetsbrudd**

Ved ethvert brudd eller mistanke om brudd på sikkerheten, skal styret/daglig leder omgående varsles. Ledelsen skal iverksette tiltak i henhold til beredskapsplanen.

Du skal kontakte support/klubbens ledelse, hvis dine IT-enheter har virus eller oppfører seg unormalt. Du skal også kontakte support/klubbens ledelse, hvis du har mistanke om at antivirusprogrammet ikke virker korrekt.

Du skal være påpasselig ved mottagelse av e-post og filer fra mistenkelige avsendere, e-poster uten emneangivelse og øvrige mistenkelige henvendelser.

**Bruk av e-post**

Personopplysninger kan i utgangspunktet sendes på e-post (NB! Personopplysningslovens bestemmelser gjelder). Gjelder det sensitive personopplysninger (f. eks helseopplysninger vedr. en av klubbens ansatte eller medlemmer) og/eller fødselsnummer, må opplysningene sikres. Dette kan eksempelvis gjøres ved å lagre opplysningene i en fildelingsløsning, hvor adgang til innholdet krever adgangskode. Du kan så dele dokumentet med den/de som skal ha tilgang og sende en e-post med en lenke til dokumentet. Denne fremgangsmåten anbefales også i tilfeller hvor ikke sensitive personopplysninger om flere/mange skal deles.

Du skal med jevne mellomrom slette mottatte, sendte og andre lagrede e-poster som inneholder personopplysninger og som ikke skal arkiveres. Slettingen skal være permanent.

Hvis du bruker en privat e-postadresse for å sende og motta klubbens e-poster, skal du sikre deg at du har den nødvendige sikkerhet på denne e-post kontoen og datamaskinen/telefonen. Andre personer skal ikke ha tilgang til denne e-postkontoen, eksempelvis må du ikke dele den med din ektefelle/samboer.

Du bør unngå å lagre personopplysninger på din private datamaskin. Hvis du likevel har behov for å lagre personopplysninger på din private datamaskin, skal du sikre deg at opplysningene ikke er tilgjengelige for andre i din husstand, og at de slettes fra din datamaskin så snart du ikke lenger har behov for opplysningene.

Adgang til [sett inn klubbens navn]s administrasjonssystemer: [lønnssystemer, økonomisystemer mm.]:

Det er [klubbens ledelse, daglig leder, styreleder] som administrerer adgang til administrasjonssystemene. Adgangen til systemene skal løpende tilpasses, slik at det kun er personer med behov for adgang som rent faktisk har det. Ansatte, styremedlemmer og frivillige skal ha adgang til de personopplysninger de har bruk for til løsning av sin(e) oppgave(r), men ikke opplysninger utover dette. Blir du oppmerksom på at du kan se flere opplysninger enn du har bruk for, eller at du fortsatt har adgang etter at ditt verv eller ansettelsesforhold er avsluttet, skal du be om at din adgang til systemet endres/fjernes.

De personopplysninger som du gis adgang til skal kun anvendes i relasjon til din oppgave i [sett inn klubbens navn].

**Databehandling**

Informasjonssøkning

Det er ikke tillatt å søke etter personopplysninger som ikke er relevant for det arbeid du skal utføre.

Blir du oppmerksom på at du har adgang til data du ikke burde ha adgang til, skal du uten unødig opphold meddele dette til klubbens daglige ledelse.

Eksport/utsendelse av data

Det skal utvises omhu med hvilke personopplysninger som deles med andre. Reglene er som utgangspunkt følgende:

· Det skal kun utleveres personopplysninger som er nødvendige for å kunne utføre en spesifikk oppgave.

· Mottakeren skal gjøres oppmerksom på sitt ansvar for sikker oppbevaring og sletting.

· Sensitive personopplysninger som helseinformasjon, religion osv. skal som utgangspunkt ikke utleveres til andre enn relevante myndigheter.

· Data skal sendes/utleveres via sikre kanaler (f. eks. ved å sende en lenke til dokumentet i stedet for å legge ved dokumentet i en e-post)

· Ved utsendelse til større grupper, skal deres kontaktopplysninger (f.eks. e-post adresser) være skjult for mottakerne, for eksempel ved bruk av blindkopifeltet.

Sletting av personopplysninger

Følgende data skal fortløpende slettes fra klubbens lagringsmedier. Dette gjelder både trykte og digitale medier.

· Data som ikke lenger er relevante for utførelsen av en oppgave.

· Data som skal slettes på grunn av tilbakekallelse av samtykke fra personen dataene omhandler.

· Data som ikke lenger skal oppbevares som følge av lovgivning.

**Beredskap**

Sikkerhetsbrudd skal meddeles til styret/daglig leder, som har ansvaret for den videre håndtering og dokumentasjon av sikkerhetsbruddet.

**Sanksjonering**

Overtredelser av denne instruksen kan bli sanksjonert. Det er klubbens styre som fastsetter sanksjonen. Sanksjonen kan bestå av disiplinærforføyninger som; irettesettelse, bortvisning, utelukkelse i inntil en måned og bøteleggelse inntil kr. 5 000,- såfremt det framkommer av regelverket at det kan gis bot. I tillegg gjelder arbeidsmiljølovens bestemmelser.

[Sett inn klubbens navn, dato]

**Bekreftelse for mottatt og lest IT-instruks**

Jeg \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_bekrefter ved min underskrift nedenfor at jeg har lest og forstått [sett inn klubbens navn]s IT-instruks.

Dato:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_