Nedenfor finder du skabelon til brug for udfærdigelse af IT-instruks til jeres golfklub. IT-instruksen skal udleveres (og læses) af alle, der gives adgang til golfklubbens persondata i den ene eller den anden henseende. Det betyder, at IT-instruksen skal udleveres til alle ansatte, bestyrelsesmedlemmer og frivillige. I henhold til persondatareglerne påhviler det alle, der behandler persondata at sikre sig, at data behandles sikkert og korrekt, så data ikke misbruges, mistes eller behandles forkert. I forhold til at sikre dette er det et krav, at man uddanner og instruerer sit personale og relevante personer, der får adgang til persondata, om, hvordan man skal og må behandle data. Det er også at krav, at der regelmæssigt følges op på, at instruksen kendes/overholdes. **Derfor er det DGU's anbefaling, at golfklubben en gang årligt genudsender IT-instruksen til ansatte, bestyrelsesmedlemmer og frivillige med besked om at genopfriske instruksen og om at blive ved med at følge reglerne, når de har med klubbens persondata at gøre, og så gemmer denne mail til dokumentation for, at man rent faktisk har fulgt op på sin forpligtelse om at instruere om behandlingen af klubbens data.** Såfremt I gerne vil have sikkerhed for, at dem der får politikken udleveret rent faktisk har læst denne, kan I nederst indarbejde plads til, at modtageren skal kvittere for at have modtaget og læst denne politik. Dette vil give klubben endnu mere dokumentation for, at man har gjort sit bedste, for at overholde lovens krav om uddannelse og instruks.

En særlig udfordring for golfklubber, der i høj grad anvender frivillige til at udføre diverse opgaver, er, at dataene oftest sendes "ud af klubbens systemer", hvor klubben så ikke længere kan styre, hvad der sker med data. Instruksen nedenfor forsøger at tage højde for dette problem, ved at instruere om, hvordan data må bruges uden for klubbens systemer. Såfremt I formår at holde alle data inde for klubbens systemer, eksempelvis ved at data, der deles, deles via SharePoint eller lignende løsning, som klubben har indkøbt, og hvortil adgang kræver adgangskode, vil dette bestemt være at foretrække, da I derved i langt højere grad har styr på jeres persondata.

Skabelonen nedenfor skal anvendes således, at alt tekst skal gennemlæses for at tjekke, om det skrevne også passer på jeres golfklub. Hvis ikke det passer, retter I teksten til, så det passer med forholdende i jeres klub. Alle tekster anført i skarpe parenteser og med kursiv *[xxx]* skal udfyldes/tilrettes af jer. Hvis den allerede foreslåede tekst er passende for jeres klub, fjerne I blot parentesen og fjerner kursiveringen af teksten. Hvis der er forhold, som er relevant i jeres klub, og som ikke er medtaget i skabelonen, tilføjer I naturligvis bare det nødvendige.

IT-instruks og instruks om bruges af persondata for Gilleleje Golfklub

Gældende fra 25 May 2018

Generelt

I denne IT-instruks finder du de regler, der gælder for brugen af Gilleleje Golfklub's IT-systemer samt brugen af de persondata, som Gilleleje Golfklub giver dig adgang til, til brug for udførelse af en eller flere opgaver for golfklubben. Persondata er alle data, der fortæller noget om en given person. Begrebet er altså meget bredt og omfatter eksempelvis: navn, e-mail, telefonnumre, medlemsnumre, men også ting som tøjstørrelse og resultater i en turnering.

Gilleleje Golfklub skal til enhver tid beskytte og værne om de persondata vi får fra medlemmer, gæster, ansatte og øvrige samarbejdspartnere, så vi overholder de persondataretlige regler. Derfor pålægger vi også enhver, der har adgang til persondata i eller fra Gilleleje Golfklub at efterleve de retningslinjer der er angivet i denne instruks. Data må ikke kopieres eller videregives til personer, der ikke har legitim adgang til disse.

Computere, telefoner og andet der benyttes til at tilgå data

Ethvert apparat der kan benyttes til eller giver adgang til Gilleleje Golfklub's data, skal være beskyttet af passwords og/eller biometrisk sikring (fingeraftryks-løsning). Se mere om kravene til passwords nedenfor. Du skal låse apparatet, når du forlader det, også selvom det kun er for kortere tid, når du sidder og arbejder med Gilleleje Golfklub's data. Apparatet skal være beskyttet, så fornyet adgang skal etableres hvis apparatet har været ubenyttet længere en *15* minutter. Dette omfatter også private apparater som computere, telefoner

og andre enheder, som du måtte benytte til at læse eller opbevare mails og dokumenter fra Gilleleje Golfklub.

Opbevaring af data/arkivering

Fysiske data

Fysiske persondata er oplysninger om personer i notesbøger, protokoller, fysiske print m.v.

Følsomme persondata[1] og oplysninger om CPR-numre, lovovertrædelser og straffedomme skal beskyttes med en højere grad af sikkerhed, end almindelige persondata, da det kan have langt større konsekvenser for personen bag data, hvis dataene kommer i de forkerte hænder.

Har du med almindelige persondata at gøre, skal du generelt huske at rydde op efter dig, hente print i printeren o. lign. så persondataene ikke bliver delt med uvedkommende personer.

Har du følsomme persondata, oplysninger om CPR-numre, lovovertrædelser eller straffedomme på trykte medier skal disse være låst inde, når du ikke benytter dem, og når du forlader kontoret. Sådanne oplysninger vil sædvanligvis kun haves om ansatte i Gilleleje Golfklub, og disse skal kun deles med dem i klubben, som har et behov for at se disse. Haves sådanne oplysninger om andre end de ansatte, skal de håndteres som beskrevet oven for

Elektroniske data

Elektroniske persondata er oplysninger om personer i IT-systemer, på telefoner, på USB-stick og anden elektronisk form.

Alle data skal opbevares i programmer, der er installeret eller godkendt af Gilleleje Golfklub. Du må ikke selv installere ny software eller downloade programmer fra internettet, som benyttes til at tilgå Gilleleje Golfklub's data. Dette betyder også, at du ikke må downloade eller benytte alternative fildelingstjenester end det, som Gilleleje Golfklub har instrueret dig om at benytte.

Dataopbevaring lokalt

Persondata, der opbevares lokalt (onsite), skal opbevares på enheder (Server, NAS osv.), der er beskyttet af password. Enhederne skal opbevares i aflåst lokale. Det anbefales, at lokalet er tyverisikret.

I tilfælde af at systemerne skal serviceres, så skal der indgås aftale med leverandøren om beskyttelse af data. I tilfælde af tyveri skal reglerne for sikkerhedsbrud følges, og ledelsen skal underrettes.

Dataopbevaring online

Alle persondata, der opbevares online, skal tilgås via en sikker forbindelse. Dette sker typisk via en browser, som understøtter https. eller lignende krypteret adgang. Kan du ikke se, om det er https der benyttes, så kontakt leverandøren for at sikre, at adgangen er krypteret. Dette sker typisk ved anvendelse af certifikater.

Digitale data skal være beskyttet af samme grad af sikkerhed som fysiske data og følsomme persondata skal beskyttes i højere grad end almindelige data, se ovenfor.

Alle data skal opbevares på en måde, så de kun deles med dem, der har et sagligt formål med dataene, ligesom arkivering af data skal ske efter samme retningslinjer.

Ved fratræden skal dine arkiver gøres tilgængelige for bestyrelsen.

---

[1] Følsomme persondata er oplysninger om: race og etnisk oprindelse; politisk, religiøs eller filosofiske overbevisning, fagforeningsmæssige tilhørsforhold, genetiske og biometriske data, helbredsoplysninger eller oplysninger om seksuelle forhold eller -orientering.

Du må ikke opbevare persondata på dit C-drev, USB-nøgler eller lignende, hvor filer og oplysninger uforvarende kan blive slettet permanent eller lettere kan mistes og/eller komme til uvedkommendes kendskab.

Videregivelse af personoplysninger
Videregivelse af personoplysninger er en behandling omfattet af persondatareglerne. Medlemsoplysningerne må gerne videregives til andre medlemmer i golfklubben, når det har et sagligt formål. Således må medlemsoplysninger gerne deles i klubblad eller på lukkede hjemmesider, men de må ikke offentliggøres på offentligt tilgængelige hjemmesider uden samtykke fra de medlemmer, hvis oplysninger man ønsker at offentliggøre. Når du videregiver personoplysninger inden for klubben, skal du stadig kun videregive de oplysninger, der er relevante for den, du deler med. Hvis du bliver bedt om telefonnumre på en række medlemmer skal der ikke udleveres en liste, hvor også e-mailadresserne står.

Du skal være påpasselige med ikke at videregive personoplysninger uberettiget, f.eks. ved ukritisk at videresende mails, der selv eller i vedhæftede filer indeholder personoplysninger, som ikke burde videregives, eller ved utilsigtet at uploade eller udlevere dokumenter med personoplysninger, som ikke bør være tilgængelige for alle og enhver. Kollegaer, bestyrelsesmedlemmer m.v. kan også være uvedkommende, især når du behandler følsomme personoplysninger.

Vær opmærksom på, at sponsorer er selvstændige erhvervsdrivende, der ikke har noget med klubben at gøre, hvorfor medlemsoplysninger ikke må videregives til disse. Hvis golfklubbens pro og cafe-/ restaurationsejer ikke er ansat af klubben, gælder det samme i forhold til disse.

Brugernavne og passwords
Det anbefales at brugen af fælles brugerkonti og passwords undgås. Ved fratrædelse/ophør med en funktion, skal brugernavne og passwords der er udleveret til disse personer ændres omgående.

Passwords du benytter i forbindelse med, at du tilgår *[indsæt* Gilleleje Golfklub's persondata skal være forskelligt fra de passwords, du bruger til dine private gøremål, og skal være på mindst 8 tegn, bestående af 3 dele i form af store- og små bogstaver, tal og specialtegn. Du må ikke give dit password til andre, og du skal skifte dit password, hvis det bliver kendt af andre.

Passwords til systemer der indeholder personfølsomme data skal skiftes minimum hver 90. dag. I golfklubber vil det normalt kun være i oplysningerne om de ansatte i klubben, der vil være personfølsomme data i form af oplysninger om sygdomsforhold og/eller fagforeningsmæssige tilhørsforhold.

Sikkerhedsbrud
Ved ethvert brud eller mistanke om brud på sikkerheden skal klubbens ledelse omgående orienteres, der iværksætter foranstaltninger i henhold til beredskabsplanen.

Du skal kontakte ledelsen, hvis dine it-enheder har virus eller opfører sig mærkeligt. Du skal også kontakte ledelsen, hvis du har mistanke om, at antivirusprogrammet ikke virker korrekt.

Du skal være påpasselig ved modtagelse af mails og filer fra mærkelige afsendere, mails uden emneangivelse og henvendelser, der i øvrigt er mistænkelige.

Brug af e-mail

Alle former for persondata kan sendes på mail, hvis de pågældende persondata i øvrigt må videregives efter reglerne i persondatalovgivningen. Er der tale om følsomme data (eksempelvis oplysninger om sygdomsforhold på en af klubbens ansatte), bør det overvejes, om oplysningerne kan deles med de relevante på en anden måde end via mail. Dette kan eksempelvis være ved at lægge oplysningerne i fil delings løsning, hvor adgang til indholdet kræver adgangskode. Du kan stadig sende mail om, at de relevante personer skal gå ind og se dokumenterne, men undlad så vidt muligt at sende selve de følsomme oplysninger ud af golfklubbens system, hvor du mister kontrollen med data.

Du skal med jævne mellemrum slette de e-mails, modtagne, gemte og sendte, der indeholder persondata og ikke længere er aktuelle og ikke skal arkiveres. Sletningen skal være permanent.

Såfremt du bruger en privat mail til at modtage golfklubbens mails på, skal du sikre dig, at du har den nødvendige sikkerhed på denne mail/computer, at der ikke er andre der har adgang til denne mail, eksempelvis må du ikke dele mailen med din ægtefælle, og endelig bør du undlade at downloade og gemme oplysninger hjemme på din egen computer. Hvis du alligevel gemmer det modtagne hos dig privat, skal du sikre dig, at oplysninger ikke er tilgængelige for andre i din husstand, og at de slettes fra din computer, så snart du ikke længere har behov for oplysningerne.

Adgang til Gilleleje Golfklub's administrationssystemer *[(GolfBox/GolfWorks), lønsystemer, økonomisystemer m.m.]*:
Det er golfklubbens sekretariat, der administrerer adgange til administrationssystemerne. Adgangene til systemerne skal løbende tilpasses, så det alene er dem der har behov for adgang, der rent faktisk har det. Ansatte, bestyrelsesmedlemmer og frivillige skal have adgang til de personoplysninger, som de har brug for til løsning af deres opgave, men ikke mere. Bliver du opmærksom på, at du kan se flere oplysninger, end du har brug for, eller at din adgang forbliver åben, uanset at du ikke længere deltager i bestyrelsen eller frivilligt arbejde, skal du bede om, at din adgang til systemet lukkes ned.

De persondata som du gives adgang til må alene anvendes til brug for din opgave i Gilleleje Golfklub.

Databehandling

Informationssøgning
Det er forbudt at søge efter personinformationer der ikke er relevant for det arbejde der skal udføres.

Får man kendskab til at man har adgang til data man ikke burde have adgang til, så skal man uden unødigt ophold meddele dette til klubbens daglige ledelse.

Eksport/udsendelse af data
Der skal udvises omhu med hvilke persondata der deles med andre. Reglen er som udgangspunkt følgende:

- Der må kun udleveres de persondata der er nødvendige for at kunne udføre en specifik opgave.
- Modtageren skal gøres opmærksom på sit ansvar for betryggende opbevaring og sletning.
- Personfølsomme data som CPR-nummer, sygdomsforløb, religion osv. må som udgangspunkt ikke udleveres til andre end relevante myndigheder.
- Data skal sendes/udleveres ad sikre kanaler.
- Ved udsendelse til større grupper, så skal deres kontaktoplysninger (f.eks. e-mails) være skjult for modtagerne, for eksempel ved brug af BCC funktionen.

Sletning af persondata
Følgende data skal slettes fra klubbens datalagre. Datalagre er også de lagre der indehaves af medlemmer, partnere m.m. Det gælder både trykte og digitale medier.

- Data der ikke længere er relevante for udførelsen af en opgave
- Data der skal slettes som følge af tilbagekaldelse af samtykke fra personen hvis data der er tale om
- Data der ikke længere skal opbevares som følge af lovgivning

Beredskab
Sikkerhedsbrud skal meddeles til bestyrelsen, der forestår den videre håndtering og dokumentation af sikkerhedsbruddet.

[Sanktionering
Overtrædelse af denne politik vil blive sanktioneret. Det er klubbens bestyrelse der fastsætter sanktionen. Sanktionen kan strække sig fra en skriftlig advarsel til eksklusion/afskedigelse fra klubben]

Gilleleje Golfklub, 8 May 2018

Kvittering for at have læst og modtaget IT-politik

Jeg _____(indsæt navn med blokbogstaver) bekræfter ved min underskrift nedenfor at have læst og forstået denne IT-politik for Gilleleje Golfklub

Dato /

_____

Underskrift