Ide- og Udviklingscenter
for Viborg Pensionister

IT sikkerhed

IT SIKKERHEDSREGLER FOR IDE- OG UDVIKLINGSCENTER FOR VIBORG PENSIONISTER

Foreningen har formuleret og vedtaget følgende IT sikkerhedsregler. Løbende tages reglerne op til revision, og reglerne opbevares altid.

Hvilke persondata indsamles af foreningen - og hvorfor:

Til brug for registrering af kursusdeltagere, opkrævning af deltagerbetaling, ansøgning om kommunale tilskud indsamles:

- CPR nummer
- Navn
- Adresse
- Telefonnummer
- Mailadresse
- Bopælskommune

Indsamling sker ved kursustilmelding af den underviser, der modtager tilmelding. Oplysninger videregives straks til foreningens registerfører.

Behandling af persondata

Persondata registreres i foreningens deltagerregister, hvorfra der generes lister over kursusdeltagere mv.
Deltagerlister distribueres til foreningens undervisere via mails eller i papirform.

Opbevaring af persondata

Foreningens deltagerregister opbevares i elektronisk form hos foreningens registerfører.
Deltagerregistret opbevares på PC med behørig adgangsbeskyttelse (password). Backups er ligeledes forsynet med adgangsbeskyttelse.
Kun foreningens formand, kasserer og registerfører kan få adgang til de fuldstændige persondata for foreningens kursister.
Deltagerlister for igangværende kursushold opbevares hos foreningens undervisere elektronisk (mails) eller i papirform.
Foreningens undervisere har underskrevet tro- og loveerklæring vedrørende anvendelse, opbevaring og destruering af deltagerlister.

Sletning af data

Af hensyn til dokumentation ifølge bogføringsreglerne skal bilag, der dokumenterer økonomiske transaktioner opbevares i 5 år. Herefter slettes oplysningerne. Hvis dokumenter eller korrespondance, der indeholder persondata, ikke bruges som bogføringsbilag, slettes de, når de ikke længere er relevante for arbejdet i foreningen, dvs. når den aktivitet, de omhandler, er slut. Data med historisk relevans kan opbevares længere.

Foreningens undervisere sletter/destruerer ved kursers afslutning data for de deltagere, der stopper på holdet.

Ansvarlig for IT sikkerhed i foreningen og kontaktoplysninger på den ansvarlige:

Foreningens formand er den IT-ansvarlige person i foreningen. (Foreningens mailadresse er identisk med privat mailadressen)

Linda Thanild
Teglmarken 26
8800 Viborg
Tlf. 4042 0759
lindathanild@gmail.com

Tilfælde af databrud

I tilfælde af databrud, dvs. at persondata bliver stjålet, slipper ud ved et uheld, kommer til uvedkommendes kendskab eller lignende, skal følgende ske:

- Overvej alvoren af hændelsen. Foras landsforbund kontaktes altid.
- De personer, hvis data er sluppet ud, skal underrettes. Her kan backup være nødvendig, hvis maskinen er blevet hacket og låst.
- I tilfælde af alvorlige brud, skal Datatilsynet underrettes. Det skal ske indenfor 72 timer efter at bruddet er opdaget. Det er altid et alvorligt brud, hvis følsomme personoplysninger er sluppet ud. Ved almindelige personoplysninger vurderes det i det konkrete tilfælde, om bruddet er alvorligt. Er der tvivl, så opfat i udgangspunktet bruddet som alvorligt.
- Det skal besluttes hvilke foranstaltninger der skal iværksættes, for at begrænse skaden og forhindre at det sker igen. Herunder skal foreningens IT-sikkerhedspolitik og –procedurer gennemgås, for at lokalisere svagheder eller behov for ændringer.
- Beskriv altid hvad der er sket (hændelserne), så det senere kan dokumenteres, hvad der blev gjort og vurderet i situationen.

Revurdering af IT sikkerhedsreglerne

IT sikkerhedsreglerne vurderes løbende og behandles årligt i foreningens bestyrelse. Medlemmerne orienteres på generalforsamling om: Foreningens Persondata-regler og Foreningens IT sikkerhedsregler.