Bering Valgmenighed
*Aarhusegnens Grundtvigske Valgmenighed*

# Privatlivspolitik for medarbejdere, bestyrelse og udvalg i Bering Valgmenighed

**Torshøjvænget 15, 8361 Hasselager**

**CVR nr. 1968 8828**

Valgmenigheden behandler såvel almindelige personoplysninger som særlige personfølsomme personoplysninger og har derfor udarbejdet denne interne privatlivspolitik, der informerer og instruerer alle ansatte og valgmenighedens bestyrelse og udvalg i, hvordan vi behandler personoplysninger. Formålet hermed er at sikre, at valgmenigheden altid har en passende sikkerhed for behandling af personoplysninger, så oplysningerne beskyttes mod uautoriseret offentliggørelse og mod, at uvedkommende får adgang eller kendskab til dem. Heri er valgmenighedens interne regler på området, herunder regler for menighedens IT-sikkerhed samt instruks ved konstatering af brud på persondatasikkerhed.

Valgmenigheden har udarbejdet en datafortegnelse, som er en fortegnelse over vores behandling af personoplysninger. Valgmenighedens medarbejdere og valgmenigheds bestyrelses- og udvalgsmedlemmer er forpligtede til at gennemlæse fortegnelsen med henblik på at opnå et overblik over behandlingen af personoplysninger, som finder sted i valgmenigheden.

Endvidere er valgmenighedens medarbejdere og bestyrelses- og udvalgsmedlemmer forpligtigede til at gennemlæse denne politik både med henblik på at holde sig orienteret om valgmenighedens politik på området, men også for at overholde de regler og instrukser, som valgmenigheden har herom.

## Opbevaring af og adgang til personoplysninger

Valgmenighedens medarbejdere og bestyrelses- og udvalgsmedlemmer har pligt til altid at opbevare dokumenter og udstyr med personoplysninger forsvarligt og utilgængeligt for uvedkommende.

Det betyder blandt andet at:

- Dokumenter (elektroniske såvel som på papir), der indeholder personoplysninger, skal altid opbevares på en måde, hvor kun relevante personer har adgang.

- De computere og lignende udstyr, som menighedens medarbejdere anvender, må ikke efterlades uden låst skærm og skal være sikret med kode.

- Personalemapper opbevares i aflåst skab. Det samme gør sig gældende for eventuelle print af lister mv., hvoraf medlemmernes cpr.nr. og indkomstoplysninger fremgår.

- Det er kun menighedens kasserer/forretningsfører, som har adgang til medlemmernes indkomstoplysninger.

- Medlemslister må kun udleveres til præst og formand. Disse lister skal være uden cpr.nr. og skal opbevares i aflåst skab.

## Brug af mail

Selve medlemskabet af valgmenigheden anses som en personoplysning om medlemmets religiøse overbevisning og dermed en særlig personfølsom oplysning. Det betyder, at der er særlige forholdsregler, der skal overholdes i forbindelse med afsendelse af og modtagelse af mails.

Ved afsendelse og modtagelse af mail skal der skelnes mellem mails vedrørende valgmenighedens almindelige liv og hverdag på den ene side og mails vedrørende valgmenighedens religiøse liv på den anden side.

Det er tilladt at sende og modtage mails om valgmenighedens almindelige liv og hverdag, uden at disse sendes sikkert (krypteret og signeret). F.eks. mails hvor valgmenigheden udsender sit kirkeblad eller nyhedsmail, mails hvor der aftales praktiske ting – f.eks. hvem der medbringer kage, køber ind, gør rent osv. samt indkaldes til valgmenighedsudvalgsmøde (bestyrelsesmøder/udvalgsmøder) mv.

*Det er ikke tilladt at sende og modtage mails om valgmenighedens religiøse liv, uden at disse sendes sikkert (krypteret og signeret). F.eks. mails der vedrører ind- og udmeldelser, dåb, vielse og begravelser/bisættelser mv.*

*Mails, som indeholder cpr.nr., skal altid sendes sikkert (krypteret og signeret). Det samme gør sig gældende for mails, som indeholder særlige personfølsomme oplysninger, f.eks. oplysninger om sygdomme, sociale problemer, familiærre relationer, strafbare forhold osv.*

Såvel valgmenighedens medarbejdere som bestyrelses- og udvalgsmedlemmer skal overholde disse retningslinjer vedrørende afsendelse og modtagelse af mails, og valgmenigheden stiller i nødvendigt omfang en teknisk løsning til rådighed, hvorfra mails kan sendes og modtages sikkert.

Hvis der modtages mails, som burde være sendt sikkert, disse hurtigst muligt slettes (også fra slettet post), og hvis det er nødvendigt, skal oplysninger forinden overføres til en sikker opbevaringsmetode.

## Brug af billeder på menighedens hjemmeside, facebookside og kirkeblad

Ved upload af billeder skal medarbejderen være opmærksom på, at det kun er tilladt at uploade situationsbilleder. Situationsbilleder er billeder, hvor en aktivitet eller en situation er det egentlige formål med billedet. F.eks. et billede ud over menigheden, som sidder i kirken under en gudstjeneste.

Ved upload af billeder skal medarbejderen altid være opmærksom på, at personerne på billederne ikke med rimelighed må kunne føle sig udstillet, udnyttet eller krænket.

Særligt bemærkes, at offentliggørelse af holdbillede af f.eks. konfirmander kræver samtykke fra alle konfirmandernes forældre. I forbindelse med indskrivning til konfirmationsforberedelse skal samtykke hertil underskrives.

## Samtaler i det offentlige rum

Det er ikke tilladt at føre samtaler i det offentlige rum, som gør det muligt for omkringværende at identificere de medlemmer eller pårørende, det drejer sig om.

## IT-sikkerhed

- De computere og lignende udstyr, som valgmenighedens personale- og medlemsadministration udføres på, skal til enhver tid håndteres sikkert og forsvarligt, herunder skal der bruges skærmlås og adgangskode.

- Adgangskoder og passwords må ikke genbruges til flere tjenester.

- Adgangskoder/passwords opbevares sikkert og adskilt fra udstyret – undgå, om muligt, at nedskrive disse.

- Der skal løbende foretages back up af menighedens data.

- Der skal etableres firewalls og antivirus beskyttelse på alle computere.

- Man må ikke åbne mistænkelige mails og hjemmesider.

- Mails vedrørende valgmenighedens religiøse liv samt mails, som indeholder særlige personfølsomme oplysninger eller cpr.nr., skal altid sendes og modtages sikkert (krypteret og signeret).

## Sletning

Valgmenigheden sletter personoplysninger i henhold til retningslinjer på området.

Personoplysninger opbevares dog aldrig længere end nødvendigt.

Personaleoplysninger opbevares, så længe ansættelsesforholdet er gældende. Efter fratrædelse slettes de oplysninger, som ikke skal opbevares længere i henhold til særlovgivning. Portrætbillede på menighedens hjemmeside slettes straks ved fratrædelsen. Lønoplysninger opbevares til udgangen af året plus 5 år.

Jobansøgninger gemmes maksimalt i 6 måneder, medmindre der er givet samtykke til andet.

Personoplysninger om vores medlemmer slettes og makuleres vedudgangen af året plus 5 år (ved forpligtigelseserklæringer 10 år).

Dog opbevares de førte kirkebøger til evig tid.

Endvidere opbevares medlemslister tilbage i tiden indeholdende navn og adresse af lokalhistoriske årsager.

Beslutningsreferater fra valgmenigheds bestyrelses- og udvalgsmøder opbevares, så længe valgmenigheden eksisterer. Det sker for at kunne dokumentere den overordnede ledelses beslutninger. Vær opmærksom på, at beslutningsreferater ikke bør indeholde personoplysninger.

Personoplysninger om bestyrelses- og udvalgsmedlemmer opbevares, så længe vedkommende er medlem af udvalget (udvalg/bestyrelse). Dog slettes navn og medlemsperiode ikke, ligesom disse oplysninger fortsat fremgår af referater, årsregnskaber og vedtægter. Portrætbillede på valgmenighedens hjemmeside slettes straks ved udtræden.

Gravstedsbreve slettes straks efter fredningsperiodens udløb.

Flerårige vedligeholdelsesaftaler slettes straks efter aftalens udløb.

Når et gravsted nedlægges, slettes alle oplysninger og dokumenter vedrørende gravstedet.

## Sikkerhedsbrud - anmeldelsespligt

Hvis valgmenighedens ansatte eller bestyrelses- og udvalgsmedlemmer konstaterer eller formoder et sikkerhedsbrud, så har vedkommende pligt til hurtigst muligt at give valgmenighedens formand meddelelse herom.

Et sikkerhedsbrud kan f.eks. være et hackerangreb, eller at valgmenigheden på anden måde mister kontrollen over de personoplysninger, som vi behandler.

Valgmenighedens formand skal herefter vurdere, om bruddet kan medføre risiko for fysiske personers rettigheder eller frihedsrettigheder. I så fald skal formanden uden unødig forsinkelse og om muligt senest 72 timer efter bruddet anmelde bruddet til Datatilsynet. Anmeldelse sker digitalt på virk.dk:
https://indberet.integration.virk.dk/myndigheder/stat/ERST/Indberetning_af_brud_paa_sikkerhed#tab2

Uanset om bruddet er anmeldelsespligtigt eller ej, skal alle brud registreres internt.

Desuden skal valgmenighedens formand informere de berørte personer om buddet, hvis der er høj risiko for, at pågældende f.eks. kan blive udsat for diskrimination, identitetstyveri eller bedrageri på baggrund af sikkerhedsbruddet.

## Opdatering af denne politik

Bering Valgmenigheden er forpligtet til at overholde reglerne om databeskyttelse. Vi gennemgår derfor regelmæssigt denne politik for at holde den opdateret og i overensstemmelse med lovgivningen.

Valgmenigheden (bestyrelse og udvalg) er forpligtet til mindst én gang årligt at gennemgå menighedens datafortegnelse, interne og eksterne privatlivspolitik med henblik på, at disse altid er opdaterede og i overensstemmelse med lovgivningen.

Denne politik kan ændres uden varsel. Den nyeste opdaterede politik vil blive delt med valgmenighedens personale og bestyrelsesmedlemmer, som til enhver tid er forpligtede til at holde sig opdaterede med den nyeste udgave af denne.

*Denne politik er senest opdateret den 23. august 2023*