

VASA KYRKLIGA SAMFÄLLIGHETS DATASKYDD- OCH DATASÄKERHETSPOLICY

Godkänd av gemensamma kyrkorådet 28.11.2024

Innehåll

1. Syftet med dataskydds- och datasäkerhetspolicyn	2
2. Definitioner av dataskydd och datasäkerhet	2
3. Allmänna principer för dataskydd	3
4. Allmänna principer för datasäkerhet	4
5. Roller och ansvar	5

1. Syftet med dataskydds- och datasäkerhetspolicyn

Vasa kyrkliga samfällighet och dess församlingar är en enda informationshanteringsenhet, arkivbildare och personuppgiftsansvarig. Syftet med dataskydds- och datasäkerhetspolicyn är att sätta upp enhetliga mål för genomförandet av dataskydd och datasäkerhet i hela den kyrkliga samfälligheten. Målet är att trygga verksamhetens konfidentialitet och minska riskerna i anslutning till dataskydd och datasäkerhet.

Genom att ta hand om dataskyddet och datasäkerheten försäkrar vi att de registrerade personerna kan lita på att deras integritet respekteras och att deras personuppgifter skyddas. Vi följer lagstiftning och rekommendationer som gäller dataskydd och datasäkerhet, bland annat kyrkolagen, dataskyddsförordningen, dataskyddslagen, offentlighetslagen och, i den utsträckning som definieras i kyrkolagen, informationshanteringslagen, arkivlagen och lagen om behandling av kunduppgifter inom social- och hälsovården.

Vi tillämpar de principer som anges i denna policy i all verksamhet som den kyrkliga samfälligheten bedriver. Dessutom följer vi Finlands evangelisk-lutherska kyrkas datasäkerhetspolicy och datasäkerhetsbestämmelser. I den kyrkliga samfällighetens och IT-områdets anvisningar preciseras hur vi genomför principerna för dataskydd och datasäkerhet i praktiken.

2. Definitioner av dataskydd och datasäkerhet

Med dataskydd avses skydd av personuppgifter i enlighet med dataskyddslagstiftningen. Dataskydd är en grundläggande rättighet som skyddar den registrerades rättigheter vid behandlingen av personuppgifter. Personuppgifter är alla uppgifter som anknyter till en identifierad eller identifierbar fysisk person.

Med datasäkerhet avses de åtgärder som görs för att säkerställa uppgifternas konfidentialitet, integritet och tillgänglighet. Med hjälp av datasäkerhet försäkrar man att

- uppgifter endast är tillgängliga för de aktörer som har tillstånd att behandla dem (konfidentialitet),
- uppgifter endast ändras på ett kontrollerat sätt och inte ändras eller försvinner av misstag (integritet),
- uppgifter är tillgängliga när de behövs (tillgänglighet).

Datasäkerhetsåtgärder möjliggör en säker behandling av personuppgifter. Således är datasäkerhet en metod för att genomföra dataskydd.

3. Allmänna principer för dataskydd

Korrekthet och bundenhet till användningsändamålet

Vi behandlar personuppgifter korrekt och endast i sådana syften som är motiverade med tanke på församlingens verksamhet. Vi behandlar endast uppgifter med stöd av de rättsliga grunder som anges i dataskyddsförordningen.

Vi bedömer konsekvenserna av och riskerna med behandlingen av personuppgifter med tanke på en persons rättigheter. Vi beaktar dataskyddet i all behandling av personuppgifter.

Vi ser till att skydda personuppgifter som tillhör särskilda kategorier av personuppgifter. Vi behandlar dessa uppgifter endast inom ramen för de gränser som lagen tillåter och endast i den utsträckning som är nödvändig. Särskilda kategorier av personuppgifter är uppgifter som bland annat gäller hälsa, medlemskap i religionssamfund och fackförbund samt sexuell läggning.

Konfidentialitet

Vi ser till att alla anställda, frivilligarbetare, förtroendevalda och övriga personer som deltar i behandlingen är medvetna om sina skyldigheter i anslutning till dataskydd. De är bundna av tystnadsplikt som är lagstadgad eller skriftligen avtalad.

Vi lämnar ut personuppgifter till tredje parter endast om lagen förpliktar oss till det eller om vi har personens samtycke eller annan rättslig grund för utlämnandet.

Vi säkerställer att våra samarbetspartner och underleverantörer har förbundit sig till våra dataskyddsprinciper. Vi ser till att korrekta avtal görs upp och att instruktioner ges till våra samarbetspartner.

Korrekthet

Vi ser till att personuppgifterna är aktuella och att felaktiga personuppgifter tas bort eller korrigeras omedelbart.

Ansvarsskyldighet

Vi dokumenterar vår verksamhet för behandling av personuppgifter på lämpligt sätt och granskar dokumentationen regelbundet.

Lagringsminimering

Vi lagrar personuppgifter enbart så länge som lagen eller ändamålet för vilket de behandlas kräver. När vi inte längre behöver personuppgifterna, raderar, anonymiserar eller arkiverar vi dem i enlighet med arkivbildningsplanen.

Transparens

Vi behandlar personuppgifter transparent genom att de registrerade är medvetna om vilka uppgifter vi behandlar, hur och i vilket syfte.

Ombesörjande av den registrerades rättigheter

Vi ser till att den registrerades rättigheter tillgodoses. Enligt lag har den registrerade rätt att be om tillgång till de personuppgifter som gäller honom eller henne själv samt rätt att be om att rätta och avlägsna uppgifter, flytta uppgifter till ett annat system eller begränsa behandlingen. Den registrerade har också rätt att göra en invändning mot behandlingen av personuppgifter. Dessutom har den registrerade rätt att återkalla sitt samtycke till behandling av personuppgifter om behandlingen grundar sig på samtycke. Den registrerade har rätt att överklaga till tillsynsmyndigheten.

Utövandet av den registrerades rättigheter kan vara begränsad när vi behandlar uppgifterna till exempel på grundval av en lagstadgad uppgift.

4. Allmänna principer för datasäkerhet

Lagstadgad datasäkerhet

Enligt dataskyddsförordningen ska den personuppgiftsansvarige identifiera de risker som anknyter till behandlingen av personuppgifter och vidta tillräckliga åtgärder för att skydda uppgifterna. Arkivlagen föreskriver att handlingar ska förvaras så att de är skyddade mot förstörelse, skada och obehörig användning. I informationshanteringslagen finns å sin sida bestämmelser om skyldigheten att säkerställa informationssäkerheten i fråga om informationsmaterial och informationssystem.

Fysisk datasäkerhet

Vi sköter om uppgifternas konfidentialitet, integritet och tillgänglighet genom tillräckliga fysiska åtgärder. Sådana åtgärder är till exempel lås- och passerkontrollsystem samt skydd av arkivlokaler.

Teknisk datasäkerhet

Vi sköter om uppgifternas konfidentialitet, integritet och tillgänglighet genom tillräckliga tekniska åtgärder. Vi genomför teknisk datasäkerhet i samarbete med IT-området, Kyrkans servicecentral och andra leverantörer av utrustning och informationssystem. Vi tar hand om användarhanteringen och följer principen om att minimera åtkomsträttigheterna.

Administrativ datasäkerhet

Vi sköter om uppgifternas konfidentialitet, integritet och tillgänglighet genom tillräckliga administrativa åtgärder. Sådana åtgärder är till exempel utarbetande av anvisningar, utbildning av personal och dokumentation av datasäkerhet och databehandling.

Reaktion på säkerhetsöverträdelser

Vi hanterar säkerhetsöverträdelser på behörigt sätt och brådskanie på det sätt som dataskyddslagstiftningen kräver. Vi vidtar alla åtgärder som behövs för att mildra de negativa konsekvenserna för enskilda personer i händelse av en säkerhetsöverträdelse.

5. Roller och ansvar

Gemensamma kyrkofullmäktige

Gemensamma kyrkofullmäktige är den kyrkliga samfällighetens högsta beslutande organ, som godkänner den kyrkliga samfällighetens verksamhets- och ekonomiplan samt bokslut och verksamhetsberättelse, i vilka dataskydds- och datasäkerhetsärenden ingår.

Gemensamma kyrkorådet

Gemensamma kyrkorådet ansvarar för att den kyrkliga samfälligheten uppfyller skyldigheterna i lagstiftningen om dataskydd och datasäkerhet samt övervakar hur dataskyddet och datasäkerheten förverkligas. Gemensamma kyrkorådet har godkänt denna dataskydds- och datasäkerhetspolicy och förbundit sig till den.

Dessutom ska gemensamma kyrkorådet

- ansvara för att de bestämmelser och anvisningar om datasäkerhet som getts till den kyrkliga samfälligheten följs,
- se till att den kyrkliga samfälligheten har utsett kontaktpersoner för dataskydd och datasäkerhet,
- godkänna den kyrkliga samfällighetens dataskydds- och datasäkerhetspolicy som är förenlig med IT-områdets datasäkerhetspolicy och kyrkans dataskydds- och datasäkerhetsriktlinjer.

Dataskyddsombud

Gemensamma kyrkorådet utser ett dataskyddsombud att ansvara för uppgifter i enlighet med dataskyddsförordningen. Enligt dataskyddsförordningen ska dataskyddsombudet

- övervaka efterlevnaden av dataskyddsreglerna inom organisationen,
- informera och ge råd till ledningen och de anställda om deras skyldigheter enligt dataskyddslagstiftningen,
- samarbeta med tillsynsmyndigheten och fungera som kontaktperson för tillsynsmyndigheten.

Dataskyddsarbetsgruppen

Gemensamma kyrkorådet utser en dataskyddsarbetsgrupp som består av medlemmar särskilt från de arbetsområden där riskerna för behandling av personuppgifter är störst.

Dataskyddsarbetsgruppen

- bereder och utvecklar dokumentation, anvisningar och interna metoder för att genomföra och påvisa dataskydd,
- rapporterar om sin verksamhet och dataskyddssituationen till gemensamma kyrkorådet.

Kontaktperson för dataskydd och datasäkerhet

Gemensamma kyrkorådet utser en kontaktperson för dataskydd och datasäkerhet.

Kontaktpersonen

- fungerar som sammankallare för dataskyddsarbetsgruppen,
- fungerar som kontaktperson mellan den kyrkliga samfälligheten och dataskyddsombudet,
- ser till att de anvisningar, rekommendationer och bestämmelser om dataskydd och datasäkerhet som han/hon har fått meddelas alla anställda,
- deltar som stöd för cheferna i introduktionen av nya medarbetare i dataskydds- och datasäkerhetsfrågor,
- tar emot anmälningar om informationssäkerhetsincidenter och säkerhetsöverträdelser inom den kyrkliga samfälligheten och rapporterar om dem till IT-områdets datasäkerhetsansvariga och till den kyrkliga samfällighetens ledningsgrupp.

Ledning och chefer

Den kyrkliga samfällighetens ledning och chefer

- ansvarar för att dataskyddet beaktas i den dagliga verksamheten, i beslutsfattandet och i avtal,
- säkerställer alla deras medarbetare är medvetna om och följer innehåller i dataskydds- och datasäkerhetspolicyn och -anvisningarna,
- meddelar till kontaktpersonen för dataskydd och datasäkerhet om det finns planer på förändringar eller reformer som gäller behandlingen av personuppgifter.

Anställda, frivilliga och förtroendevalda

Alla anställda, frivilligarbetare och förtroendevalda

- följer anvisningarna och lämpliga tillvägagångssätt för dataskydd och datasäkerhet i sin egen verksamhet,
- har tystnadsplikt i enlighet med 35 § i dataskyddslagen och sekretessförbindelsen som de undertecknat,
- är skyldiga att omedelbart underrätta kontaktpersonen för dataskydd och datasäkerhet om säkerhetsöverträdelser eller informationssäkerhetsincidenter som de upptäcker.

IT-områdets datasäkerhetsgrupp

Kustens IT-centrals datasäkerhetsgrupp upprätthåller bestämmelser, anvisningar och rekommendationer om datasäkerhetspolicyn och datasäkerheten i IT-områdets ekonomiska församlingsenheter så att de är i linje med kyrkans gemensamma bestämmelser.

Datasäkerhetsgruppen

- övervakar att datasäkerhetsbestämmelser följs,
- behandlar aktuella frågor om datasäkerhet,
- planerar och ordnar utbildning som berör datasäkerhet.

IT-områdets datasäkerhetsansvariga

Kustens IT-centrals datasäkerhetsansvariga utvecklar datasäkerheten i IT-områdets församlingar.

Den datasäkerhetsansvariga

- ansvarar för informationen om anvisningar, rekommendationer och bestämmelser som gäller datasäkerhet,
- tar emot observationer om händelser och avvikelser i anknytning till datasäkerheten och rapporterar regelbundet om dem till datasäkerhetsgruppen och kyrkans datasäkerhetschef,
- godkänner vid hotad datasäkerhet eller i exceptionella situationer en sådan ekonomisk församlingsenhets datasäkerhetsbestämmelse som gäller högst två månader.