Antaget av styrelsen: 2018-09-14, §1152
Senaste revidering: 2018-06-26

# Riktlinjer för sekretess och hantering av personuppgifter

**Policyns mål**
Det övergripande målet med Kyrkans Försäkring AB:s informationssäkerhet är att säkerställa ett tillräckligt skydd för organisationens informationsresurser, så att rätt information är tillgängligt för rätt person i rätt tid på ett spårbart sätt.

Målet är att hantera verksamhetens informationsresurser enligt vedertagen praxis samt att ställa krav vidare till leverantörer av IT-tjänster och andra berörda tredje parter.

Skyddsnivån ska vara säkerhets, risk- och kostnadsmässigt rimlig i förhållande till informationens känslighet.

Med inriktning på verksamhetens samlade information och informationssystem riktar sig denna policy till att uppnå och underhålla kravbilden från externa intressenter; Lagkrav från GDPR, rekommendationer från Datainspektionen samt Finansinspektionen.

**Policyns omfattning**
Denna policy gäller för bolagets hela verksamhet.

**Syftet med policyn**
Denna policy beskriver Bolagets ansvar för informationssäkerhet inom dess ansvarsområde.

Utgångspunkten är att Bolagets information är vital för Bolagets verksamhet och att denna ska skyddas enligt lagar och rekommendationer. Om information eller system inte hanteras på rätt sätt kan Bolagets verksamhet, goda namn och rykte äventyras.

**Dataskyddsförordningen**
EU har beslutat om en ny förordning benämns vidare som ”Allmänna dataskyddsförordningen” eller ”GDPR som trädde i kraft den 25 maj 2018. Den nya förordningen skall tillämpas av samtliga organisationer och branscher som behandlar personuppgifter.

I Sverige har GDPR (General Data Protection Regulation) ersatt nuvarande personuppgiftslagen, PUL (1998:204). Mycket av det som täcktes av personuppgiftslagen gäller även fortsättningsvis men det finns också en del nyheter som exempelvis om registren eller personuppgifter på något sätt finns kopplade till bolagets webbplats, till exempel genom en inloggningstjänst (”kundportal”) behöver en översyn göras på bolagets system och kontrollera att samarbetet med webbyrån eller leverantör har koll på de nya reglerna. Det kan till exempel gälla personers rättigheter att få sina personuppgifter raderade från systemen.

För närvarande finns ingen kundportal med inloggning men behovet och ambitionen finns. Vid införande av sådan kommer skydd mot obehörigt tillträde kontrolleras.

Bolagets anställda förekommer på hemsida och i tryck med bilder och kontaktuppgifter. Dessa hålls efter så att det endast är aktivt anställda som förekommer.

**Vad är en personuppgift?**
All information som direkt eller indirekt går att koppla till en enskild fysisk person är personuppgifter. Det kan gälla:

- Namn, adress, e-postadress och andra kontaktuppgifter
- Bilder och ljudupptagningar
- IP-nummer

- Anställningsnummer
- Personnummer

En indirekt personuppgift är något som inte kan knytas till en enskild person direkt, men som ändå berättar något om en person, till exempel ett ovanligt efternamn.

**Nya regler ersätter personuppgiftslagen PUL**
Mycket i den Allmänna dataskyddsförordningen är likt de regler som finns i PUL, till exempel att man måste få ett samtycke från personen för att få behandla personuppgifter, men det finns också nyheter såsom:

- Personen som är registrerad har en rad rättigheter som bolaget måste kunna uppfylla. Det gäller till exempel att ge en enskild person tillgång till sina uppgifter, rätt att få felaktiga personuppgifter rättade eller raderade och ges möjlighet att flytta personuppgifterna till en annan tjänst.
- Om det sker ett dataintrång eller någon annan incident som påverkar säkerheten måste bolaget anmäla det till Datainspektionen inom 72 timmar. Eventuellt även meddela de registrerade vad som hänt.
- En del organisationer och myndigheter måste ha en person som har till uppgift att hålla koll på frågor kring dataskydd, ett så kallat dataskyddsombud.
- Det införs en sanktionsavgift eller straff för de som bryter mot förordningens regler. Straffet kan bli upp till fyra procent av bolagets årsomsättning eller 20 miljoner euro (som mest) för riktigt grova brott mot förordningen.

På Datainspektionens webbplats finns listor över vad bolaget behöver göra för förändringar för att anpassa verksamheten till det nya regelverket.

**KFAB:s åtgärder med anledning av införandet av GDPR**

<u>Personuppgiftsregister, Registeransvarig</u>
Bolaget har med anledning av GDPR tagit fram ett register över de personuppgifter som bolaget hanterar. Denna lista hålls uppdaterad av i bolaget utsedd person, Annika Jonsson.
De personuppgifter som bolaget hanterar är till största delen kunders representanter som förekommer i e-postkonversation, telefonsamtal och därmed i noteringar i Bolagets affärssystem. Det finns också personuppgifter för anställda, styrelse och ”tredjeman” som kan vara skadelidande i olycksfallsskador, ansvarsskador eller att de förekommer i skadeärenden som gärningsmän.

<u>Personuppgiftsbiträdesavtal</u>
För alla skadeärenden finns personuppgiftsbiträdesavtal upprättat med Nordic Loss Adjusting AB som är Bolagets avtalade skadereglerare. Personuppgiftsbiträdesavtal finns också upprättat med Restvärdesräddningen som i undantagsfall kan komma i kontakt med personuppgifter hos våra kunder.

**Revidering av dokument**

| | | |
|---|---|---|
| 2018-06-26 | Nytt styrdokument | I enlighet med Compliancerapport Q1 2018 |