Dataskyddspolicy

Policyns mål

Det övergripande målet med Kyrkans Försäkring AB:s (”**Bolaget**”) dataskyddspolicy är att efterleva gällande dataskyddslagstiftning såsom Europaparlamentets och Rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (”**GDPR**”) samt nationell reglering såsom lagar, föreskrifter, allmänna råd och praxis.

Policyns omfattning

Samtliga personuppgifter som hanteras inom ramen för Bolagets verksamhet omfattas av denna policy. Alla regler i denna policy rörande exempelvis lagring, gallring, skydd för personuppgifter och registrerades rättigheter gäller även för personuppgifter i så kallat ostrukturerat material. Med ostrukturerat material förstås all typ av material som inte är sökbart i ett register eller i en databas. Exempel på ostrukturerat material är personuppgifter i löpande text, e-post eller i pärmar.

Syftet med policyn

Syftet med denna Policy är att fastställa övergripande principer och riktlinjer för att Bolaget ska uppnå ett adekvat skydd för personuppgifter, samt säkerställa regelefterlevnad. Vidare syftar denna policy till att främja enskilda personers kontroll och rättigheter rörande de personuppgifter som Bolaget behandlar. Policyn syftar också till att säkerställa kunders och andra enskilda personers, rätt att ha insyn i och kontroll över, de personuppgifter som Bolaget behandlar.

Organisation och ansvar

Styrelsen är ytterst ansvarig för att Bolaget efterlever gällande externa regelverk och är således också ytterst ansvarig för personuppgiftshanteringen i Bolaget. Styrelsen ansvarar för att fastställa denna policy minst en gång per år.

VD ansvarar för att införa processer och mekanismer för att upprätthålla regelefterlevnaden utifrån styrelsens direktiv. VD ska också säkerställa att denna Policy implementeras i verksamheten.

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.

Kategorier av registrerade

Bolaget hanterar personuppgifter för tre kategorier av registrerade: 1) kunder, 2) medarbetare och uppdragstagare, samt 3) övriga. Kategorin ”övriga” kan exempelvis omfatta styrelseledamöter och personer som uttryckligen visat intresse för Bolagets tjänster, dvs. eventuella blivande kunder, eller personer som har figurerat i Bolaget HR-process såsom eventuella rekryteringar, referenser eller

liknande. Kategorin kunder omfattar både kunder som är fysiska personer och företrädare eller kontaktpersoner hos juridiska personer med vilka Bolaget har en avtalsrelation.

Grundläggande principer för dataskydd

Det personliga integritetsskyddet är en grundpelare i GDPR vilket innebär att integritetsskyddet ska iakttas genom hela livscykeln av personuppgiftsbehandlingen. Andra grundläggande principer som Bolaget behöver följa vid personuppgiftsbehandling är principerna om laglighet och öppenhet, uppgiftsminimering, ändamålsbegränsning, korrekthet, lagringsminimering, integritet och konfidentialitet samt principen om ansvarsskyldighet.

Att en behandling ska vara *laglig och öppen* betyder att det ska finnas en laglig grund i enhetlighet med Dataskyddslagstiftningen. Vidare ska behandlingen vara öppen och transparent gentemot den registrerade. Vid inhämtande av personuppgifter ska enbart uppgifter som är adekvata, relevanta och inte för omfattande för ändamålet inhämtas. Det betyder att det inte är tillåtet att inhämta uppgifter för obestämda framtida behov eller fler än vad behovet kräver s.k. *uppgiftsminimering*.

Vid behandling av personuppgifter ska uppgifter enbart samlas in för särskilda, uttryckligt angivna och berättigade ändamål. I praktiken innebär detta att den som samlar in personuppgifterna inte senare får behandla personuppgifterna för ett annat ändamål, s.k. *ändamålsbegränsning*.

Korrekthet innebär att personuppgifterna ska vara korrekta och uppdaterade. Den personuppgiftsansvariga och/eller personuppgiftbiträden/underbiträden har skyldigheten att säkerställa att personuppgifter som är felaktiga ska raderas eller rättas utan dröjsmål.

I enlighet med GDPR ska Bolaget inte spara fler uppgifter än nödvändigt eller under längre tid än nödvändigt. Vidare är målet att ge ramarna för att säkerställa att gallring av personuppgifter sker på ett ändamålsenligt och effektivt sätt samt i enlighet med externa regler s.k. *lagringsminimering*.

De personuppgifter som har inhämtats av Bolaget ska skyddas gentemot förlust, förstöring eller skada genom olyckshändelse. Obehörig eller otillåten behandling ska också ingå i skyddsåtgärderna. Detta kallar man för principen om *integritet och konfidentialitet*.

Det är den som behandlar personuppgifterna, personuppgiftsansvarig och/eller personuppgiftsbiträden/underbiträden, som ansvarar för att dessa principer efterlevs och efterföljs, dvs. Bolaget har en *ansvarsskyldighet*.

Laglig grund

Behandling av personuppgifter inom Bolaget är endast tillåten ifall någon av de i GDPR föreskrivna lagliga grunderna är uppfylld. De lagliga grunderna är fullgörande av avtal, fullgörande av rättslig förpliktelse, intresseavvägning, samtycke, skydd av den registrerades grundläggande intressen samt utförande av uppgift av allmänt intresse. De lagliga grunder som Bolaget förväntas stödja sina behandlingar på är fullgörande av avtal, uppfyllande av rättslig förpliktelse, uppfyllande av rättslig förpliktelse, intresseavvägning samt samtycke.

Med fullgörande av avtal avses att behandlingen av personuppgifter krävs för att Bolaget ska kunna fullgöra ett avtal med den registrerade eller vidta åtgärder som den registrerade begärt innan avtal ingås. Det kan t.ex. handla om att registrera en försäkringstagare eller registrera anställningsavtal.

Personuppgifter får också behandlas om det är nödvändigt för Bolaget att uppfylla en rättslig förpliktelse. Den rättsliga förpliktelsen ska följa av svensk rätt eller av EU-rätt. Exempel på en rättslig förpliktelse är bokföringsskyldigheten som anges i Bokföringslagen eller skyldigheten att lämna kontrolluppgifter till Skatteverket enligt Skatteförfarandelagen.
Det är vidare tillåtet för Bolaget att behandla personuppgifter efter att en intresseavvägning har skett. För att Bolaget ska kunna grunda behandling av personuppgifter på intresseavvägning krävs att den

registrerades fri- och rättigheter inte väger tyngre än Bolagets berättigade intressen för att genomföra behandlingen. GDPR stadgar att ett berättigat intresse kan ligga till grund för behandling i det fall det existerar ett relevant och lämpligt förhållande med den registrerade, ex. vis om den registrerade är en kund. Slutligen är det tillåtet att i vissa fall behandla personuppgifter med stöd av den lagliga grunden samtycke.

Personuppgiftsregister, Registeransvarig

Bolaget ska föra en registerförteckning över den personuppgiftshantering som Bolaget har i sin verksamhet. Förteckningen syftar till att skapa intern kontroll över den egna personuppgiftshanteringen samt som ett led i att kunna uppvisa efterlevnad av GDPR. Registerförteckningen ska vid var tid hållas uppdaterad.
Underwritingansvarig / Ekonomiansvarig ansvarar för den löpande förvaltningen av Bolagets registerförteckning.

Information

Bolaget ska tillgängliggöra, men även i vissa fall tillhandahålla, information om hur Bolaget behandlar registrerades personuppgifter samt villkoren för utövandet av den registrerades rättigheter. Informationen ska vara skriftlig och finnas tillgänglig på ett sådant sätt att samtliga registrerade kan ta del av informationen. Vidare ska informationen vara utformad på ett enkelt och tydligt sätt samt i ett lätt tillgängligt format. Bolaget ska tillgängliggöra informationen på Bolagets webbplats som en del av de allmänna villkor som samtliga av Bolagets kunder får del av när en avtalsrelation etableras.

Registrerades rättigheter

GDPR innefattar flertalet bestämmelser som syftar till att ge registrerade kontroll över hur dennes personuppgifter hanteras samt möjlighet att utöva vissa rättigheter kopplade till sin personuppgiftshantering. Dessa rättigheter innefattar rätt till registerutdrag, rätt till rättelse, rätt till radering (s.k. ”rätten att bli glömd”), rätt till begränsning, rätt till invändning, rätt att slippa automatiserad behandling och rätt till dataportabilitet.

Bolaget ska underlätta utövandet av den registrerades rättigheter. Vidare ska Bolaget utan onödigt dröjsmål och senast en månad efter att ha mottagit begäran tillhandahålla den registrerade information om de åtgärder som vidtagits med anledning av begäran. Information och åtgärder ska tillhandahållas kostnadsfritt så länge den registrerades begäran inte är uppenbart ogrundade eller orimliga, särskilt beaktat att begäran skulle vara tätt återkommande. I dessa fall får Bolaget ta ut en rimlig avgift för att täcka administrativa kostnader.
Underwritingansvarig / Ekonomiansvarig är ansvarig för att tillgodose inkommen begäran från registrerad.

Registerutdrag

Den registrerade har rätt att få ut ett registerutdrag över vilka/vilken personuppgiftsbehandling den registrerade är föremål för. Bolaget ska som regel lämna ut informationen inom en månad. I det fall begäran om registerutdrag anses vara orimlig och/eller ogrundad, exempelvis om den registrerade återkommer med begäran om registerutdrag gång på gång, har Bolaget rätt att ta ut en administrativ avgift. Bolaget kan också i sådana fall ha rätt att vägra lämna ut ett registerutdrag till den registrerade.

Registrerad kan få utdrag som grundar sig på en sökning på personens namn eller andra personuppgifter i Bolagets affärssystem SAHARA samt en allmän sökning på Bolagets server ”G”. Ett registerutdrag får inte ha en negativ inverkan på andras integritet. I praktiken innebär det exempelvis att Bolaget ska stryka över eventuell information om tredjeperson i det fall de förekommer i registerutdraget.

Rätt till rättelse

Den registrerades rätt till rättelse innebär att Bolaget vid en begäran från en registrerad, utan onödigt dröjsmål, ska rätta felaktiga personuppgifter om den registrerade och sedan informera den registrerade om att rättelsen är genomförd.

Rätt till radering

GDPR innefattar en rätt för den registrerade att få sina personuppgifter raderade under vissa omständigheter:

- om ändamålet med behandlingen har upphört,
- om den registrerade återkallar sitt samtycke,
- om behandlingens ändamål baseras på direktmarknadsföring,
- om behandlingen av den registrerades personuppgifter saknar laglig grund eller radering av personuppgifter krävs för att uppfylla en rättslig skyldighet.

Vidare krävs det, i det fall den registrerades personuppgifter har lämnats ut till tredje part och den registrerade kräver radering, att även den tredje parten blir informerad om raderingen.

Rätt till invändning

Den registrerade har rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne som grundar sig på en intresseavvägning. Bolaget får då inte längre behandla personuppgifterna och måste därmed radera dessa, såvida Bolaget inte kan påvisa att det föreligger tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om uppgifterna är nödvändiga för att fastställa, utöva eller försvara rättsliga anspråk.

Rätt till begränsning

Den registrerade har rätt att kräva att Bolagets behandling av personuppgifter begränsas under vissa förutsättningar. Med begränsning avses att Bolaget ska markera personuppgifterna så att dessa endast behandlas för vissa avgränsade syften. Rätten till att få personuppgift begränsad kan exempelvis aktualiseras i samband med att en registrerad invänder mot en behandling som görs med stöd av en intresseavvägning. Om den registrerade i samband med en sådan invändning även begär begränsning av uppgifterna så måste Bolaget skyndsamt ta ställning till om det har rätt att behandla uppgifterna.

Rätt till dataportabilitet

Den registrerade har rätt att få sina personuppgifter överförda från Bolaget till en annan personuppgiftsansvarig.

Rätt att slippa automatiserat beslutsfattande inkl. profilering

Den registrerade har rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, profilering inbegripet, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne.

Lagring och gallring

I enlighet med GDPR och de grundläggande principerna för behandling av personuppgifter ska personuppgifter enbart behandlas och lagras för de ändamål som de ursprungligen inhämtades för. Vidare ska uppgifterna inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen, s.k. lagringsminimering. Det krävs därmed att Bolaget har bra rutiner och instruktioner för gallring. Att spara personuppgifter endast för att ”de kan vara bra att ha” är inte tillåtet.

Bolagets lagrings och gallringsrutiner finns samlade i Bolagets Instruktion för lagring och gallring.

Personuppgiftsbiträdesavtal

GDPR stadgar att en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för någon annans räkning är ett personuppgiftsbiträde. Vid anlitande av ett personuppgiftsbiträde krävs det ett skriftligt personuppgiftsbiträdesavtal. Det är Bolagets skyldighet att enbart anlita personuppgiftsbiträden som uppfyller kraven i GDPR.

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.

Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som leder till att personuppgifter:

- Förstörs, oavsiktligt eller olagligt
- Går förlorade eller ändras
- Avslöjas till någon obehörig

Det har ingen betydelse om incidenten sker oavsiktligt eller med avsikt. En personuppgiftsincident kan bedömas vara allvarlig när nedanstående kriterier uppfylls:

- Konfidentiell eller strikt konfidentiell information omfattas
- Incidenten kan leda till allvarliga konsekvenser för en/flera individer
- Incidenten innefattar en stor mängd personuppgifter
- Incidenten involverar ett stort antal individer

Om en personuppgiftsincident inträffar har Bolaget en skyldighet att rapportera incidenten till Datainspektionen inom 72 timmar från det att incidenten har skett. I de fall där personuppgiftsincidenten kan anses ha en hög risk för den registrerades fri- och rättigheter har Bolaget även skyldigheten att informera de berörda registrerade. Oavsett om personuppgiftsincidenten föranleder en anmälan till Datainspektionen ska Bolaget alltid dokumentera det inträffade.

Samtliga personuppgiftsincidenter/misstänkta personuppgifter ska rapporteras till Underwritingansvarig / Ekonomiansvarig för vidare utredning, dokumentering samt eventuell rapportering till Datainspektionen.

Behandling av personuppgifter utanför EU/EES

Bolaget behandlar huvudsakligen personuppgifter inom EU/EES, men i undantagsfall kan dessa uppgifter överföras till, och behandlas i, land utanför EU/EES, s.k. tredjeland. Detta gäller till exempel när det görs enstaka överföringar till eller från en mottagare utanför EU/EES.

När Bolaget hanterar överföringar till tredjeland ska särskild uppmärksamhet visas och därtill ska rimliga legala, tekniska och organisatoriska åtgärder vidtas, för att säkerställa att den registrerades data hanteras säkert och med en lämplig skyddsnivå som är jämförbar med och i samma nivå som det skydd som erbjuds inom EU/EES. Vidare ska den registrerade informeras om att dennes personuppgifter i samband med transaktionen, överförs till tredjeland.