

Fullmaktskollen.se - Informationssäkerhet

FMK:s policy för Informationssäkerhet syftar till att säkerställa att information som lämnas till FMK, kommunikation mellan FMK och dess Uppdragsgivare, samt hanteringen av informationen av FMK och dess underleverantörer sker på ett korrekt och säkert.

FMK ska löpande tillse att säkerheten, i den digitala infrastruktur som ägs och administreras av FMK, Fullmaktskollen.se, upprätthålls och uppdateras med vid var tid lämplig teknik som tar i beaktande aktuella tekniska hotbilder.

1 Allmänt - tillämpningsområde

FMK:s Uppdragsgivare är verksamma inom livförsäkrings- och pensionsområdet och är bl. a. försäkringsgivare och försäkringsförmedlare. Det finns inte någon lag som reglerar allmän försäkringssekretess. För att säkerställa att information om Fullmakt inte obehörigen röjs, ska FMK tillse att FMK och dess underleverantörer följer dessa riktlinjer.

För att upprätthålla en säker och korrekt hantering av den information som distribueras via Tjänsten ska Uppdragsgivare att för dess utnyttjande av Tjänsten via Uppdragsgivarens egna IT-system tillse att erforderlig behörighetskontroll sker enligt nedan p. 1.1.

1.1 Behörighetskontrollsystem

Tjänsterna som tillhandahålls via den digitala infrastruktur som ägs och administreras av FMK, Fullmaktskollen.se, är åtkomlig via ett antal webbapplikationer (se p. 4).

Det ska finnas behörighetskontrollsystem för åtkomst till uppgifterna i Tjänsterna. För medarbetare hos FMK eller dess underleverantörer ges åtkomst endast till utsedda behöriga personer och loggning sker då dessa behöriga personer bereds tillträde till Fullmaktskollen.se.

När Fullmaktsgivaren loggar in på Fullmaktskollen.se verifieras dennes identitet med godkänd e-legitimation.

Uppdragsgivare, vilka genom inloggning genom integrerat webbgränssnitt, använder Tjänsterna, ska tillse att ett behörighetskontrollsystem finns för Uppdragsgivarens åtkomst. Loggfiler för identifiering av Uppdragsgivarens behöriga personer som använt Tjänsterna genom integrerat webbgränssnitt ska bevaras och förevisas för FMK på begäran.

1.2 Utlämnande av uppgifter

Uppgifter om Fullmakt, får endast lämnas ut i enlighet med de villkor som gäller för Tjänsten, i enlighet med Bilaga A, Processbeskrivning eller till

underleverantörer i samband med åtgärder för säkerställande av funktionaliteten i Tjänsterna.

För behandling av personuppgifter ska all sådan behandling ske i enlighet med vid var tid gällande personuppgiftsbiträdesavtal.

2 Säkerhetskrav - Fullmaktskollen.se

2.1 Kryptering

Datakommunikation innehållande uppgifter hänförliga till en Fullmakt som administreras av FMK via Fullmaktskollen.se ska skyddas genom kryptering samt ske i enlighet med den av FMK vid var tid angivna säkerhetsstandarden¹. I och med att nya sårbarheter upptäcks i kryptoalgoritmer och protokoll kan kraven komma att förändras.

Kommunikation med Fullmaktskollen.se:s API ska ske via HTTPS med klientcertifikatsautentisering. Alla certifikat ska vara utgivna av en av bägge kommunikationsparter godkänd Certificate Authority². Privata nycklar ska hanteras varsamt och certifikat revokeras vid misstankar om oavsiktlig spridning.

2.2 Brandvägg

Fullmaktskollen.se ska vara skyddat av brandvägg där enbart den trafik som anses nödvändig för att tillhandahålla Tjänsterna och upprätthålla dess funktionalitet ska fungera släpps igenom. Kommunikation med Fullmaktskollen.se ska ske över internet via en säker anslutning enligt avsnitt 2.1 Kryptering. Databaser i Fullmaktskollen.se finns i Microsoft Azure vilket kan komma att förändras över tiden. Mer information om skyddet finns hos Microsofts Azure Trust Center³.

2.3 Säkerhetsåtgärder

2.3.1 Territoriell tillämpning

Allt data som FMK förvaltar för Tjänsterna i Fullmaktskollen.se, finns inom EU:s gränser i en s.k. molnmiljö. Överföring av data utanför EU:s gränser kan komma ske vid bl. a. e-postkommunikation samt visst tekniskt underhåll och support. När så sker får det endast ske om sådan överföring regleras av standardkontraktsklausuler och så kallade Binding Corporate Rules (BCR) som följer EU:s vid var tid gällande lagstiftning.

¹ Drift tillhandahålls av Softtronic AB som är säkerhetscertifierade enligt ISO 27001

² Enl. Microsoft Trusted Root Certificate Program, <https://gallery.technet.microsoft.com/Trusted-Root-Certificate-123665ca>

³ <https://azure.microsoft.com/en-us/support/trust-center/>

2.3.2 Skadlig kod

FMK ska vidta åtgärder för att upptäcka och förebygga angrepp från virus och andra skadliga program genom att kontinuerligt söka igenom källkod och binärer tillhörande systemet. Uppdragsgivare ansvarar för att de filer som skickas in i systemet är fria från skadlig kod.

2.3.3 Säkerhetsuppdateringar

Den programvara som integrerar mot gränssnittet samt bakomliggande infrastruktur ska kontinuerligt hållas uppdaterade med av respektive programvaruleverantör fortfarande supportad mjukvara samt de säkerhetsuppdateringar som släppts för dessa.

2.4 Belastning

Uppdragsgivarens system som integrerar mot Fullmaktskollen.se ska anpassas efter de möjligheter som erbjuds av tjänstegränssnittet. Integrationer ska vara utformade så att de inte ställer frågor eller belastar systemet i onödan, se avsnitt 2.6 Funktionella krav.

2.5 Förändring av gränssnitt

FMK förbehåller sig rätten att fasa ut gamla versioner av applikationsgränssnittet för att kunna hålla plattformen uppdaterad. Uppdragsgivare kommer att få information minst 3 (tre) månader i förväg om vilka gränssnitt som tas bort och vad som ersatt dessa.

2.6 Funktionella krav

2.6.1 Uppdatering av eget fullmaktsregister

Uppdragsgivare kan anropa Fullmaktskollen.se:s API för att inhämta information om det egna fullmaktsbeståndet. Vid ändringar i fullmaktsbeståndet kommer en notifiering skickas till Uppdragsgivaren, vilket gör att Uppdragsgivarens register kan hållas uppdaterat. Dessa notifieringar skickas kontinuerligt av systemet och kan vid misslyckanden skickas om enligt avsnitt 2.6.3. Omsändning.

Uppdragsgivare kan initialt, och vid behov, läsa in hela sitt fullmaktsbestånd från Fullmaktskollen.se genom att iterera över de Fullmakter som registrerats i systemet. Endast Fullmakter där det föreligger ett kundförhållande eller ett kundförhållande är omedelbart förestående mellan Uppdragsgivaren och Fullmakts-givaren som omfattas av den aktuella Fullmakten får itereras av respektive Uppdragsgivare. För att begränsa belastningen på systemen finns även möjligheten att iterera över enbart de Fullmakter som ändrats mellan en given start- och sluttidpunkt.

2.6.2 Valideringsfel

Den information som skickas mellan Fullmaktskollen.se och integrerade system ska valideras av mottagaren. Om informationen inte går att tolka eller anses ogiltig ska systemet inte motta informationen.

2.6.3 Omsändning

I de fall Fullmaktskollen.se misslyckas med att meddela integrerade system om ändringar som skett i fullmaktsbeståndet kommer systemet försöka skicka om meddelandet. Detta sker enligt den vid var tid gällande gällande policyn för omsändning, vilket finns dokumenterat i Fullmaktskollen.se:s API-specifikation.

2.6.4 Ansvarsfördelning

Part, vars system integrerar med Fullmaktskollen.se ansvarar för att information som skickas till övriga system är korrekt samt för att logga information om anrop som utför ändringar i systemet.

3 Hantering av Personuppgifter

3.1 Instruktioner för behandling av personuppgifter

FMK behandlar genom tillhandahållandet av Tjänsterna personuppgifter. FMK är personuppgiftsansvarig för behandling av kontaktuppgifter som FMK inhämtat via fullmaktshanvaren eller administratör hos Uppdragsgivare.

Uppgifter om Fullmakter samt kunduppgifter behandlas på uppdrag av dess Uppdragsgivare. FMK:s agerar då i egenskap av personuppgiftsbiträde för respektive personuppgiftsansvarig Uppdragsgivare. När personuppgifter behandlas på uppdrag av personuppgiftsansvarig Uppdragsgivare ska detta ske i enlighet med mellan parterna tecknat Personuppgiftsbiträdesavtal Bilaga D samt i enlighet med vid var tid gällande skriftliga instruktioner och/eller de särskilda föreskrifter personuppgiftsansvarig Uppdragsgivare meddelat FMK.

4 Fullmaktskollens säkerhetsarkitektur

Programvaran som används i Fullmaktskollen.se består bl. a. av ett flertal webbapplikationer. Applikationsgränssnittet spelar en central roll och hanterar alla anrop som läser eller skriver data från applikationsdatabasen. Kommunikation med tjänstegränssnittet sker med hjälp av ett betrott klientcertifikat, och de anrop som utför ändringar i databasen eller skickar ut extern information lagras för att kunna spåras i efterhand.

Fullmaktsgivare loggar in på Fullmaktskollen.se:s webbgränssnitt, antingen direkt genom BankID-inloggning hos FMK:s underleverantör, eller via Single-Sign On genom en SAML2 token från en BankID-inloggning ursprungligen avsedd för en Fullmaktshavares system.

