Fullmaktskollen.se – Specifikation med instruktioner för behandling av Personuppgifter

1 Syfte

Denna Bilaga 1 till det mellan parterna träffat Personuppgiftsbiträdesavtalet specificerar syftet med FMK:s behandling av Personuppgifter för Uppdragsgivarens räkning.

Specifikationen utgör även Uppdragsgivarens instruktion till FMK för behandling av Personuppgifter för Uppdragsgivarens räkning.

2 Ändamålet

FMK:s behandling av Personuppgifter sker i syfte att skapa en effektiv och säker rutin för överföring/visning av fullmakter mellan parter som anslutits till Fullmaktskollen, dels för att skapa en bättre möjlighet för enskilda individer att få en överblick över fullmakter som den enskilda individen utfärdat.

3 Registrerade

- Fullmaktsgivare för vilka Uppdragsgivaren erhållit Fullmakt,
- Försäkringstagare hos Uppdragsgivare,
- Enskilda individer vilka registrerat sina uppgifter på fullmaktskollen.se, samt
- Anställda hos Uppdragsgivare och Fullmaktsgivare registrerade som administratörer på fullmaktskollen.se.

4 Typ av Personuppgifter som överförs

De Personuppgifter som överförs är:

- namn
- personnummer
- kontaktuppgifter, såsom e-post och telefonnummer
- loggfiler

4.1 Känsliga Personuppgifter

Överföringen rör inga s.k. särskilda kategorier av personuppgifter (känsliga personuppgifter) i enlighet med Dataskyddsregleringen

5 Behandling – vem är ansvarig för vilka uppgifter

För de personuppgifter som behandlas av FMK finns flera aktörer som är personuppgiftsansvariga.

FMK – Personuppgiftsansvarig:

FMK är personuppgiftsansvarig för de personuppgifter som Fullmaktsgivare lämnar när denne registrerar sig på Fullmaktskollen.se, till exempel kontaktuppgifter, e-post, namn och telefonnummer. Detsamma gäller personuppgifter avseende administratörer hos organisationer Fullmaktshavare och/eller BKP, anslutna till Fullmaktskollen.se och som lämnas till FMK för att kunna utnyttja tjänsten.

FMK Personuppgiftsbiträde - Fullmaktshavaren personuppgiftsansvarig:

För de personuppgifter som används i fullmakter och återkallelser är fullmaktshavaren personuppgiftsansvarig.

FMK Personuppgiftsbiträde – Behörighetskontrollerande part personuppgiftsansvarig:

Uppdragsgivare som tar emot och granskar fullmakten är också personuppgiftsansvariga för personuppgifterna i fullmakten som rör kund hos dem liksom för kunduppgift som skickas från sådan Uppdragsgivare vid förfrågan om fullmakt.

Behandling av Personuppgifter kommer ske i syfte att överföra fullmakts- och kontaktuppgifter i enlighet med villkoren i Uppdragsavtalet, se Bilaga A Processbeskrivning, samt för att upprätthålla funktionaliteten i de tjänster som tillhandahålls samt för fakturerings- och statistikändamål.

6 Tekniska och organisatoriska säkerhetsåtgärder

6.1 Åtkomstskydd

När datorutrustning och löstagbara datamedier hos Personuppgiftsbiträdet inte står under uppsikt ska utrustningen och medierna låsas in för att skyddas mot obehörig användning, påverkan och stöld. I annat fall ska Personuppgifterna krypteras.

För det fall eventuella bärbara datorer används vid Behandlingar ska Personuppgifterna på fasta och löstagbara lagringsmedier alltid vara krypterade.

I det fall att databasen ligger i molntjänst ska lösningar där kryperingsnyckeln förvaras utan åtkomst för molntjänstleverantören vara implementerad (Customer-Managed-Key).

Krypteringsnycklarna ska förvaras i ett s.k. "Key Vault" som är en speciell server som är placerad inom EU. I ”Key Vault” kan molntjänstleverantören varken se eller extrahera krypteringsnyckeln.

6.2 Säkerhetskopia

Personuppgifterna ska regelbundet överföras till säkerhetskopior. Kopiorna ska förvaras avskilt och väl skyddade så att Personuppgifterna kan återskapas efter en störning. Personuppgiftsbiträdet ska ha en rutin för test av återläsning.

6.3 Behörighetskontroll

Ett tekniskt system för behörighetskontroll ska styra åtkomsten till Personuppgifterna för Personuppgiftsbiträdet. Behörigheten ska begränsas till dem som behöver uppgifterna för sitt arbete. Användaridentitet och lösenord ska vara personliga och får inte överlåtas på någon annan. Det ska finnas rutiner för tilldelning och borttagande av behörigheter.

För det fall det, i samband med supportärende, är nödvändigt att exponera personuppgifter för underleverantör, tillika underbiträde, i tredje land, ska alltid särskilt samtycke inhämtas av berörd Uppdragsgivare tillika personuppgiftsansvarig innan sådan behandling får ske.

6.4 Loggning

Åtkomst till Personuppgifter ska kunna följas upp i efterhand genom en logg eller liknande underlag. Underlaget ska kunna kontrolleras av Personuppgiftsbiträdet och återrapporteras till den Personuppgiftsansvarige.

6.5 Datakommunikation

Anslutning för extern datakommunikation ska skyddas med sådan teknisk funktion som säkerställer att uppkopplingen är behörig.

Personuppgifter som överförs via datorkommunikation utanför lokaler som kontrolleras av Personuppgiftsbiträdet ska skyddas med kryptering.

6.6 Utplåning

När fasta eller löstagbara lagringsmedier som innehåller Personuppgifter inte längre ska användas för sitt ändamål ska Personuppgifterna raderas på sådant sätt att de inte kan återskapas.

6.7 Reparation och service

När reparation och service av datorutrustning, vilken används för att lagra Kunds Personuppgifter, utförs av annan än Personuppgiftsbiträdet, ska avtal som reglerar säkerhet och sekretess träffas med serviceföretaget.

Vid servicebesök ska servicen ske under Personuppgiftsbiträdets överinseende. Är detta inte möjligt ska lagringsmedier som innehåller Personuppgifter avlägsnas.

Service via fjärrstyrd datakommunikation får endast ske efter säker elektronisk identifiering av den som utför servicen. Servicepersonal ska ges åtkomst i systemet endast vid servicetillfället. Finns separat kommunikationsingång för service ska den vara stängd när service inte pågår.

7. Lagring och gallring

Personuppgifter som behandlas ska lagras och gallras i enlighet med Uppdragsavtalet samt respektive Uppdragsgivares särskilda instruktioner.

8. Särskilda instruktioner

Utöver vad som följer av Uppdragsavtalet, Personuppgiftsbiträdesavtalet jämte denna specifikation ska FMK vid behandling av Personuppgifter för Uppdragsgivaren beakta följande:

Gallringsrutiner gällande programvaran och dess förvaltning för den digitala fullmaktsnoden fullmaktskollen.se

Gallring av personuppgifter ska ske löpande för att varken behandling eller lagring av uppgifter ska ske längre än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Nedanstående gallringsrutiner ska tillämpas på de behandlingar/personuppgifter som sker i programvaran och förvaltningen för Fullmaktskollen.se

De behandlingar där personuppgifter förekommer raderas och gallras enligt följande:

Ej underskrivna fullmakter

Ej underskrivna fullmakter ska gallras efter 30 dagar.

Skäl: En period om 30 dagar bedöms krävas för att fullmaktsgivaren ska ges tillräcklig tid för att skriva under en fullmakt. Detta sker inte alltid omedelbart på grund av olika skäl, t.ex. resor eller sjukdom.

Inaktiva fullmakter

Inaktiva fullmakter är fullmakter som inte längre är giltiga. Sådana fullmakter ska gallras efter elva år.

Skäl: Gallringstiden är satt utifrån gällande preskriptionstider i försäkrings-verksamhet plus ett år enligt praxis. Uppgift om en inaktiv fullmakt kan komma att ha betydelse i en eventuell tvist mellan fullmaktsgivare/fullmaktshavare/BKP.

Backuper av systemet

Dagliga backuper av programvarans huvudsakliga lagringsmedium ska gallras på löpande tolvmånadersbasis.

Skäl: En intresseavvägning har gjorts varvid det kan konstateras att antalet registrerade personuppgifter totalt är förhållandevis omfattande men att

personuppgifterna i sig inte är några känsliga uppgifter. Återläsningar på sådant vis där personuppgifter utelämnas skulle inverka menligt på möjligheterna att använda systemets information för en återställning till tidigare version och/eller vid en eventuell rättslig tvist.

Tekniska loggar/annan registrering i syfte att möjliggöra och förenkla felsökning i systemet samt förenkla återställning vid eventuella incidenter

Dessa registreringar ska gallras på löpande tolvmånadersbasis.

Skäl: Denna typ av registreringar innehåller personuppgifter av icke känslig karaktär, exempelvis namn, personnummer, telefonnummer och e-postadresser. Skälen till gallringsperioden överensstämmer med ovan gallring av back-up.

Revisionsloggar/annan registrering som är bevisbärande för vem som utfört vilka handlingar i systemet kopplat till att skapa, justera, skicka ut och radera fullmakter samt individers inloggningar till systemet.

Dessa registreringar ska gallras efter elva år.

Skäl: Denna typ av registreringar innehåller personuppgifter relaterade till dessa handlingar, exempelvis namn, personnummer, telefonnummer och e-postadresser. Skälen till gallringsperioden överensstämmer med ovan gallring av inaktiva fullmakter.

Fullmaktskollen

9. Underbiträden

Samtliga de underleverantörer som behandlar personuppgifter såsom underbiträden till Fullmaktskollen i enlighet med Avtalet är angivna nedan.

Vid anlitande av nytt underbiträde eller förändringar i övrigt avseende behandlingen ska Fullmaktskollen tillse att sådan förändring sker i enlighet med p. 11 i parternas Personuppgiftsbiträdesavtal samt tillse att nedanstående lista är aktuell. Lista över vid var tid aktuella underleverantörer finns tillgänglig på *www.fullmaktskollen.se*

Bolagsnamn och org.nr	Kategorier av registrerade	Kategorier av personuppgifter*	Syftet med behandlingen	Grunden för behandlingen**	Plats *** Land****
Microsoft Corporation, Registration Number (CRN): 256796 Microsoft Ireland Operations Limited, One Microsoft Place, Dublin, Irland	Se punkt 3 ovan	Se punkt 4 ovan	Se punkt 2 ovan - Tillhandahållande av drift av och miljö för tjänsten.	Personuppgiftsbiträdesavtal ingånget mellan FMK och Uppdragsgivarna. Underbiträdesavtal ingånget mellan FMK och Microsoft.	EU/EES Nederländerna Sverige
Softronic AB, 556249-0192	Se punkt 3 ovan	Se punkt 4 ovan	Se punkt 2 ovan Tillhandahållande av drift av och miljö samt mejl- och sms-tjänster för tjänsten	Personuppgiftsbiträdesavtal ingånget mellan FMK och Uppdragsgivarna. Underbiträdesavtal ingånget mellan FMK och Leverantören 180425	EU/EES Sverige
Mailjet SAS 13 rue de l'Aubrac Paris, Ile de France 75012, Frankrike	Se punkt 3 ovan BKP:er för uppdragsgivaren Fullmaktsgivare för uppdragsgivaren	Se punkt 4 ovan -E-postadresser till fullmaktsgivare Innehåller namn, Listor med studsade, blockerade/ej nådd och felaktiga E-postadresser Inga personnummer eller andra särskilda kategorier av PU.	Se punkt 2 ovan Mejlutskick till BKP:er som inte är digitalt anslutna till tjänsten Kommunicera via E-post för kommunikation med de registrerade i tjänsten	Personuppgiftsbiträdesavtal ingånget mellan FMK och Uppdragsgivarna. Underbiträdesavtal ingånget mellan FMK och Leverantören samt underbiträdesavtal mellan Leverantören och Mailjet. https://www.mailjet.com/dpa/ https://www.mailjet.com/wp-content/uploads/2020/03/Annex-1_-List-of-Subcontractors-EN-VAL.pdf	EU/EES Tyskland/Belgien
Link mobility AB Götgatan 78, 118 30 Stockholm Org nr: 556532-6401	Se punkt 3 ovan Fullmaktsgivare för uppdragsgivaren	Se punkt 4 ovan Namn och telefonnummer Inga personnummer eller andra särskilda kategorier av PU.	Se punkt 2 ovan Kommunicera via SMS med de registrerade i tjänsten.	Personuppgiftsbiträdesavtal ingånget mellan FMK och Uppdragsgivarna. Underbiträdesavtal ingånget mellan FMK och Leverantören samt underbiträdesavtal mellan Leverantören och Link mobility Link mobilitys underbiträden är per 2021-07-09 följande: https://linkmobility.com/wp-content/uploads/2021/07/LINK-subprocessors-list-Sweden-09July2021.pdf	EU/EES Irland/Tyskland/Frankrike /Nederländerna
Atlassian Pty Ltd (ABN 102 443 916), Level 6, 341 George StreetSydney NSW 2000 Australia	Se punkt 3 ovan	Se punkt 4 ovan	Se punkt 2 ovan -Tillhandahållande av verktyget JIRA som bl.a. används av förvaltningen som stöd för ärendehantering/support där personuppgifter kan förekomma.	Personuppgiftsbiträdesavtal ingånget mellan FMK och Uppdragsgivarna. Underbiträdesavtal ingånget mellan FMK och Leverantören samt underbiträdesavtal mellan Leverantören och Atlassian Pty Ltd. All behandling sker via AWS Europe molntjänst.	Personuppgiftsbehandling sker endast från datacenter inom EU (Amazon Web Services – Dublin, Irland och Frankfurt, Tyskland).
CGI Sverige AB, 556337-2191	Se punkt 3 ovan	Se punkt 4 ovan Banktillhörighet IP-adress	Säker identifiering genom Bank-iD/E-legitimation	Personuppgiftsbiträdesavtal ingånget mellan FMK och Uppdragsgivarna. Underbiträdesavtal ingånget mellan FMK och CGI 190218, uppdaterat 250430	EU/EES Sverige
Det noteras att Leverantören anlitar sådana e-legitimationsutfärdare, som kunden aktivt valt, som underleverantör(er) för tillhandahållande av tjänsterna. E-legitimationsutfärdare får ta del av personuppgifter men är ej att anses som underbiträden. För CGI:s leverans av eID-tjänst till Fullmaktskollen är detta: ” Swedbank AB, org. nr 502017-7753 ”					

Bolagsnamn och org.nr	Kategorier av registrerade	Kategorier av personuppgifter*	Syftet med behandlingen	Grunden för behandlingen**	Plats *** Land****
XBP Europe AB, 556455-0373	Se punkt 3 ovan	Se punkt 4 ovan	Dokument- digitalisering - scanningtjänst	Personuppgiftsbiträdesavtal ingånget mellan FMK och Uppdragsgivarna. Underbiträdesavtal ingånget mellan FMK och Leverantören 180516	Inom EU/EES Sverige
Svensk Försäkring Administration AB 556668-2216	Se punkt 3 ovan	Se punkt 4 ovan	Administrativa stödtjänster inom IT	Personuppgiftsbiträdesavtal ingånget mellan FMK och Uppdragsgivarna. Underbiträdesavtal ingånget mellan FMK och SFAB 180618.	EU/EES Sverige
Truesec Group AB 556690-8074	Se punkt 3 ovan	Se punkt 4 ovan	Säkerhetsövervakning Managed Detection and Response (**"MDR"**) samt standby CSIRT	Personuppgiftsbiträdesavtal ingånget mellan FMK och Uppdragsgivarna. Underbiträdesavtal ingånget mellan FMK och Leverantören 261104	EU Sverige, Danmark, Finland, Tyskland

*typ av uppgifter och om känsliga personuppgifter behandlas jfr art 9 GDPR
** hänvisning till aktuellt PuB-avtal, standardklausuler m.m.
*** inom eller utanför EES
****för IKT-tjänst specificeras primärt land/länder för uppgiftsbehandling