

Kreditfondens behandling av personuppgifter i egenskap av personuppgiftsbiträde – personuppgiftsbiträdesavtal; utgör en integrerad del av kund- / affärsrelation

1. Uppdragsgivarens åtagande

Uppdragsgivaren är personuppgiftsansvarig för den behandling av personuppgifter som Kreditfonden utför inom ramen för kund- / affärsrelationen och ansvarar således för att behandlingen sker i enlighet med gällande rätt. Det innebär att uppdragsgivaren ansvarar för att denne äger rätt att föra över uppgifterna till Kreditfonden och låta Kreditfonden behandla uppgifterna inom ramen för kund- / affärsrelationen.

I kund- / affärsrelation samt bifogade [Bilaga 1](#) och [Bilaga 2](#) finns en närmare beskrivning av den behandling som Kreditfonden förväntas utföra samt under vilka förutsättningar. Denna beskrivning utgör uppdragsgivarens instruktioner till Kreditfonden.

2. Kreditfondens allmänna åtagande

Kreditfonden ska inom ramen för kund- / affärsrelationen behandla personuppgifter i den utsträckning och på det sätt som framgår av uppdragsgivarens instruktioner, dvs. i enlighet med vad som framgår av kund- / affärsrelation och underbilagor till detta personuppgiftsbiträdesavtal och kund- / affärsrelation.

3. Säkerhetsåtgärder

Kreditfonden vidtar lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken och för att skydda de personuppgifter som vi behandlar mot personuppgiftsincidenter. Endast den personal hos Kreditfonden som behöver tillgång till personuppgifterna för att utföra kund- / affärsrelationen har tillgång till dem. De är vidare skyldiga att iakttäta sekretess som inte är mindre omfattande än det sekretessåtagande som följer av kund- / affärsrelation. En närmare beskrivning av Kreditfondens säkerhetsåtgärder framgår av [Bilaga 3](#).

För det fall en personuppgiftsincident inträffar kommer Kreditfonden, så snart Kreditfonden fått kännedom om den, att utan onödigt dröjsmål skriftligen underrätta Uppdragsgivaren. Kreditfonden kommer i samband därmed och så snart som möjligt att tillhandahålla Uppdragsgivaren en beskrivning av personuppgiftsincidentens art, kategorier av och antalet registrerade som berörs, samt kategorier av och antalet personuppgiftsposter som berörs; de sannolika konsekvenserna av personuppgiftsincidenten; samt en beskrivning av de åtgärder som vi, i förekommande fall, redan har vidtagit eller avser att vidta för att åtgärda personuppgiftsincidenten och/eller för att begränsa dess eventuella negativa effekter.

4. Anlitande av underbiträde

Såsom följer av avtal och/eller av bifogade allmänna villkor har Kreditfonden rätt att anlita underleverantör, underkonsult eller andra tredje parter ("Underbiträden") för att behandla personuppgifter för Uppdragsgivarens räkning. Kreditfonden har ingått personuppgiftsbiträdesavtal med dessa Underbiträden. Underbiträdena uppfyller kraven i tillämplig dataskyddslagstiftning. Kreditfonden är fullt ansvariga gentemot Uppdragsgivaren för Underbiträdenas skyldigheter.

5. Överföring av personuppgifter till tredje land

Kreditfonden har rätt att överföra personuppgifter som tillhör Uppdragsgivaren till ett tredje land (en stat som inte ingår i EU eller är ansluten till EES), under förutsättning att (i) det tredje landet säkerställer en adekvat skyddsnivå för personuppgifter enligt ett beslut meddelat av EU-kommissionen, (ii) Kreditfonden säkerställer att det finns lämpliga skyddsåtgärder på plats enligt tillämplig personuppgiftslagstiftning, t.ex. standardiserade dataskyddsbestämmelser som antagits av EU-kommissionen, som omfattar överföringen och behandlingen av personuppgifterna; eller (iii) om något annat undantag enligt tillämplig personuppgiftslagstiftning föreligger som omfattar behandlingen av personuppgifter.

6. Registrerades rättigheter

Uppdragsgivaren är ansvarig för att bedöma om en registrerads begäran om att få utöva sina rättigheter är berättigad i förhållande till gällande lag och för att lämna instruktioner till Kreditfonden vilket stöd Uppdragsgivaren önskar för att uppfylla den registrerades begäran. Kreditfonden är berett att tillhandahålla den information som Uppdragsgivaren behöver i samband med en begäran från en registrerad under förutsättning att Kreditfonden har tillgång till informationen. Kreditfonden är vidare berett att, i samband med begäran om rättelse, radering, behandlingsbegränsning och dataportabilitet, vara uppdragsgivaren behjälplig, i den mån det är möjligt, i att vidta åtgärderna.

Kreditfonden ska utan onödigt dröjsmål informera uppdragsgivaren om klagomål och andra meddelanden som Kreditfonden erhållit från en registrerad. Uppdragsgivaren ansvarar därefter för hanteringen och är den som tillhandahåller information till eller ansvarar för vidtagna åtgärder i förhållande till den registrerade.

7. Uppdragsgivarens rätt till information vid konsekvensbedömningar och förhandsråd

Kreditfonden ska på Uppdragsgivarens begäran bistå denne med nödvändig information som Kreditfonden har tillgång till, för att uppdragsgivaren ska kunna uppfylla sina skyldigheter att genomföra konsekvensbedömning och förhandssamråd med berörda tillsynsmyndigheter avseende den behandling av personuppgifter som omfattas av detta personuppgiftsbiträdesavtal.

8. Återlämnande av personuppgifter

Uppdragsgivaren har rätt att vid kund- / affärsrelations upphörande begära radering av eller återlämnande av personuppgifter som Kreditfonden behandlar som personuppgiftsbiträde. Notera dock att personuppgifter i Kreditfondens arbetspapper kommer att arkiveras, dels för att tillsynsmyndigheter ska kunna granska utfört uppdrag i efterhand vid kvalitetskontroller och efter eventuella anmälningar, dels för att Kreditfonden ska kunna fastställa, göra gällande eller försvara sig mot rättsliga anspråk. Personuppgifterna kommer att raderas efter elva (11) år. För denna behandling är Kreditfonden ensam personuppgiftsansvarig.

9. Ansvar

Bestämmelserna avseende ansvar i kund- / affärsrelation ska äga motsvarande tillämpning på detta personuppgiftsbiträdesavtal.

10. Granskning

Uppdragsgivaren har rätt att genomföra inspektion av de tekniska och organisatoriska åtgärder som Kreditfonden vidtar för att uppfylla sina skyldigheter enligt personuppgiftslagstiftningen. Till undvikande av missförstånd ska en inspektion endast avse sådan information som är nödvändig för att Uppdragsgivaren ska kunna fastställa att vi vidtar lämpliga tekniska och organisatoriska åtgärder för uppfylla Kreditfondens skyldigheter enligt detta åtagande och ska under inga omständigheter omfatta annan information rörande Kreditfondens verksamhet som inte är av betydelse för Kreditfondens behandling av personuppgifter för uppdragsgivarens räkning. Inspektion ska genomföras av en av båda parter gemensamt utsedd tredje part. Den tredje parten ska underteckna en sekretessförbindelse avseende all information som den tredje parten får del av inom ramen för inspektionen. För det fall uppdragsgivaren önskar utnyttja sin rätt till inspektion ska Uppdragsgivaren skriftligen meddela Kreditfonden detta minst trettio (30) dagar i förväg. Uppdragsgivaren bär kostnaderna för den tredje partens arbete och utlägg. I övrigt bär parterna sina respektive kostnader som uppstår i samband med en inspektion.

Bilaga 1
BESKRIVNING AV BEHANDLINGEN AV PERSONUPPGIFTER SOM SKER INOM RAMEN FÖR KUND- / AFFÄRSRELATIONEN

Kategorier av Registrerade	Kategorier av Personuppgifter	Ändamål med Behandlingen	Behandlingar av Personuppgifter	Platser	Bevarande av Personuppgifter
Kunder (Investerare / låntagare)	<p>Uppgifter kopplade till förvaltning av alternativ investeringsfond i enlighet med lagen (2013:561): Namn, personnummer, adress, e-mail, kreditstatus, bankkonto, depåinstitut, depå, försäkringsnummer, innehav, kredituppgifter, köphistorik, kvalitetsutvärdering.</p> <p>Uppgifter till följd av svensk eller utländsk lag, myndighetsföreskrift, handelsregler eller avtal/villkor för visst värdepapper.</p>	<p>För att genomföra förvaltning av alternativ investeringsfond i enlighet med lagen (2013:561).</p> <p>Personuppgifter kommer att användas i den mån de är relevanta för ovan.</p>	<p>Information, inklusive personuppgifter, inhämtas på fil från kund. För detta används systemen MS 365, alternativt ett lagringsmedium som bestäms tillsammans med kund. Microsoft Excel används för vissa beräkningar. Temporär lagring sker på Kreditfondens servrar hos MS 365 och på gemensamma arbetsytor i Google Drive.</p>	<p>Personuppgifterna behandlas av Kreditfonden i Sverige.</p> <p>MS 365 och Google-lagring sker såväl inom som utanför EU/EES – ändamålsenliga skyddsåtgärder enligt Personuppgifts-biträdesavtalets avsnitt 5 har vidtagits.</p>	<p>Personuppgifter i Kreditfondens arbetspapper kommer att arkiveras i elva (11) år, dels för att tillsynsmyndigheter ska kunna granska utfört uppdrag i efterhand vid kvalitetskontroller och efter eventuella anmälningar, dels för att Kreditfonden ska kunna fastställa, göra gällande eller försvara sig mot rättsliga anspråk.</p> <p>Personuppgifter i övriga handlingar kommer, i enlighet med kundens instruktioner, att raderas eller återlämnas vid kund- / affärsrelations upphörande.</p>
Leverantörer/konsulter	<p>Uppgifter kopplade till försäljning och leverans av varor och tjänster till företaget: Namn, personnummer, adress, e-mail, bankkonto, kvalitetsutvärdering.</p>	Se ovan.	Se ovan.	Se ovan.	Se ovan.

Bilaga 2
FÖRTECKNING ÖVER UNDERBITRÄDEN

Underbiträde	Underbitrådets uppgift	Platser
Microsoft Ireland Operations Ltd, Dublin, Irland	Drift och underhåll av MS365 samt tillhandahållande av epost, kalender och arbetsverktyg	EU/EES och Tredje land https://products.office.com/sv-SE/where-is-your-data-located?ms.officeurl=datamaps&geo=Europe#Europe
Google Inc, Mountain View, California, USA	Tillhandahållande av arbetsverktyg	EU/EES och Tredje land https://www.google.com/about/datacenters/inside/locations/index.html
Sentat Asset Management AB, Box 16 357, 103 26 Stockholm	AIF-förvaltare	EU/EES och Tredje land http://www.sentat.se/
ISEC Group AB, Riddargatan 17, 114 57 Stockholm	Backoffice	EU/EES https://www.isec.com/
KPMG AB, Box 382 101 27 STOCKHOLM	Oberoende värdering	EU/EES https://home.kpmg.com/se/sv/home.html
Danske Bank A/S, Danmark, Sverige Filial, Norrmalmstorg 1, 111 46 Stockholm	Förvaringsinstitut	EU/EES https://danskebank.se/stora-foretag-och-institutioner/startside
Upplyningscentralen	Kredituppföljning	EU/EES https://www.uc.se/kredituppfoljning/
Euroclear Sweden AB, Box 191, 101 23 Stockholm	Central värdepappersförvarare	EU/EES https://www.euroclear.com/en.html
PWC Sverige AB Torsgatan 21, 113 21 Stockholm	Revision	EU/EES https://www.pwc.se/

Bilaga 3

TEKNISKA OCH ORGANISATORISKA SÄKERHETSÅRGÄRDER

1. Informationssäkerhetspolicy

Kreditfonden följer "Informationssäkerhetspolicy för Kreditfonden" och "Daglig informationssäkerhet".

2. Organisation av informationssäkerhetsarbetet

Kreditfondens VD är ansvarig för informationssäkerheten inom företaget och regelbundet rapporterar till styrelsen samt till Riskansvarig. Härutöver sker löpande avstämningar med företagets externa juristfunktion. Rollen som personuppgiftsombud innehas av VD.

3. Personalsäkerhet

I den utsträckning svensk lagstiftning tillåter utförs bakgrundskontroll av all personal före anställning. Detsamma gäller för personal som tillhandahålls av tredje part.

All ny personal informeras om sitt säkerhetsansvar och bekräftar skriftligen att de förbinder sig att följa alla tillämpliga riktlinjer och rutiner samt Kreditfondens krav på tystnadsplikt.

Minst en gång genomgår alla anställda och konsulter ett program för säkerhetsmedvetande samt en säkerhetsutbildning.

För underleverantörer är dokumentet "Kreditfondens tredjepartsleverantörer - Riktlinjer för informationssäkerhet" en integrerad del av avtalet.

4. Fysisk och miljörelaterad säkerhet

Serverlokaler är ändamålsenligt skyddade mot intrång, stöld, brand, vattenskador, strömavbrott och andra faror. Fysisk åtkomst till serverlokaler har begränsats till ett minimum av personal.

Fysisk åtkomst till kontorslokaler har begränsats till Kreditfondens personal. Besökare tas emot i en yttre zon. Kreditfonden har en "Clean Desk Policy".

Säkra behållare finns för omhändertagande av känslig pappersdokumentation.

5. Drift- och kommunikationssäkerhet

Alla persondatorer är utrustade med hårddiskryptering enligt senaste standard, lösenordskyddade, skärmläckare, personliga brandväggar, antivirusprogramvara och VPN.

Endast Kreditfondens utrustning kan få åtkomst till Kreditfondens nätverk.

Lösningar för säker delning av information med kunder finns tillgängliga. Kreditfonden förbjuder användning av tjänster som Dropbox, Box, Drive, etc. Kreditfonden har rutiner för säker radering av datamedia.

Radering av kundinformation utförs i enlighet med avtal med kund samt utifrån legala krav.

6. Styrning av åtkomst

Åtkomst till information baseras på användarens roll och ansvar. Behörighet ges utifrån principen att

endast den som behöver tillgång till informationen för att utföra en arbetsuppgift inom ramen för ett uppdrag får tillgång till den. Alla användarkonton är hänförliga till en enskild individ.

Beslut om åtkomst fattas av informationsägaren (för kundinformation är detta kund- och/eller uppdragsansvarig). Informationsägare går igenom användarbehörigheter minst årligen.

Kreditfonden har formella rutiner för att lägga till, ändra och ta bort användarkonton samt för att ändra logisk access när arbetsuppgifter förändras. Inaktiva användarkonton spärras med automatik. Vidare finns rutin för att dra tillbaka fysisk och logisk access för personal och konsulter som slutar vid Kreditfonden.

Antalet användarkonton med höga behörigheter, som systemadministratör och motsvarande, har nedbringats till ett minimum. Personal med tillgång till sådana användarkonton använder separata konton när de utför normala arbetsuppgifter.

Systemstöd tillämpas för tvingande lösenordsbyten, krav på lösenordsstruktur samt utelåsning efter misslyckade åtkomstförsök.

7. Incidenthantering

Kreditfonden har en formell incidenthanteringsprocess. Processen hanterar frågor såsom vem som ansvarar för vad och vad ansvaret innebär samt hur rapportering, klassificering och eskalering ska ske. Skulle en incident bestå i att lagar, regler eller avtalsförpliktelser har åsidosatts, finns risk- och/eller skadereducerande rutiner, samt rutiner för utredning och, i förekommande fall, för rapportering till kunder och tillsynsmyndighet.

I Kreditfondens obligatoriska utbildning inom säkerhetsområdet ingår hur en säkerhetsöverträdelse eller incident (inklusive personuppgiftsincident) ska identifieras och vem/vilka som i så fall ska kontaktas.

8. Hantering av verksamhetens kontinuitet

Kreditfonden har en kontinuitetsplan för verksamheten. Planen har kommunicerats till samtliga intressenter och uppdateras årligen. Vidare finns katastrofplaner för Kreditfondens IT-miljö. Planerna uppdateras årligen.

9. Efterlevnad

Kontroll av efterlevnad av ovan beskrivet regelverk, med löpande uppföljningar. Revisioner initieras även av Kreditfonden, exempelvis självutvärderingar, granskningar utförda av Kreditfondens internrevisionsenhet, tekniska säkerhetsgranskningar, intrångstester, riskanalyser av nya lösningar m.m. Rapportering av informationssäkerhetsfrågor sker till VD samt Styrelsen.