# Policy om behandling av personuppgifter

December 2024

## Inledning och syfte

Syftet med denna policy är att fastställa de grundläggande principer som ska gälla vid behandling av de registrerades personuppgifter i Avanzas processer och system. Avanza behandlar personuppgifter både i egenskap av personuppgiftsansvarig samt i egenskap av personuppgiftsbiträde.

Principerna ska säkerställa att Avanza har ett lämpligt skydd för de personuppgifter som hanteras och de registrerades rättigheter samt att hanteringen följer gällande lagar och regler.

## Definitioner

Samtliga definitioner nedan ska ha den betydelse som följer av Europaparlamentets och rådets förordning (EU) 2016/679 och skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsförordningen) eller enligt den svenska tillsynsmyndigheten Integritetsskyddsmyndighetens beskrivning.

### Personuppgifter

Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

### Integritetskänsliga personuppgifter

Det finns personuppgifter som anses vara särskilt skyddsvärda. Dessa kan kräva ytterligare säkerhetsåtgärder vid behandling och innebära utökade risker gentemot den registrerade. Exempel på integritetskänsliga personuppgifter är personnummer.

### Särskilda personuppgifter (”känsliga personuppgifter”)

Varje personuppgift som avser information om politiska åsikter, etniskt ursprung, religiös eller filosofisk övertygelse, medlemskap i en fackförening, uppgifter om hälsa och uppgifter om en fysisk persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person.

### Personuppgiftsansvarig

Det bolag som bestämmer ändamålen och medlen för behandlingen av personuppgifter. I Avanza-koncernen är varje bolag personuppgiftsansvarigt för sin verksamhet.

### Personuppgiftsbiträde
En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar person-uppgifter för den personuppgiftsansvariges räkning.

### Registrerad
En registrerad är den fysiska person vars personuppgifter behandlas av det Avanzabolag som är personuppgiftsansvarig för behandlingen. För Avanzas räkning är detta normalt en kund, försäkrad, förmånstagare, anställd, besökare eller konsult som är fysisk person. Det kan också röra sig om fysiska personer som inte är kunder i Avanza, men som har en anknytning eller affärsförbindelse kopplat till ett visst innehav. Exempel på dessa är gode män, fullmaktshavare, överförmyndare eller andra typer av ombud.

### Behandling
En åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av person-uppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

### Personuppgiftsincident
En personuppgiftsincident är en (avsiktlig eller oavsiktlig) säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter. Den kan också leda till ett obehörigt röjande av eller obehörig åtkomst till personuppgifter.

# Principer för behandling av personuppgifter

## Inledning
All behandling av personuppgifter måste uppfylla de grundläggande principerna som anges nedan. Varje bolag inom Avanzakoncernen måste kunna visa att principerna följs med hänsyn till den behandling respektive bolag ansvarar för.

## Laglighet, korrekthet och öppenhet
Personuppgifterna ska behandlas på ett lagligt, korrekt (rättvis och rimlig) och öppet sätt i förhållande till den registrerade. En personuppgiftsbehandling blir laglig genom att Avanza identifierar en legal grund för behandlingen av personuppgifter.

De registrerade, vars personuppgifter behandlas, ska ges tydlig information om hur behandlingen sker.

Känsliga personuppgifter får i regel inte behandlas. Om behandling av känsliga personuppgifter är nödvändigt för specifika ändamål får det endast ske med stöd av dem undantag som finns. Integritetskänsliga personuppgifter ska behandlas i begränsad omfattning.

## Ändamålsbegränsning
Personuppgifter ska bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Det innebär att Avanza måste ha ändamålen klara för sig redan innan insamlingen av personuppgifter påbörjas. Personuppgifterna får sedan inte behandlas på ett sätt som är oförenligt med dessa ändamål.

## Uppgiftsminimering
Personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Avanza ska inte samla in personuppgifter för obestämda framtida behov, oavsett om sådan lagring kan hänföras till annan affärsnytta.

## Korrekthet
Personuppgifterna ska vara korrekta och uppdaterade. Avanza ska vidta åtgärder för att säkerställa att felaktiga personuppgifter raderas eller rättas utan onödigt dröjsmål.

## Lagringsminimering
Personuppgifterna får inte sparas i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål som personuppgifterna behandlas. När personuppgifterna inte längre behövs för de ändamålen ska de raderas eller avidentifieras.

## Integritet och konfidentialitet
Personuppgifterna ska skyddas mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom misstag. Avanza ska därför se till att lämpliga tekniska och organisatoriska åtgärder vidtas för att skydda personuppgifterna.

Avanza ska ha etablerade processer och rutiner för att identifiera, hantera, utreda, dokumentera och rapportera personuppgiftsincidenter om det finns en risk eller hög risk för den registrerade.

### Överföring och delning av personuppgifter till tredje part, tredjeland eller internationella organisationer
En överföring och delning av personuppgifter utanför EU och det Europeiska Ekonomiska Samarbetsområdet (EES) är endast tillåtet under de förutsättningar som redogörs i GDPR.

### Registrerades rättigheter
De personer vars personuppgifter behandlas av Avanza har ett antal rättigheter som bland annat innebär att de registrerade ska få information om när och hur deras personuppgifter behandlas och få tillgång till sina personuppgifter. Rättigheterna innefattar även rätt att, i vissa fall, få sina uppgifter rättade, raderade eller begränsade i sin användning samt möjligheten att kunna flytta sina uppgifter.

### Registerförteckning
Avanza ska föra ett register över sina behandlingar av personuppgifter. På begäran och vid tillsyn måste Avanza göra registret tillgängligt för Integritetsskyddsmyndigheten.

### Ansvarsskyldighet
Avanza ansvarar för att principerna om personuppgiftsbehandling följs och måste kunna visa på vilket sätt principerna efterlevs. Avanza måste därför se till att lämpliga tekniska och organisatoriska åtgärder vidtas för att skydda personuppgifterna.

# Roller och ansvar

## Personuppgiftsansvarig

Varje legal enhet inom Avanzakoncernen är personuppgiftsansvarig för den behandling av personuppgifter som den legala enheten bestämmer ändamålen för. En legal enhet inom Avanzakoncernen kan även uppdra åt en annan legal enhet, inom eller utom Avanzakoncernen, att för Avanzas räkning utföra hela eller viss del av den faktiska behandlingen av personuppgifter. Om Avanza uppdrar åt ett biträde att utföra personuppgiftsbehandlingen kvarstår aktuell legal enhet inom Avanza som personuppgiftsansvarig.

## Personuppgiftsbiträden

Normalt är tredjepartsleverantörer eller andra externa avtalsparter personuppgiftsbiträde åt bolag inom Avanza, inom ramen för utlagd verksamheten eller köp av tjänst, gett den externa avtalsparten i uppdrag att behandla personuppgifter för Avanzas räkning. En biträdesrelation kan dock också uppstå mellan interna koncernbolag, beroende på intern outsourcing av tjänster.

## VD

VD är ytterst ansvarig för efterlevnad av externa och interna regelverk kopplat till dataskydd. VD ska säkerställa att det finns instruktioner för dem grundläggande principerna samt tydliggörande av ansvarsfördelning inom Avanza.

## Dataskyddsombud – DPO

VD ska utse ett särskilt dataskyddsombud (Data Protection Officer, DPO) för Avanza Bank AB (publ) och Försäkringsaktiebolaget Avanza Pension som ska kontrollera efterlevnaden av tillämpliga regelverk som avser behandling av personuppgifter. Dataskyddsombudet ska även vara en kontaktpunkt för tillsynsmyndigheten och de registrerade. DPO ska ha en självständig roll i förhållande till ledningen. VD ska se till att det finns interna regler som närmare anger DPO:s ansvarsområden.

DPO ska minst årligen informera styrelsen om efterlevnaden av tillämpliga regelverk som avser behandling av personuppgifter utifrån genomförda granskningar samt informera om prioriterade aktiviteter inom området.

## Verksamhetens ansvar

Medarbetare, uppdragstagare, konsulter eller annan part som behandlar personuppgifter på uppdrag av Avanza får enbart behandla personuppgifter enligt de förutsättningar som anges i Avanzas interna regelverk.

Enheter och funktioner inom Avanza ska bidra i arbetet med att säkerställa att behandling av personuppgifter inom verksamheten följer dem grundläggande principerna.

# Samarbete med tillsynsmyndigheten

Avanzas DPO ansvarar för direkt kontakt med Integritetsskyddsmyndigheten i de fall frågor eller tillsynsärenden inleds mot Avanza Bank AB (publ) eller Försäkringsaktiebolaget Avanza Pension. I de fall tillsyn inleds mot andra koncernbolag, med undantag för intressebolag, ska ansvarig i respektive bolag informera Avanzas DPO.