Policy om behandling av personuppgifter

Oktober 2019

Inledning och syfte

Denna policy anger de grundläggande principer som ska gälla för behandling av de registrerades personuppgifter i Avanzas processer och system. Avanza behandlar personuppgifter både i egenskap av personuppgiftsansvarig samt i egenskap av personuppgiftsbiträde.

Syftet med dessa regler är att säkerställa att Avanza har ett lämpligt säkerhetsskydd för de personuppgifter som hanteras samt att den personliga integriteten beaktas i verksamheten.

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).

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.

Särskilda personuppgifter

Varje upplysning som avser information om 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 personuppgifter 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 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 personuppgifter, 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.

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 och öppet sätt i förhållande till den registrerade. Det ska finnas en legal grund för behandling. Den legala grunden kan variera beroende på vilket ändamål behandlingen utförs på.

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. För att säkerställa att personuppgifter inte sparas längre än nödvändigt ska Avanza införa särskilda tidsfrister och rutiner för radering och avidentifiering.

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.

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.

Allmänt om hantering av personuppgifter

Överföring av personuppgifter till tredjeland eller internationella organisationer
Vid överföring av personuppgifter till länder utanför EU och EES (så kallad tredjelandsöverföring) gäller särskilda regler. VD ska se till att det finns interna regler som anger vilka krav som gäller vid överföring av personuppgifter till tredje land.

Anmälan av en personuppgiftsincident till Datainspektionen
Om det inträffar en personuppgiftsincident, till exempel ett dataintrång eller en oavsiktlig förlust av personuppgifter, måste detta i vissa fall anmälas till Datainspektionen. Avanza kan också behöva informera kunder och anställda som berörs av incidenten, om vilka eventuella konsekvenser incidenten kan få. VD ska se till att det finns interna regler som avser processen för hantering av personuppgiftsincidenter.

Registerförteckning
Avanza ska föra ett register över sina behandlingar av personuppgifter. På begäran och vid tillsyn måste Avanza göra registret tillgängligt för Datainspektionen. VD ska se till att det finns interna regler som avser register över behandlingar av personuppgifter.

Registrerades rättigheter
De personer vars personuppgifter behandlas av Avanza har ett antal rättigheter som innebär att de registrerade ska få information om när och hur deras personuppgifter behandlas och ha kontroll över sina egna uppgifter. Därför har de bland annat rätt att i vissa fall få sina uppgifter rättade, raderade eller begränsade i sin användning. Även kunna få ut eller flytta sina uppgifter. VD ska se till att det finns interna regler som avser Avanzas hantering av de registrerades rättigheter.

Roller och ansvar

Personuppgiftsansvarig
Varje legal enhet inom Avanzakoncernen är personuppgiftsansvarig för den behandling av personuppgifter som den legala enheten bestämmer ändamålen för. Medarbetare får enbart behandla personuppgifter enligt de förutsättningar som anges i Avanzas interna regelverk.

En legal enhet inom Avanzakoncernen kan även uppdra åt en annan legal enhet, inom eller utom Avanza-koncernen, att för Avanzas räkning utföra hela eller viss del av den faktiska behandlingen av person-uppgifter. Om Avanza uppdrar åt ett biträde att utföra personuppgiftsbehandlingen kvarstår aktuell legal enhet inom Avanza som personuppgiftsansvarig.

Personuppgiftsbiträden

Allmänt

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.

Biträdesavtal och instruktioner

Om Avanza ger ett externt bolag i uppdrag att behandla personuppgifter (om exempelvis kunder eller anställda) för Avanzas räkning krävs att ett särskilt personuppgiftsbiträdesavtal ingås som reglerar denna behandling. Varje beställaransvarig eller avtalsägare ansvarar för att se till att ett biträdesavtal upprättas. Avanza ska endast anlita sådana personuppgiftsbiträden som kan förväntas uppfylla de krav som följer av gällande lagstiftning.

Uppföljning och kontroll,

Avtalsägare ska följa upp och kontrollera personuppgiftsbiträden utifrån de krav som framgår i avtalet. Sådan uppföljning och kontroll ska ske riskbaserat. Motsvarande skyldighet åligger beställaransvarig inom verksamheten vid interna biträdesförhållanden. VD ska se till att det finns interna regler som avser uppföljning och kontroll av köpta och utlagda tjänster avseende behandling av personuppgifter.

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.

Övriga enheter och funktioner

Ett stort antal enheter och funktioner inom Avanza ska bidra i arbetet med att säkerställa att behandling av personuppgifter inom verksamheten är ändamålsenlig. VD ska se till att det finns interna regler som närmare anger respektive enhets eller funktions ansvarsområden.

Samarbete med tillsynsmyndigheten

Avanzas DPO ansvarar för direkt kontakt med Datainspektionen 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.