

VARNING FÖR KRYPTOTILLGÅNGAR



Kryptotillgångar kan vara riskabla och ditt skydd, om det finns något, kan vara begränsat

Alla kryptotillgångar och kryptotillgångstjänster är inte likvärdiga och regleras inte heller på samma sätt (om ens alls). Även om en ny förordning som kallas Mica (förordningen om marknader för kryptotillgångar) nu har införts i EU och reglerar verksamhet som omfattar vissa kryptotillgångar, är de flesta kryptotillgångar fortsatt volatila och mycket riskfyllda. Därmed är de kanske inte lämpliga för alla konsumenter som en form av investering, betalning eller växling.

Beroende på vilken typ av kryptotillgång och leverantör du väljer, kan du utsättas för högre risker och kanske endast

ha begränsat eller inget konsumentskydd (t.ex. tillgång till fullständig information och transparenta processer för klagomålshantering). Detta gäller särskilt om du använder eller investerar i kryptotillgångar/kryptotillgångstjänster som erbjuds av företag som är etablerade utanför EU och av leverantörer som inte regleras enligt Mica.

För att bättre förstå de olika typerna av kryptotillgångar och leverantörer kan du ta en titt på faktabladet Förklaring av kryptotillgångar: [Vad betyder Mica för dig som konsument?](#).

Vad du bör fråga dig själv innan du investerar i kryptotillgångar

1

Känner jag till de risker jag tar när jag investerar i eller använder kryptotillgångar?

- Innan du investerar bör du ta dig tid att lära dig mer om de produkter eller tjänster du är intresserad av.
- Som med alla investeringar, överväg om dessa risker är värda att ta med tanke på dina egna mål och ekonomiska omständigheter.

2

Är de företag/aktörer som jag överväger att använda auktoriserade att tillhandahålla kryptotillgångstjänster i EU?

- Du kan kontrollera om en leverantör är auktoriserad i EU genom att:
 - Kontrollera Esmas register (shorturl.at/zZwVI)*. Den nationella finansiella tillsynsmyndighetens kan också tillhandahålla en "svart lista" över icke auktoriserade kryptotillgångsföretag, inbegripet tjänsteleverantörer. Du kan också kontrollera tillsynsmyndighetens hemsida eller I-SCAN-listan (iosco.org/i-scan/).
 - Kontrollera företagets webbplats. Dess rättsliga status kan nämnas på deras webbplats. Tänk på att företag i vissa fall kan få tillstånd för endast en del av sin verksamhet (endast vissa tjänster, inte alla). Kontrollera vilka tjänster företaget får tillhandahålla.

3

Är de enheter jag använder för att köpa, lagra eller överföra kryptotillgångar och för att hålla mina privata nycklar säkra?

- Att förlora privata nycklar till kryptotillgångar leder till permanent och oåterkallelig förlust av åtkomst och ägande.
- Att hålla dina enheter och nyckellagring säkra är viktigt för att skydda dina kryptotillgångar, särskilt genom att:
 - Se till att din enhet och annan kryptorelaterad programvara alltid är uppdaterad till den senaste versionen för att minska säkerhetsbrister.
 - Använd starka och unika lösenord för vart och ett av dina kryptokonton, håll ditt lösenord hemligt och undvik att återanvända samma autentiseringsuppgifter på olika plattformar. Se några tips här (shorturl.at/7ns3I).
 - Undvik att logga in på dina kryptokonton via offentliga eller osäkra wifinätverk.

Vilka är de största riskerna du kan råka ut för?



Extrema prisrörelser

Värdet på de flesta kryptotillgångar, inklusive vissa som är reglerade, kan vara mycket volatilt, vilket innebär att priset på dem kan falla och stiga snabbt under korta tidsperioder. Du kan förlora en hel del, eller till och med alla, pengar som du investerat.



Likviditetsrisker

Marknader för kryptotillgångar kan ha likviditetsbegränsningar, vilket kan begränsa din förmåga att sälja kryptotillgångar till det pris eller under den tid du vill.



Vilseledande information

Vissa kryptotillgångar och relaterade produkter marknadsförs aggressivt med hjälp av information som är förvirrande, ofullständig, felaktig och ibland avsiktligt vilseledande. Var uppmärksam på riskerna med den här typen av marknadsföring, särskilt på sociala medier där influerare kan uppmuntras att marknadsföra vissa kryptotillgångar.



Bedrägerier, bluffar och cyberattacker

Det finns många bedrägliga system för kryptotillgångar, cyberattacker och bluffar, och du bör vara medveten om att deras enda syfte är att lura dig på dina pengar med hjälp av olika tekniker. Bedragare kan använda nätfiskemejl (phishing), socialmanipulation och skadliga länkar, lovar orealistiskt höga avkastningar eller hävdar att de är auktoriserade eller reglerade när de inte är det.



Begränsat skydd

Mica-förordningen ger ett visst konsumentskydd när det gäller specifika typer av kryptotillgångar och kryptotjänster (t.ex. tillgång till fullständig information och transparenta processer för klagomålshantering). Konsumentsskyddet är dock inte lika omfattande som det som gäller för mer traditionella finansiella produkter (du kommer t.ex. inte att omfattas av ersättningssystem). För kryptotillgångar eller tjänster som erbjuds av företag som inte är reglerade i EU kan du, om något går fel, kanske inte dra nytta av något konsumentskydd alls eller ett konsumentskydd som är mindre omfattande än det som gäller i EU.



Produktkomplexitet

Egenskaperna hos och riskerna med kryptotillgångar samt alla produkter med en underliggande kryptotillgång, kan vara svåra att förstå. Var försiktig när du köper kryptotillgångar eller relaterade investeringsprodukter, särskilt om du är osäker på hur deras värde bestäms och vilka risker de medför.

Rättslig grund och bakgrund

Denna varning baseras på artikel 9.3 i de europeiska tillsynsmyndigheternas inrättandeförordningar och följer på tidigare varningar, som inkluderar 2022 års [varning](#) om riskerna med kryptotillgångar.

Termen kryptotillgång avser en digital representation av ett värde eller en rättigheter som kan överföras och lagras elektroniskt med hjälp av en distribuerad liggare eller liknande teknik.

EU:s förordning om marknader för kryptotillgångar (Mica) är fullt tillämplig sedan den 30 december 2024.

* Du bör vara medveten om att endast företag som är auktoriserade och noterade i Esmas register får tillhandahålla kryptotillgångstjänster i EU enligt Mica-förordningen. En övergångsperiod gäller dock fram till juli 2026 i vissa medlemsstater, och vissa företag kan bedriva verksamhet enligt nationell rätt fram till dess att de erhåller Mica-auktorisering. Det innebär att du inte kan dra nytta av något Mica-skydd om du använder tjänster från sådana leverantörer innan övergångsperioden löper ut och leverantören är auktoriserad enligt Mica.

Se även detaljer om övergångsperioden per EU-land här([shorturl.at/Cs49L](#)).