Regeringskansliet
Faktapromemoria 2020/21:FPM16

Förordning om digital operativ motståndskraft i den finansiella sektorn

2020/21:FPM16

Finansdepartementet

2020-10-26

Dokumentbeteckning

COM(2020) 595
Förslag till EU-parlamentets och rådets förordning om digital operativ motståndskraft i den finansiella sektorn och ändring av förordning (EU) 1060/2012, (EU) 600/2014 och (EU) 909/2014

Sammanfattning

Kommissionens förslag till en förordning om digital operativ motståndskraft i den finansiella sektorn (DORA-förordningen) syftar till att säkerställa att deltagare i det finansiella systemet har vidtagit de skyddsåtgärder som krävs för att motverka cyberattacker och andra it-relaterade risker. Förslaget innehåller krav som innebär att merparten av de aktörer som är aktiva i den finansiella sektorn ska bli mer motståndskraftiga mot informations- och kommunikationsrelaterade (IKT) störningar och hot. För att uppnå det finns i DORA-förordningen bestämmelser om styrning; riskhantering, rapportering och testning. Enligt förslaget ska det också införas en tillsynsram för företag som levererar informations- och kommunikationsrelaterade tjänster (IKT-leverantörer) till den finansiella sektorn.

Sammanfattningsvis syftar förslaget till att stärka den finansiella sektorns motståndskraft mot IKT-risker, inte att höja förlusttäckningsgraden i händelse av en IKT-händelse. De bestämmelser som ingår i DORA-förordningen är således av kvalitativ natur och berör inte kapitalkrav.

Regeringen välkomnar förslaget om stärkt digital operativ motståndskraft i den finansiella sektorn. Det är positivt att lagstiftningen harmoniseras och tydliggörs för de aktörer som ska tillämpa den. Vidare välkomnar regeringen förslaget om en tillsynsram för IKT-leverantörer. Samtidigt är det av vikt att förordningens omfattning utformas proportionerligt både i förhållande till aktörernas typ, storlek och komplexitet samt vad gäller nivå på riskhantering, rapportering och testning som aktörerna blir föremål för. Kretsen av aktörer bör utformas så att syftet med regleringen uppnås. Regeringen kommer att

verka för att reglerna utformas så att de blir ändamålsenliga. Nationell tillsynsstruktur bör beaktas. Regeringen anser att förslaget står i överensstämmelse med subsidiaritetsprincipen och proportionalitets-principen.

Regeringen anser att kostnader för berörda myndigheter samt statsbudgeten till följd av förslaget ska hanteras inom befintliga ekonomiska ramar. Merkostnader för EU-budgeten ska täckas av omprioriteringar och inte med nya medel.

1 Förslaget

1.1 Ärendets bakgrund

Förslaget till en förordning om digital operativ motståndskraft för den finansiella sektorn (DORA-förordningen) ingår som en del i det paket om digitalisering av finanssektorn som kommissionen presenterade den 24 september 2020. En av de fyra prioriteringar som kommissionen identifierat i meddelandet om en strategi för digitalisering av finanssektorn i EU handlar om att hantera risker som följer av den digitala omställningen. I linje med detta har kommissionen lämnat förslaget till DORA-förordningen.

Kommissionen har i det förberedande arbetet med DORA-förordningen genomfört konsultationer med externa intressenter. Kommissionen har beaktat de tekniska råd om förstärkt riskhantering av IKT-risker i den finansiella sektorn och om ett samlat ramverk för avancerade penetrationstester som utfärdats av de europeiska tillsynsmyndigheterna (Europeiska bankmyndigheten (Eba), Europeiska värdepappers- och marknadsmyndigheten (Esma) och Europeiska försäkrings och tjänstepensionsmyndigheten (Eiopa)). Därutöver har kommissionen beaktat det arbete som utförts på området av andra internationella fora såsom Internationell valutafonden (IMF), G7, Financial Stability Board (FSB), Europeiska systemrisknämnden (ESRB) och Baselkommittén för banktillsyn (BCBS).

Övriga delar i paketet om digitalisering av finanssektorn behandlas i faktapm 2020/21:FPM12, 2020/21:FPM13, 2020/21:FPM14 och 2020/21:FPM15. Det finns ännu ingen officiell svensk språkversion av förslaget.

1.2 Förslagets innehåll

Den föreslagna DORA-förordningen kan delas upp i fyra olika delar: Bestämmelser om styrning och riskhantering, rapportering, testning och en tillsynsram för IKT-leverantörer som levererar tjänster till den finansiella sektorn. Förordningens omfattar ett stort antal typer av företag: Kreditinstitut, betalningsinstitut, institut för elektroniska pengar, värdepappersföretag, tillhandahållare av tjänster för kryptotillgångar, utgivare av kryptotillgångar, tillhandahållare av asset referenced tokens,

utgivare av signifikanta asset-referenced tokens, värdepapperscentraler, centrala motparter, handelsplatser, transaktionsregister, förvaltare av alternativa investeringsfonder, fondbolag, leverantörer av datarapporteringstjänster, försäkringsföretag, återförsäkringsföretag, försäkringsförmedlare, försäkringsförmedlare som bedriver förmedling som sidoverksamhet, återförsäkringsförmedlare, tjänstepensionsinstitut, kreditvärderingsinstitut, revisorer och registrerade revisionsbolag, administratörer av kritiska referensvärden, leverantörer av gräsrotsfinansieringstjänster, värdepapperiseringsregister och tredjepartsleverantörer av IKT-tjänster. Alla dessa typer av aktörer, med undantag för tredjepartsleverantörer av IKT-tjänster, anges i förordningen under samlingsbeteckningen ”finansiella enheter”.

1.2.1 Styrning och riskhantering

I den föreslagna DORA-förordningen finns bestämmelser som tydliggör ledningens ansvar för IKT-risker, vilket ställer krav på organisation och ledningens kontroll över hur det finansiella enheter hanterar IKT-risker, både i relation till interna system och utkontrakterade system.

Bestämmelserna om riskhantering omfattar krav på dokumentation och framtagande samt bibehållande av ett IKT-riskramverk. I detta ramverk ingår policyer, strategier, processer, IKT-protokoll och verktyg som är nödvändiga för att säkerställa att all relevant infrastruktur, inklusive servrar, lokaler, datacenter och hårdvara, är tillräckligt skyddade för att förhindra fysisk skada, obehörig åtkomst eller utnyttjande. Ramverket ska ses över varje år och uppdateras efter behov. Vidare ska ramverket inkludera en strategi för digital motståndskraft som beskriver genomförandet av ramverket. Dessutom finns krav på klassificering av alla IKT-funktioner i en finansiell enhet och identifiering av risker kopplade till dessa funktioner, här ingår även IKT-funktioner som utkontrakterats till tredje part. Det finns också krav att de finansiella enheterna löpande ska övervaka och kontrollera sina IKT-system och använda sig av lämpliga säkerhetsverktyg och processer i enlighet med en dokumenterad säkerhetsstrategi. I linje med det finns även krav på att det finns mekanismer och system på plats för att upptäcka avvikande aktiviteter i systemen. Därtill ska de finansiella enheterna ta fram kontinuitetsplaner, återhämtningsplaner och kommunikationsplaner som ska ingå i IKT-riskramverket. Det finns också krav på att de finansiella enheterna har tillgång till backupsystem och har metoder som syftar till att återställa information. Slutligen finns bestämmelser om uppföljning och rapportering av eventuella IKT-incidenter i syfte att hantera dem på ett adekvat sätt samt tillvara ta erfarenheter och identifiera vilka förbättringar som behöver genomföras. De europeiska tillsynsmyndigheterna ska i samråd med EU:s datasäkerhetsmyndighet Enisa ta fram tekniska standarder med mer detaljerade regler om riskhantering och riskramverket.

Tredjepartsrisker ska ingå som en integrerad del av de finansiella enheternas IKT-riskramverk. Det ställs bl.a. krav på dokumentation, att de finansiella

enheterna ska värdera de risker som kan uppkomma till följd av utkontrakteringen och på exitstrategier. Vidare finns bestämmelser om vilka avtalsområden ett utkontrakteringskontrakt ska innehålla för att säkerställa de finansiella enheternas IKT-säkerhet och kontroll i samband med utkontrakteringen.

1.2.2 Rapportering av IKT-incidenter

I syfte att strömlinjeforma och harmonisera existerande rapporteringskrav finns i den föreslagna förordningen bestämmelser om rapportering av betydande IKT-incidenter. Kommissionen föreslår att förhållandet mellan DORA-förordningens rapporteringskrav och de rapporteringskrav som framgår av Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet) strömlinjeformas så att berörda företag inte behöver rapportera enligt båda regelverken utan endast enligt rapporteringskraven i den nya förordningen. Vidare harmoniseras de bestämmelser om rapportering som finns i Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG (PSD2) så att rapportering om betydande IKT-incidenter undantas eftersom de istället ska regleras i den nya förordningen.

Den föreslagna DORA-förordningen innehåller krav på de finansiella enheterna att ta fram processer för att hantera, kontrollera och förteckna IKT-incidenter. Vidare ska IKT-incidenter klassificeras utifrån vissa faktorer såsom hur många motparter som drabbades av incidenten, långvarighet, graden av allvarlighet och om kritiska system var föremål för incidenten och incidentens ekonomiska effekter.

Betydande IKT-incidenter ska rapporteras till behöriga myndigheter inom vissa bestämda tidsramar. Sådana rapporter ska även innehålla information så att den behöriga myndigheten kan avgöra om incidenten kan påverka aktörer i andra länder. Den behöriga myndigheten ska i sin tur informera Eba, Esma eller Eiopa beroende vilken sektor som berörs och Europeiska centralbanken (ECB) samt, i de fall incidenten rör ett kreditinstitut, betalningsinstitut eller institut för elektroniska pengar, till den enhet för hantering av incidenter som definieras i NIS-direktivet. I Sverige är Myndigheten för samhällsskydd och beredskap (MSB) den enheten (benämns vanligen CSIRT-enhet).

De europeiska tillsynsmyndigheterna ska i samråd med Enisa och den ECB ta fram tekniska standarder med mer detaljerade bestämmelser om klassificering och gränsvärden för vilka incidenter som ska betraktas som betydande incidenter.

1.2.3 Testning av IKT-säkerhet

I den föreslagna DORA-förordningen finns bestämmelser som reglerar i vilken omfattning finansiella enheter ska testa sina IKT-system. Det är dels generella bestämmelser som omfattar krav på finansiella enheter att ta fram testprogram som en integrerad del av IKT-riskramverket, dels särskilda bestämmelser om avancerade penetrationstester. Avancerade penetrationstester innebär att en cyberattack under kontrollerade former simuleras mot en organisations anställda, processer och teknik. Dessa tester är inte utformade för att godkänna eller underkänna ett företags kapacitet, utan syftar till att identifiera brister för att sedan kunna förbättra motståndskraften. Behörig myndighet ska identifiera vilka enheter som ska omfattas av dessa tester. De europeiska tillsynsmyndigheterna ska ta fram detaljerade tekniska standarder dels om vilka typer av finansiella enheter som ska omfattas av dessa tester, dels om testerna som sådana.

1.2.4 En tillsynsram för IKT-leverantörer

Teknikföretag blir allt viktigare inom finanssektorn i egenskap av it-leverantörer till finansiella företag. Mot den bakgrunden innehåller den föreslagna förordningen bestämmelser som syftar till att möjliggöra övervakning av kritiska tredjepartsleverantörer av IKT-tjänster. Kommissionen föreslår att en tillsynsram upprättas inom ramen för nuvarande tillsynsstruktur. Det innebär att ett forum för övervakning etableras under de europeiska tillsynsmyndigheternas gemensamma kommitté. Detta forum ska identifiera vilka IKT-leverantörer som ska definieras som kritiska samt bestämma vilken av de europeiska tillsynsmyndigheterna som är bäst lämpad att vara den myndighet som vara ansvarig förövervakningen över en viss kritisk IKT-leverantör. Den ansvariga övervakningsmyndigheten ska utvärdera om en kritisk IKT-leverantör har tillräckligt omfattande, sunda och effektiva regler, processer, mekanismer och arrangemang för att hantera de IKT-risker de kan utsätta finansiella enheter för. Baserat på den bedömningen ska den ansvariga övervakningsmyndigheten ta fram en övervakningsplan för varje enskild kritisk IKT-leverantör. När en övervakningsplan är framtagen får nationella behöriga myndigheter endast vidta åtgärder som berör dessa kritiska IKT-leverantörer i överenskommelse med den ansvariga övervakningsmyndigheten.

För att kunna utföra sitt uppdrag får den ansvariga övervakningsmyndigheten rätt att begära information och dokumentation, utföra undersökningar och platsundersökningar samt begära in rapporter från kritiska IKT-leverantörer. Den ansvariga övervakningsmyndigheten kan förena sådan begäran med vite. Vidare kan den ansvariga övervakningsmyndigheten rikta rekommendationer till en kritisk IKT-leverantör. I detta arbete ska den ansvariga övervakningsmyndigheten biträdas av ett gemensamt undersökningsteam bestående av representanter från de behöriga myndigheterna.

Nationella behöriga myndigheter kan mot bakgrund av en sådan rekommendation vidta åtgärder mot finansiella enheter som använder sig av den IKT-leverantör som rekommendationen berör. Vidare ska de behöriga myndigheterna övervaka hur finansiella enheter beaktar de risker som den ansvariga övervakningsmyndigheten har identifierat i rekommendationen och som riktats till IKT-leverantören. Vid behov kan behörig myndighet vidta åtgärder mot finansiella enheter som innebär att de temporärt eller permanent, helt eller delvis slutar använda tjänster från den aktuella IKT-leverantören.

1.3 Gällande svenska regler och förslagets effekt på dessa

Eftersom den föreslagna regleringen är i form av en direkt tillämplig EU-förordning krävs inga lagstiftningsåtgärder för att genomföra den i svensk rätt. Svensk lagstiftning kan dock behöva anpassas till följd av t.ex. följdändringar i vissa direktiv som framgår av kommissionens meddelande KOM(2020) 596.

1.4 Budgetära konsekvenser / Konsekvensanalys

1.4.1 Kommissionens konsekvensanalys

Av kommissionens konsekvensanalys, SWD(2020) 198, framgår att stärkt motståndskraft till följd av den nya regleringen kan leda till besparingar för EU:s finansiella system med uppskattningsvis 10 procent av kostnader som uppstår till följd av IKT-incidenter. Det motsvarar cirka 200 miljoner - 2,7 miljarder euro per år enigt de uppskattningar som finns att tillgå. Vidare anser kommissionen att en harmonisering av rapporteringskrav och ramverk för avancerade penetrationstester leder till besparingar för finansiella enheter. Kostnader för finansiella enheter och IKT-leverantörer kan uppkomma till följd av anpassningar till den nya regleringen.

För behöriga myndigheter kan kostnader uppkomma i samband med att rapporteringsmängden ökar, t.ex. i samband med investeringar i nödvändig infrastruktur. Kostnader kan också uppkomma för behöriga myndigheter för att anpassa tillsynsverksamheten efter den ny regleringen.

Vidare uppkommer kostnader för de europeiska tillsynsmyndigheterna med anledning av uppgifter som ska tillkomma enligt den föreslagna nya förordningen att övervaka kritiska IKT-leverantörer. Dessa kostnader avser 18 nya heltidstjänster, it-investeringar och administrativa kostnader. Sammantaget innebär förslaget ökade kostnader för de europeiska tillsynsmyndigheterna på ca 30 miljoner euro under perioden 2022 - 2027. Kommissionen betonar att kostnaderna kan variera över tid beroende på hur många IKT-leverantörer som identifieras som kritiska och storleken på dessa. Mot bakgrund av att övervakningen kommer att vara avgiftsbelagd uppger kommissionen att förslaget inte kommer att påverka EU-budgeten

utöver kostnaden för personella resurser. Det kan noteras att dessa avgifter även omfattar kostnader som kan uppkomma för nationella tillsynsmyndigheter som deltar i de gemensamma tillsynsteam som involveras i arbetet. Regeringen anser att kostnadsökningar som belastar i EU-budgeten kostnadsökningar ska täckas av omprioriteringar och inte med nya medel.

1.4.2 Förslagets konsekvenser i Sverige

Berörd behörig myndighet i Sverige är Finansinspektionen utom på ett område. Enligt förslaget ska även revisorer och registrerade revisionsbolag omfattas av den föreslagna förordningen och det är Revisorsinspektionen är behörig myndighet för dem.

Det kan noteras att förslaget om harmoniserad rapportering innebär att finansiella enheter, som i dag är skyldiga att rapportera IKT-incidenter till Myndigheten för samhällsskydd och beredskap (MSB) i enlighet med NIS-direktivet, endast behöver rapportera incidenter definierade enligt den föreslagna nya förordningen och tillhörande tekniska standarder, till Finansinspektionen.

Det kan också noteras att avancerade penetrationstester i Sverige koordineras av Riksbanken. Enligt förslaget ska dessa typer av tester hanteras av behörig myndighet, vilket innebär att det kan påverka nuvarande organisering av koordinering av avancerade penetrationstester i Sverige.

Regeringen konstaterar att förslaget kan innebära kostnadsökningar för behöriga nationella myndigheter i form av ökad tillsynsaktivitet och investeringar i infrastruktur till följd av ökad inrapportering. Regeringen anser att dessa kostnader ska hanteras inom myndigheternas befintliga ekonomiska ramar.

Regeringen konstaterar att förslaget kommer att påverka EU-budgeten såvitt avser kostnader för de europeiska tillsynsmyndigheternas verksamhet kopplat till tillsynsram för kritiska IKT-leverantörer som inte täcks av tillsynsavgifter. Regeringen anser att dessa kostnadsökningar ska täckas av omprioriteringar i EU-budgeten och inte med nya medel.

2 Ståndpunkter

2.1 Preliminär svensk ståndpunkt

Regeringen välkomnar ett förslag om stärkt digital operativ motståndskraft i finanssektorn. Det är positivt att lagstiftning harmoniseras och tydliggörs för de aktörer som ska tillämpa den samt att kraven på motståndskraften mot it-incidenter förstärks. Samtidigt är det av vikt att förordningens omfattning utformas proportionerligt både i förhållande till aktörernas typ, storlek och komplexitet samt vad gäller nivå på riskhantering, rapportering och testning

som aktörerna blir föremål för. Kretsen av aktörer bör utformas så att syftet med regleringen uppnås. Regeringen kommer att verka för att reglerna utformas så att de blir ändamålsenliga. Nationell tillsynsstruktur bör beaktas.

Regeringen välkomnar en tillsynsram för kritiska IKT-leverantörer på EU-nivå. Reglerna bör utformas så att de inte hindrar nationella behöriga myndigheter att utföra effektiv tillsyn av finansiella enheters utkontraktering av IKT-tjänster. Vidare bör tillsynsramen för IKT-leverantörer genomföras på ett så kostnadseffektivt sätt som möjligt.

Regeringen anser att kostnader för berörda myndigheter samt statsbudgeten till följd av förslagen ska hanteras inom befintliga ekonomiska ramar. Merkostnader för EU-budgeten ska täckas av omprioriteringar och inte med nya medel.

2.2 Medlemsstaternas ståndpunkter

Medlemsstaterna lämnade sina initiala kommentarer till paketet om digitalisering av finanssektorn vid Ekofinrådet den 6 oktober. Då diskuterades huvudsakligen strategierna om digitalisering av finanssektorn och massbetalningar. Såtillvida diskuterades inte förslaget till DORA-förordningen i detalj.

2.3 Institutionernas ståndpunkter

Institutionernas ståndpunkter, förutom kommissionens, är ännu inte kända.

2.4 Remissinstansernas ståndpunkter

Förslaget har inte remitterats. Flera myndigheter, organisationer och företag har inbjudits att lämna synpunkter på förslaget och en referensgrupp har bildats.

3 Förslagets förutsättningar

3.1 Rättslig grund och beslutsförfarande

Den rättsliga grunden för förslaget utgörs av artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget). Rådet beslutar med kvalificerad majoritet och Europaparlamentet är medbeslutande

3.2 Subsidiaritets- och proportionalitetsprincipen

Kommissionen uppger att proportionalitetsprincipen genomsyrar den föreslagna DORA-förordningen på flera sätt. Det ställs inte samma krav på mikroföretag när det gäller styrning och hantering av IKT-risker. Mikroföretag definieras som företag som sysselsätter färre än 10 personer

och vars omsättning eller balansomslutning inte överstiger 2 miljoner euro per år. Kraven på riskhantering är också riskbaserade; ju högre komplexitet desto högre krav på riskhantering och tvärtom. Samma princip gäller för testning och endast vissa finansiella enheter är föremål för krav på avancerade penetrationstester. Endast betydande IKT-incidenter ska rapporteras. Tillsynsramen för IKT-leverantörer omfattar endast kritiska IKT-leverantörer.

Kommissionen uppger att förslaget är förenligt med subsidiaritetsprincipen och anger följande skäl. Den finansiella sektorn i EU är i dag till stor del av enhetligt reglerad på EU-nivå. Den fragmentering av reglering av IKT-risker som idag existerar kan endast avhjälpas på EU-nivå, exempelvis harmonisering av rapportering. För att undvika fragmenterade nationella regelverk när det gäller testning är EU-lagstiftning nödvändigt. Övervakning av IKT-leverantörer sker mest effektivt på EU-nivå för att möjliggöra övervakning av koncentrationsrisker och smittorisker ur ett EU-perspektiv.

Regeringen delar kommissionens uppfattning att förslaget är förenligt med subsidiaritetsprincipen. Vidare delar regeringen kommissionens uppfattning att förslaget är förenligt med proportionalitetsprincipen men kommer att analysera den frågan närmare.

4 Övrigt

4.1 Fortsatt behandling av ärendet

Förhandlingar i rådsarbetsgruppen för finansiella tjänster har inletts. Någon närmare tidsplan för förhandlingarna har inte presenterats. Förslaget är prioriterat av det tyska ordförandeskapet som planerar att rådsslutsatser om förslaget till förordning ska antas vid Ekofinrådets möte i december.

4.2 Fackuttryck/termer

Avancerade penetrationstester innebär att en cyberattack under kontrollerade former simuleras mot en organisations anställda, processer och teknik. Dessa tester är inte utformade för att godkänna eller underkänna ett företags kapacitet, utan syftar till att identifiera brister för att sedan kunna förbättra motståndskraften.

Asset-referenced tokens: Kryptotillgångar som konstruerats för att hålla ett relativt stabilt värde genom att tillgångarna på något sätt stöds av värdepapper, råvaror eller banktillgodohavanden i t.ex. dollar eller euro.

Digital operativ motståndskraft: finansiella företags förmåga att tillförsäkra deras operativa integritet ur ett tekniskt perspektiv för att säkerheten i nätverk och informationssystem ska kunna upprätthållas.

Distribuerad databasteknik: Distribuerad databasteknik eller distribuerad lagring av kod är ett system för registrering av transaktioner av tillgångar där

transaktionerna och deras detaljer registreras i flera identiska exemplar på många datorer. Syftet är att göra det omöjligt att radera eller förvanska information utan att det upptäcks. Den vanligaste typen av sådan teknik kallas blockkedja.

Finansiella enheter: Samlingsbegrepp för alla typer av företag som den föreslagna förordningen omfattar förutom IKT-leverantörer. De typer av företag som avses med begreppet är: Kreditinstitut, betalningsinstitut, institut för elektroniska pengar, värdepappersföretag, tillhandahållare av tjänster för kryptotillgångar, utgivare av kryptotillgångar, tillhandahållare av asset referenced tokens, utgivare av signifikanta asset-referenced tokens, värdepapperscentraler, centrala motparter, handelsplatser, transaktionsregister, förvaltare av alternativa investeringsfonder, fondbolag, leverantörer av datarapporteringstjänster, försäkringsföretag, återförsäkringsföretag, försäkringsförmedlare, försäkringsförmedlare som bedriver förmedling som sidoverksamhet, återförsäkringsförmedlare, tjänstepensionsinstitut, kreditvärderingsinstitut, revisorer och registrerade revisionsbolag, administratörer av kritiska referensvärden, leverantörer av gräsrotsfinansieringstjänster och värdepapperiseringsregister

IKT-leverantörer: Företag som levererar informations- och kommunikationsrelaterade tjänster till den finansiella sektorn.

Kryptotillgångar: En digital representation av värde eller rättigheter som kan överföras och lagras elektroniskt med hjälp av distribuerad databasteknik eller liknande teknik. Omfattar virtuella valutor, kryptovalutor och andra kryptomedel med tokens.

Tokens: Tokens är samlingsnamnet för virtuella valutor eller värdepappersliknande enheter som består av kryptokoder och som kan skapas i en blockkedja.