

I

(Lagstiftningsakter)

FÖRORDNINGAR

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2023/1113

av den 31 maj 2023

om uppgifter som ska åtfölja överföringar av medel och vissa kryptotillgångar och ändring av direktiv (EU) 2015/849

(omarbetning)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska centralbankens yttrande ⁽¹⁾,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ⁽²⁾,

i enlighet med det ordinarie lagstiftningsförfarandet ⁽³⁾, och

av följande skäl:

- (1) Europaparlamentets och rådets förordning (EU) 2015/847 ⁽⁴⁾ har ändrats väsentligt ⁽⁵⁾. Eftersom ytterligare ändringar ska göras, bör den förordningen av tydlighetsskäl omarbetas.
- (2) Förordning (EU) 2015/847 antogs för att säkerställa att de krav som tagits fram av arbetsgruppen för finansiella åtgärder (FATF) avseende leverantörer av tjänster för elektroniska överföringar tillämpas på ett enhetligt sätt i hela unionen, särskilt kravet på att betaltjänstleverantörer måste se till att överföring av medel åtföljs av uppgifter om betalaren och betalningsmottagaren. De senaste ändringarna av FATF:s standarder om ny teknik, som gjordes i juni 2019, syftar till att reglera virtuella tillgångar och leverantörer av tjänster för virtuella tillgångar, och medför nya och liknande skyldigheter för leverantörer av tjänster för virtuella tillgångar i syfte att underlätta spårning av

⁽¹⁾ EUT C 68, 9.2.2022, s. 2.

⁽²⁾ EUT C 152, 6.4.2022, s. 89.

⁽³⁾ Europaparlamentets ståndpunkt av den 20 april 2023 (ännu inte offentliggjord i EUT) och rådets beslut av den 16 maj 2023.

⁽⁴⁾ Europaparlamentets och rådets förordning (EU) 2015/847 av den 20 maj 2015 om uppgifter som ska åtfölja överföringar av medel och om upphävande av förordning (EG) nr 1781/2006 (EUT L 141, 5.6.2015, s. 1).

⁽⁵⁾ Se bilaga I.

överföringar av virtuella tillgångar. Utöver dessa ändringar ska leverantörer av tjänster för virtuella tillgångar se till att överföringar av virtuella tillgångar åtföljs av uppgifter om avsändare och mottagare av dessa. Leverantörer av tjänster för virtuella tillgångar ska även inhämta, inneha och lämna de uppgifterna till motparten på andra sidan i överföringen, och på begäran göra dem tillgängliga för behöriga myndigheter.

- (3) Med tanke på att förordning (EU) 2015/847 för närvarande endast är tillämplig på överföringar av medel, det vill säga på sedlar och mynt, kontotillgodohavanden och elektroniska pengar enligt definitionen i artikel 2.2 i Europaparlamentets och rådets direktiv 2009/110/EG ⁽⁶⁾, är det lämpligt att utvidga tillämpningsområdet för förordning (EU) 2015/847 till att även omfatta överföringar av virtuella tillgångar.
- (4) De flöden av pengar från olaglig verksamhet som skapas genom överföringar av medel och virtuella tillgångar kan skada den finansiella sektorns integritet, stabilitet och anseende och utgöra ett hot mot såväl unionens inre marknad som internationell utveckling. Penningtvätt, finansiering av terrorism och organiserad brottslighet är fortfarande betydande problem som bör angripas på unionsnivå. Den sundhet, integritet och stabilitet som präglar systemet för överföring av medel och virtuella tillgångar och tilltron till det finansiella systemet i dess helhet, kan allvarligt sättas på spel genom brottslingars och deras medhjälparens försök att antingen dölja ursprunget till vinning från brott eller att överföra medel eller virtuella tillgångar för brottslig verksamhet eller terroriständamål.
- (5) För att underlätta sin brottsliga verksamhet är det sannolikt att personer som ägnar sig åt penningtvätt och finansiering av terrorism utnyttjar den fria rörligheten för kapital inom unionens integrerade finansiella område, om inte vissa samordnade åtgärder antas på unionsnivå. Internationellt samarbete inom ramen för FATF och en global tillämpning av dess rekommendationer syftar till att förhindra penningtvätt och finansiering av terrorism vid överföring av medel eller virtuella tillgångar.
- (6) På grund av räckvidden för de åtgärder som vidtas bör unionen säkerställa att de internationella standarder för bekämpning av penningtvätt och finansiering av terrorism och spridning som FATF antog den 16 februari 2012 och därefter reviderade den 21 juni 2019 (*de reviderade FATF-rekommendationerna*) och i synnerhet FATF:s rekommendation nr 15 om ny teknik, FATF:s rekommendation nr 16 om elektroniska överföringar och de reviderade tolkningsnoterna till dessa rekommendationer, tillämpas på ett enhetligt sätt i hela unionen och att det i synnerhet inte förekommer någon diskriminering eller diskrepans mellan, å ena sidan, nationella betalningar eller överföringar av virtuella tillgångar inom medlemsstaterna och, å andra sidan, gränsöverskridande betalningar eller överföringar av virtuella tillgångar mellan medlemsstaterna. Enskilda medlemsstaters icke samordnade åtgärder kan på området gränsöverskridande överföringar av medel och virtuella tillgångar inverka väsentligt på hur väl betalningssystemen och tjänsterna för virtuella tillgångar fungerar på unionsnivå och kan därför skada den inre marknaden på området finansiella tjänster.
- (7) För att främja ett enhetligt internationellt tillvägagångssätt och öka effektiviteten i kampen mot penningtvätt och finansiering av terrorism, bör man vid unionens ytterligare åtgärder ta hänsyn till utvecklingen på internationell nivå, särskilt de reviderade FATF-rekommendationerna.
- (8) Deras globala räckvidd, den hastighet med vilken transaktioner kan genomföras och den möjliga anonymitet som deras överföring erbjuder gör att virtuella tillgångar är särskilt mottagliga för brottsligt missbruk, inbegripet i gränsöverskridande sammanhang. För att effektivt hantera riskerna med missbruk av virtuella tillgångar för penningtvätt och finansiering av terrorism bör unionen verka för en tillämpning på global nivå av de standarder som genomförts genom denna förordning och en utveckling av den internationella och jurisdiktionsöverskridande dimensionen av ramen för reglering och tillsyn av överföringar av virtuella tillgångar vad gäller penningtvätt och finansiering av terrorism.

⁽⁶⁾ Europaparlamentets och rådets direktiv 2009/110/EG av den 16 september 2009 om rätten att starta och driva affärsverksamhet i institut för elektroniska pengar samt om tillsyn av sådan verksamhet, om ändring av direktiven 2005/60/EG och 2006/48/EG och om upphävande av direktiv 2000/46/EG (EUT L 267, 10.10.2009, s. 7).

- (9) Genom Europaparlamentets och rådets direktiv (EU) 2015/849 (7), till följd av ändringen genom Europaparlamentets och rådets direktiv (EU) 2018/843 (8), infördes en definition av virtuella valutor, och leverantörer som erbjuder växlingstjänster mellan virtuella valutor och fiatvalutor samt tillhandahållare av plånböcker för virtuella valutor togs med bland de enheter som omfattas av kraven för bekämpning av penningtvätt och finansiering av terrorism enligt unionsrätten. Den senaste internationella utvecklingen, särskilt inom ramverket för FATF, innebär nu ett behov att reglera ytterligare kategorier av leverantörer av tjänster för virtuella tillgångar som ännu inte omfattas, samt att bredda den nuvarande definitionen av virtuell valuta.
- (10) Definitionen av kryptotillgångar i Europaparlamentets och rådets förordning (EU) 2023/1114 (9) motsvarar definitionen av virtuella tillgångar i FATF:s reviderade rekommendationer, och att förteckningen över kryptotillgångstjänster och leverantörer av kryptotillgångstjänster som omfattas av den förordningen även omfattar de leverantörer av tjänster för virtuella tillgångar som identifierats som sådana av FATF och som anses kunna ge upphov till problem med penningtvätt och finansiering av terrorism. För att säkerställa samstämmighet i unionsrätten inom detta område bör den här förordningen använda samma definitioner av kryptotillgångar, kryptotillgångstjänster och leverantörer av kryptotillgångstjänster som de som används i förordning (EU) 2023/1114.
- (11) Genomförandet och verkställigheten av denna förordning utgör lämpliga och effektiva sätt att förebygga och bekämpa penningtvätt och finansiering av terrorism.
- (12) Denna förordning är inte avsedd att leda till omotiverade bördor eller oproportionella kostnader för betaltjänstleverantörer, leverantörer av kryptotillgångstjänster eller personer som använder deras tjänster. I det avseendet bör den förebyggande strategin vara målinriktad, proportionell och i full överensstämmelse med den fria rörligheten för kapital som garanteras i hela unionen.
- (13) I unionens reviderade strategi mot finansiering av terrorism av den 17 juli 2008 (*den reviderade strategin*) anges att insatser för att förebygga finansiering av terrorism och att kontrollera hur misstänkta terrorister använder sina egna finansiella medel måste fortsätta. Det fastslås där att FATF ständigt arbetar för att förbättra sina rekommendationer och skapa en samsyn om hur de ska genomföras. I den reviderade strategin noteras att det regelbundet utvärderas hur alla FATF-medlemmar och medlemmar av regionala organ efter FATF-modell genomför de reviderade FATF-rekommendationerna och att det därför är viktigt att medlemsstaterna intar en gemensam hållning till genomförandet.
- (14) I sitt meddelande av den 7 maj 2020 om en handlingsplan för en övergripande EU-politik för att förhindra penningtvätt och finansiering av terrorism fastställde kommissionen dessutom sex prioriterade områden för brådskande åtgärder för att förbättra unionens system för bekämpning av penningtvätt och finansiering av terrorism, bland annat fastställandet av ett enhetligt regelverk för systemet i unionen så att reglerna blir mer detaljerade och harmoniserade, särskilt för att ta hänsyn till konsekvenserna av teknisk innovation och utveckling inom internationella standarder och för att undvika olikheter i genomförandet av befintliga regler. Arbetet på internationell nivå tyder på att de sektorer eller enheter som omfattas av det systemet bör utvidgas och det bör bedömas hur det ska tillämpas på leverantörer av kryptotillgångstjänster som hittills inte omfattats av det.

(7) Europaparlamentets och rådets direktiv (EU) 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, om ändring av Europaparlamentets och rådets förordning (EU) nr 648/2012 och om upphävande av Europaparlamentets och rådets direktiv 2005/60/EG och kommissionens direktiv 2006/70/EG (EUT L 141, 5.6.2015, s. 73).

(8) Europaparlamentets och rådets direktiv (EU) 2018/843 av den 30 maj 2018 om ändring av direktiv (EU) 2015/849 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism och om ändring av direktiven 2009/138/EG och 2013/36/EU (EUT L 156, 19.6.2018, s. 43).

(9) Europaparlamentets och rådets förordning (EU) 2023/1114 av den 31 maj 2023 om marknader för kryptotillgångar och om ändring av förordningarna (EU) nr 1093/2010 och (EU) nr 1095/2010 samt av direktiven 2013/36/EU och (EU) 2019/1937 (EUT L 150, 9.6.2023, s. 40).

- (15) För att förebygga finansiering av terrorism har åtgärder vidtagits i syfte att frysa vissa personers, grupper och enheters penningmedel och ekonomiska resurser, däribland rådets förordningar (EG) nr 2580/2001⁽¹⁰⁾, (EG) nr 881/2002⁽¹¹⁾ och (EU) nr 356/2010⁽¹²⁾. Av samma skäl har åtgärder vidtagits i syfte att skydda det finansiella systemet mot att penningmedel och ekonomiska resurser överförs för terroriständamål. direktiv (EU) 2015/849 innehåller ett antal sådana åtgärder. Dessa åtgärder kan dock inte helt hindra terrorister eller andra brottslingar från att få tillgång till betalningssystem för att överföra sina medel.
- (16) För att penningtvätt och finansiering av terrorism ska kunna förebyggas, upptäckas och utredas och restriktiva åtgärder ska kunna genomföras, särskilt de som införs genom förordningarna (EG) nr 2580/2001, (EG) nr 881/2002 och (EU) nr 356/2010, är det särskilt viktigt och värdefullt att överföringar av medel och kryptotillgångar fullständigt kan spåras. För att säkerställa att uppgifterna vidarebefordras genom hela betalningskedjan eller kedjan för överföring av kryptotillgångar är det därför lämpligt att införa en skyldighet för betaltjänstleverantörerna att till överföringar av medel foga uppgifter om betalaren och betalningsmottagaren och för leverantörerna av kryptotillgångstjänster att till överföringar av kryptotillgångar foga uppgifter om avsändaren och mottagaren.
- (17) Vissa överföringar av kryptotillgångar medför särskilda högriskfaktorer för penningtvätt, finansiering av terrorism och annan brottslig verksamhet, särskilt överföringar som rör varor, transaktioner eller teknik som utformats för att öka anonymiteten, inbegripet privata plånböcker, mixertjänster eller tumlartjänster. För att säkerställa spårbarheten för sådana överföringar bör Europeiska tillsynsmyndigheten (Europeiska bankmyndigheten), som inrättades genom Europaparlamentets och rådets förordning (EU) nr 1093/2010⁽¹³⁾ (EBA), särskilt klargöra hur de riskfaktorer som förtecknas i bilaga III till direktiv (EU) 2015/849 ska tas i beaktande av leverantörer av kryptotillgångstjänster, inbegripet när de utför transaktioner med enheter utanför unionen som inte är reglerade, registrerade eller har tillstånd i något tredjeland, eller med fristående adresser. Om situationer med högre risk identifieras bör EBA utfärda riktlinjer som anger vilka skärpta åtgärder för kundkännedom som ansvariga enheter bör överväga att vidta för att minska dessa risker, inbegripet införande av lämpliga förfaranden, såsom användning av analysverktyg som använder teknik för distribuerade liggare (DLT), för att bestämma kryptotillgångarnas ursprung eller destination.
- (18) Denna förordning bör tillämpas utan att det påverkar tillämpningen av nationella restriktiva åtgärder och unionens restriktiva åtgärder som införs genom förordningar som grundas på artikel 215 i fördraget om Europeiska unionens funktionssätt, såsom förordningarna (EG) nr 2580/2001, (EG) nr 881/2002 och (EU) nr 356/2010 och rådets förordningar (EU) nr 267/2012⁽¹⁴⁾, (EU) 2016/1686⁽¹⁵⁾ och (EU) 2017/1509⁽¹⁶⁾, som kan kräva att betalarnas och betalningsmottagarnas betaltjänstleverantörer, avsändarnas och mottagarnas leverantörer av kryptotillgångstjänster, förmedlande betaltjänstleverantörer, samt förmedlande leverantörer av kryptotillgångstjänster, vidtar lämpliga åtgärder för att frysa vissa medel och kryptotillgångar eller att de iakttar särskilda restriktioner avseende vissa överföringar av medel eller kryptotillgångar. Betaltjänstleverantörer och leverantörer av

⁽¹⁰⁾ Rådets förordning (EG) nr 2580/2001 av den 27 december 2001 om särskilda restriktiva åtgärder mot vissa personer och enheter i syfte att bekämpa terrorism (EGT L 344, 28.12.2001, s. 70).

⁽¹¹⁾ Rådets förordning (EG) nr 881/2002 av den 27 maj 2002 om införande av vissa särskilda restriktiva åtgärder mot vissa med organisationerna Isil (Daish) och al-Qaida associerade personer och enheter (EGT L 139, 29.5.2002, s. 9).

⁽¹²⁾ Rådets förordning (EU) nr 356/2010 av den 26 april 2010 om införande av vissa särskilda restriktiva åtgärder mot vissa fysiska eller juridiska personer, enheter eller organ mot bakgrund av situationen i Somalia (EUT L 105, 27.4.2010, s. 1).

⁽¹³⁾ Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12).

⁽¹⁴⁾ Rådets förordning (EU) nr 267/2012 av den 23 mars 2012 om restriktiva åtgärder mot Iran och om upphävande av förordning (EU) nr 961/2010 (EUT L 88, 24.3.2012, s. 1).

⁽¹⁵⁾ Rådets genomförandeförordning (EU) 2016/1686 av den 20 september 2016 om införande av ytterligare restriktiva åtgärder mot Isil (Daish) och al-Qaida samt fysiska och juridiska personer, enheter eller organ som har samröre med dem (EUT L 255, 21.9.2016, s. 1).

⁽¹⁶⁾ Rådets förordning (EU) 2017/1509 av den 30 augusti 2017 om restriktiva åtgärder mot Demokratiska folkrepubliken Korea och om upphävande av förordning (EG) nr 329/2007 (EUT L 224, 31.8.2017, s. 1).

kryptotillgångstjänster bör ha interna strategier, förfaranden och kontroller för att säkerställa genomförandet av dessa restriktiva åtgärder, inbegripet granskning mot unionens och nationella förteckningar över personer som omfattas av sanktioner. EBA bör utfärda riktlinjer som specificerar dessa interna strategier, förfaranden och kontroller. Avsikten är att de krav på interna strategier, förfaranden och kontroller för restriktiva åtgärder som fastställs i denna förordning inom en snar framtid ska upphävas genom Europaparlamentets och rådets förordning om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism.

- (19) Behandlingen av personuppgifter enligt denna förordning bör ske i full överensstämmelse med Europaparlamentets och rådets förordning (EU) 2016/679⁽¹⁷⁾. Ytterligare behandling av personuppgifter för kommersiella ändamål bör vara strängt förbjuden. Samtliga medlemsstater anser att bekämpningen av penningtvätt och finansiering av terrorism har ett starkt allmänintresse. Vid tillämpningen av denna förordning krävs det att överföring av personuppgifter till ett tredjeland sker i enlighet med kapitel V i förordning (EU) 2016/679. Det är viktigt att betaltjänstleverantörer och leverantörer av kryptotillgångstjänster som är verksamma i flera jurisdiktioner med filialer eller dotterföretag utanför unionen inte förhindras att överföra information om misstänkta transaktioner inom samma organisation, förutsatt att de tillämpar lämpliga säkerhetsåtgärder. Avsändarens och mottagarens leverantör av kryptotillgångstjänster, betalarens och betalningsmottagarens betaltjänstleverantör samt den förmedlande betaltjänstleverantören och den förmedlande leverantören av kryptotillgångstjänster bör dessutom förfoga över lämpliga tekniska och organisatoriska medel för att skydda personuppgifter mot oavsiktlig förlust, ändring och obehörigt röjande eller obehörig åtkomst.
- (20) Personer som endast omvandlar pappersdokument till elektroniska uppgifter och som agerar enligt ett kontrakt med en betaltjänstleverantör och personer som tillhandahåller betaltjänstleverantörer enbart med meddelande-system eller andra stödsystem för överföring av medel eller system för clearing och avveckling bör inte omfattas av denna förordnings tillämpningsområde.
- (21) Personer som endast tillhandahåller kringliggande infrastruktur, såsom tjänstleverantörer av internetnätverk och internetinfrastruktur, molntjänstleverantörer eller programvaruutvecklare, som gör det möjligt för en annan enhet att tillhandahålla överföringstjänster för kryptotillgångar bör inte omfattas av denna förordning, såvida de inte utför överföringar av kryptotillgångar.
- (22) Denna förordning bör inte tillämpas på överföringar av kryptotillgångar från person till person som genomförs utan medverkan av en leverantör av kryptotillgångstjänster, eller i fall där både avsändaren och mottagaren är leverantörer av överföringstjänster för kryptotillgångar, som agerar för egen räkning.
- (23) Överföringar av medel som motsvarar de tjänster som avses i artikel 3 a–m och o i Europaparlamentets och rådets direktiv (EU) 2015/2366⁽¹⁸⁾ omfattas inte av denna förordning. Det är också lämpligt att undanta överföringar av medel och e-pengartoken, enligt definitionen i artikel 3.1.7 i förordning (EU) 2023/1114, där risken för penningtvätt eller finansiering av terrorism är liten. Sådana undantag bör omfatta betalkort, instrument för elektroniska pengar, mobiltelefoner eller annan förbetald eller efterhandsbetald digital utrustning eller it-utrustning med liknande egenskaper, där de uteslutande används för köp av varor eller tjänster och kortets, instrumentets eller utrustningens nummer åtföljer alla överföringar. Användningen av ett betalkort, ett instrument för elektroniska pengar, en mobiltelefon eller annan förbetald eller efterhandsbetald digital utrustning eller it-utrustning med liknande egenskaper för att verkställa en överföring av medel eller e-pengartoken mellan fysiska personer som agerar i egenskap av konsumenter för andra ändamål än handelsverksamhet, affärsverksamhet eller yrkesverksamhet omfattas dock av denna förordning. Dessutom bör uttag från uttagsautomater, betalning av skatter, böter eller andra avgifter, överföringar av medel som görs genom checkavbildningar, inklusive trunkerade checkar eller växlar, och överföringar av medel där både betalaren och betalningsmottagaren är betaltjänstleverantörer som agerar för egen räkning, undantas från denna förordnings tillämpningsområde.

⁽¹⁷⁾ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

⁽¹⁸⁾ 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 (EUT L 337, 23.12.2015, s. 35).

- (24) Kryptotillgångar som är unika och inte fungibla omfattas inte av kraven i denna förordning såvida de inte klassificeras som kryptotillgångar eller medel enligt förordning (EU) 2023/1114.
- (25) Uttagsautomater för kryptotillgångar (*kryptobankomater*) kan göra det möjligt för användare att överföra kryptotillgångar till en adress för kryptotillgångar genom att deponera kontanter, ofta utan någon form av identifiering och kontroll av kunden. Kryptobankomater är särskilt utsatta för risker för penningtvätt och finansiering av terrorism eftersom anonymiteten och möjligheten att använda kontanter av okänt ursprung gör dem till ett idealiskt verktyg för olaglig verksamhet. Med tanke på kryptobankomaternas roll när det gäller att tillhandahålla eller aktivt underlätta överföringar av kryptotillgångar, bör överföringar av kryptotillgångar med koppling till kryptobankomater omfattas av denna förordnings tillämpningsområde.
- (26) För att beakta de nationella betalningssystemens särskilda egenskaper, och förutsatt att det alltid är möjligt att spåra överföringen av medel tillbaka till betalaren bör medlemsstaterna dessutom kunna undanta vissa inhemska överföringar av medel som avser låga belopp som används för köp av varor eller tjänster, inbegripet elektroniska girobetalningar, från denna förordnings tillämpningsområde.
- (27) På grund av den inneboende gränslösa karaktären hos och den globala räckvidden för överföringar av kryptotillgångar och tillhandahållandet av kryptotillgångstjänster, finns det inga objektiva anledningar att göra åtskillnad mellan behandlingen av nationella överföringar och gränsöverskridande överföringar när det gäller risken för penningtvätt och finansiering av terrorism. För att återspegla dessa särdrag bör det därför inte beviljas några undantag från denna förordnings tillämpningsområde för inhemska överföringar av kryptotillgångar av lågt värde, i enlighet med FATF:s krav att alla överföringar av kryptotillgångar ska behandlas som gränsöverskridande överföringar.
- (28) Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör säkerställa att uppgifter om betalaren och betalningsmottagaren eller avsändaren och mottagaren inte saknas eller är ofullständiga.
- (29) För att inte inverka negativt på betalningssystemens effektivitet och för att skapa en rimlig avvägning mellan risken för att transaktioner kommer att ske utanför det officiella systemet som ett resultat av alltför strikta identifieringskrav och det potentiella terroristhot som små överföringar av medel innebär, bör, vid överföringar av medel där en kontroll ännu inte har ägt rum, skyldigheten att kontrollera att uppgifterna om betalaren eller betalningsmottagaren är riktiga endast tillämpas på enskilda överföringar av medel som överstiger 1 000 EUR, om inte överföringen förefaller vara sammankopplad till andra överföringar av medel som tillsammans skulle överstiga 1 000 EUR, medlen har tagits emot eller betalats ut i kontanter eller i anonyma elektroniska pengar eller det finns rimliga skäl att misstänka penningtvätt eller finansiering av terrorism.
- (30) Jämfört med överföringar av medel kan överföringar av kryptotillgångar genomföras i större skala och snabbare mellan flera jurisdiktioner tack vare deras globala räckvidd och tekniska egenskaper. Utöver kryptotillgångarnas pseudoanonymitet ger dessa särdrag hos överföringar av kryptotillgångar brottslingar möjlighet att snabbt utföra stora olagliga överföringar och samtidigt kringgå kraven på spårbarhet och undvika upptäckt genom att strukturera en stor transaktion i mindre belopp med hjälp av flera till synes orelaterade DLT-adresser, inbegripet DLT-adresser för engångsanvändning, och med användande av automatiserade processer. De flesta kryptotillgångar är också mycket volatila och deras värde kan fluktuera avsevärt på mycket kort tid, vilket gör beräkningen av sammankopplade transaktioner mer osäker. För att återspegla dessa särdrag bör överföringar av kryptotillgångar vara föremål för samma krav oavsett belopp och oavsett om de är inhemska eller gränsöverskridande överföringar.

- (31) När det gäller överföringar av medel eller överföringar av kryptotillgångar där en kontroll anses ha ägt rum bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster inte vara skyldiga att kontrollera riktigheten i de uppgifter om betalaren eller betalningsmottagaren som åtföljer varje överföring av medel, eller om avsändaren och mottagaren som åtföljer varje överföring av kryptotillgångar, förutsatt att skyldigheterna i direktiv (EU) 2015/849 är fullgjorda.
- (32) Mot bakgrund av unionens lagstiftningsakter om betaltjänster, nämligen Europaparlamentets och rådets förordning (EU) nr 260/2012⁽¹⁹⁾, direktiv (EU) 2015/2366 och Europaparlamentets och rådets förordning (EU) 2021/1230⁽²⁰⁾, bör det vara tillräckligt att föreskriva att endast förenklade uppgifter, såsom betalkontonummer eller en unik transaktionsidentifierare, åtföljer överföringar av medel inom unionen.
- (33) För att myndigheter som ansvarar för bekämpning av penningtvätt eller finansiering av terrorism i tredjeländer ska kunna spåra källan till de medel eller kryptotillgångar som används för sådana ändamål bör överföringar av medel eller överföringar av kryptotillgångar från unionen till utanför unionen åtföljas av fullständiga uppgifter om betalaren och betalningsmottagaren när det gäller överföring av medel och om avsändaren och mottagaren när det gäller överföring av kryptotillgångar. Fullständiga uppgifter om betalaren och betalningsmottagaren bör omfatta identifieringskoden för juridiska personer (LEI), eller en likvärdig officiell identifieringskod, om den identifieringskoden lämnas av betalaren till sin betaltjänstleverantör, eftersom det skulle göra det möjligt att bättre identifiera de parter som deltar i en överföring av medel och enkelt skulle kunna inkluderas i befintliga format för betalningsmeddelanden, såsom det som utvecklats av Internationella standardiseringsorganisationen för elektroniskt datautbyte mellan finansiella institut. De myndigheter som ansvarar för bekämpning av penningtvätt eller finansiering av terrorism i tredjeländer bör endast ges tillgång till fullständiga uppgifter om betalaren och betalningsmottagaren eller om avsändaren och mottagaren, beroende på vad som är tillämpligt, för att kunna förebygga, upptäcka och utreda penningtvätt eller finansiering av terrorism.
- (34) Kryptotillgångar finns i en gränslös virtuell verklighet och kan överföras till vilken leverantör av kryptotillgångstjänster som helst, oberoende av om den leverantören är registrerad eller inte i en viss jurisdiktion. Många jurisdiktioner utanför unionen har regler om dataskydd och verkställighet som skiljer sig från dem som gäller i unionen. Vid överföring av kryptotillgångar för en kunds räkning till en leverantör av kryptotillgångstjänster som inte är registrerad i unionen bör avsändarens leverantör av kryptotillgångstjänster bedöma förmågan hos mottagarens leverantör av kryptotillgångstjänster att ta emot och lagra den information som krävs enligt denna förordning i enlighet med förordning (EU) 2016/679, i tillämpliga fall med användning av tillgängliga alternativ i kapitel V i förordning (EU) 2016/679. Europeiska dataskyddsstyrelsen bör, efter samråd med EBA, utfärda riktlinjer för det praktiska genomförandet av dataskyddskrav för överföring av personuppgifter till tredjeländer i samband med överföringar av kryptotillgångar. Det kan uppstå situationer där personuppgifter inte kan över-sändas på grund av att kraven i förordning (EU) 2016/679 inte kan uppfyllas. EBA bör utfärda riktlinjer om lämpliga förfaranden för att avgöra om överföringen av kryptotillgångar bör verkställas, aviseras eller avbrytas i sådana fall.
- (35) Medlemsstaternas myndigheter som ansvarar för att bekämpa penningtvätt och finansiering av terrorism och berörda rättsliga och brottsbekämpande myndigheter i medlemsstaterna och på unionsnivå bör intensifiera samarbetet sinsemellan och med berörda myndigheter i tredjeländer, inklusive i utvecklingsländer, i syfte att ytterligare stärka öppenheten, samt utbytet av information och bästa praxis.
- (36) Avsändarens leverantör av kryptotillgångstjänster bör säkerställa att överföringar av kryptotillgångar åtföljs av avsändarens namn, avsändarens adress i den distribuerade liggaren, i fall där en överföring av kryptotillgångar registrerats på ett nätverk som använder DLT eller liknande teknik, avsändarens kontonummer för kryptotillgångar, i fall där konto finns och används för transaktionen, avsändarens adress, inbegripet landets namn, officiella personliga dokumentnummer och kundnummer, eller, alternativt, avsändarens födelsedatum och

⁽¹⁹⁾ Europaparlamentets och rådets förordning (EU) nr 260/2012 av den 14 mars 2012 om antagande av tekniska och affärsmässiga krav för betalningar och autogireringar i euro och om ändring av förordning (EG) nr 924/2009 (EUT L 94, 30.3.2012, s. 22).

⁽²⁰⁾ Europaparlamentets och rådets förordning (EU) 2021/1230 av den 14 juli 2021 om gränsöverskridande betalningar i unionen (EUT L 274, 30.7.2021, s. 20).

födelseort och, under förutsättning att det nödvändiga fältet finns i det relevanta meddelandeformatet, och om avsändaren har tillhandahållit denna kod till sin leverantör av kryptotillgångstjänster, den aktuella LEI-koden, eller, om sådan saknas, någon annan tillgänglig likvärdig officiell identifieringskod för avsändaren. Uppgifterna bör lämnas på ett säkert sätt och före, eller samtidigt som eller i samband med, överföringen av kryptotillgångar.

- (37) Avsändarens leverantör av kryptotillgångstjänster bör även säkerställa att överföringar av kryptotillgångar åtföljs av mottagarens namn, mottagarens adress i den distribuerade liggaren, i fall där en överföring av kryptotillgångar registrerats på ett nätverk som använder DLT eller liknande teknik, mottagarens kontonummer, i fall där konto finns och används för transaktionen, samt, under förutsättning att det nödvändiga fältet finns i det relevanta meddelandeformatet, och om avsändaren har tillhandahållit denna kod till sin leverantör av kryptotillgångstjänster, den aktuella LEI-koden, eller, om sådan saknas, någon annan tillgänglig likvärdig officiell identifieringskod för mottagaren. Uppgifterna bör lämnas på ett säkert sätt och före, eller samtidigt som eller i samband med, överföringen av kryptotillgångar.
- (38) När det gäller överföringar av kryptotillgångar bör kraven i denna förordning tillämpas på alla överföringar, inbegripet överföring av kryptotillgångar till eller från en fristående adress, så länge en leverantör av kryptotillgångstjänster är inblandad.
- (39) Vid överföring till eller från en fristående adress bör leverantören av kryptotillgångstjänster samla in uppgifterna om både avsändaren och mottagaren, vanligtvis från dess kund. Leverantören av kryptotillgångstjänster bör i princip inte vara skyldig att kontrollera uppgifterna om användaren av den fristående adressen. Vid en överföring av ett belopp som överstiger 1 000 EUR och som sänds till eller tas emot från en fristående adress på uppdrag av en kund till en leverantör av kryptotillgångstjänster bör dock den leverantören av kryptotillgångstjänster kontrollera om den kunden faktiskt äger eller kontrollerar den fristående adressen.
- (40) Vad gäller medel som överförs från en enskild betalare till flera betalningsmottagare med en batchöverföring som innehåller enskilda överföringar från unionen till utanför unionen, bör det föreskrivas att sådana enskilda överföringar endast ska åtföljas av betalarens betalkontonummer eller den unika transaktionsidentifieraren samt fullständiga uppgifter om betalningsmottagaren, under förutsättning att batchfilen innehåller fullständiga verifierade uppgifter om betalaren och fullständiga uppgifter om betalningsmottagaren, som är fullständigt spårbara.
- (41) När det gäller batchöverföringar av kryptotillgångar bör inlämning av uppgifter om avsändaren och mottagaren i batchfiler godtas så länge som den inlämningen sker omedelbart och säkert. Det bör inte vara tillåtet att lämna in de erforderliga uppgifterna efter överföringen, eftersom inlämningen måste ske före eller vid den tidpunkt då transaktionen slutförs, och leverantörer av kryptotillgångstjänster eller andra ansvariga enheter bör lämna in de erforderliga uppgifterna samtidigt som batchöverföringen av kryptotillgångar sker.
- (42) För att kunna kontrollera om erforderliga uppgifter om betalaren och betalningsmottagaren åtföljer överföringarna av medel, och för att upptäcka misstänkta transaktioner, bör betalningsmottagarens betaltjänstleverantör och den förmedlande betaltjänstleverantören ha effektiva förfaranden för fastställande av huruvida uppgifter om betalaren och betalningsmottagaren saknas eller är ofullständiga. Dessa förfaranden bör inbegripa övervakning efter eller samtidigt med överföringarna där så är lämpligt. De behöriga myndigheterna bör säkerställa att betaltjänstleverantörerna inkluderar den nödvändiga transaktionsinformationen i den elektroniska överföringen eller i ett tillhörande meddelande genom hela betalningskedjan.
- (43) När det gäller överföringar av kryptotillgångar bör mottagarens leverantör av kryptotillgångstjänster införa effektiva förfaranden för att upptäcka om uppgifter om avsändaren eller mottagaren saknas eller är ofullständiga. Dessa förfaranden bör, när så är lämpligt, omfatta övervakning efter eller samtidigt med överföringarna. Det bör inte krävas att uppgifterna direkt medföljer själva överföringen av kryptotillgångar, så länge som de lämnas in före, eller samtidigt som eller i samband med, överföringen av kryptotillgångar och görs tillgängliga för berörda myndigheter på begäran.

- (44) Mot bakgrund av den potentiella risk för penningtvätt och finansiering av terrorism som anonyma betalningar utgör bör det krävas att betaltjänstleverantörer begär uppgifter om betalaren och betalningsmottagaren och att leverantörer av kryptotillgångstjänster begär uppgifter om avsändaren och mottagaren. I enlighet med den riskbaserade metod som FATF utvecklat bör områden med högre respektive lägre risk fastställas för att risken för penningtvätt och finansiering av terrorism ska kunna motverkas bättre. Därför bör mottagarens leverantör av kryptotillgångstjänster, betalningsmottagarens betaltjänstleverantör, den förmedlande betaltjänstleverantören och den förmedlande leverantören av kryptotillgångstjänster ha effektiva riskbaserade förfaranden som är tillämpliga när en överföring av medel saknar de nödvändiga uppgifterna om betalaren eller betalningsmottagaren, eller när en överföring av kryptotillgångar saknar de nödvändiga uppgifterna om avsändaren eller mottagaren, för att den tjänstleverantören ska kunna avgöra om den ska verkställa, avvisa eller avbryta den överföringen och fastställa de lämpliga uppföljningsåtgärder som ska vidtas.
- (45) Leverantörer av kryptotillgångstjänster bör, liksom alla ansvariga enheter, bedöma och övervaka den risk som är förknippad med deras kunder, produkter och leveranskanaler. Leverantörer av kryptotillgångstjänster bör också bedöma den risk som är förknippad med deras transaktioner, även när de utför överföringar till eller från fristående adresser. I händelse av att leverantören av kryptotillgångstjänster har eller får kännedom om felaktiga uppgifter om avsändare eller mottagare som använder en fristående adress, eller om leverantören av kryptotillgångstjänster stöter på ovanliga eller misstänkta transaktionsmönster eller situationer med högre risk för penningtvätt och finansiering av terrorism i samband med överföringar som inbegriper fristående adresser, bör den leverantören av kryptotillgångstjänster, när så är lämpligt, vidta skärpta åtgärder för kundkännedom för att hantera och minska riskerna på lämpligt sätt. Leverantören av kryptotillgångstjänster bör ta hänsyn till dessa omständigheter vid bedömningen av huruvida en överföring av kryptotillgångar, eller en relaterad transaktion, är ovanlig och om den ska rapporteras till finansunderrättelseenheten (FIU) i enlighet med direktiv (EU) 2015/849.
- (46) Denna förordning bör ses över i samband med antagandet av en Europaparlamentets och rådets förordning om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, ett Europaparlamentets och rådets direktiv om de mekanismer som medlemsstaterna ska inrätta för att förhindra att det finansiella systemet används för penningtvätt och finansiering av terrorism och om upphävande av direktiv (EU) 2015/849 och en Europaparlamentets och rådets förordning om inrättande av en myndighet för bekämpning av penningtvätt och finansiering av terrorism och om ändring av förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010, (EU) nr 1095/2010, för att säkerställa överensstämmelse med de relevanta bestämmelserna.
- (47) Betalningsmottagarens betaltjänstleverantör, den förmedlande betaltjänstleverantören, mottagarens leverantör av kryptotillgångstjänster eller den förmedlande leverantören av kryptotillgångstjänster bör vid bedömningen av riskerna vara särskilt vaksam om den får kännedom om att uppgifter om betalaren eller betalningsmottagaren, eller om avsändaren eller mottagaren, beroende på vad som är tillämpligt, saknas eller är ofullständiga, eller om en överföring av kryptotillgångar måste anses vara misstänkt på grundval av de berörda kryptotillgångarnas ursprung eller destination, och bör rapportera misstänkta transaktioner till de behöriga myndigheterna i enlighet med rapporteringsskyldigheterna i direktiv (EU) 2015/849.
- (48) I likhet med överföringar av medel mellan betaltjänstleverantörer kan överföringar av kryptotillgångar som involverar förmedlande leverantörer av kryptotillgångstjänster underlätta överföringar som ett mellanled i en kedja av överföringar av kryptotillgångar. I linje med internationella standarder bör sådana förmedlande leverantörer också omfattas av de krav som fastställs i denna förordning, på samma sätt som befintliga skyldigheter för förmedlande betaltjänstleverantörer.
- (49) Bestämmelserna om överföringar av medel och överföringar av kryptotillgångar avseende vilka uppgifter om betalaren eller betalningsmottagaren eller avsändaren eller mottagaren som saknas eller är ofullständiga, och avseende vilka överföringar av kryptotillgångar måste anses vara misstänkta på grundval av de berörda kryptotillgångarnas ursprung eller destination, är tillämpliga utan att det påverkar betaltjänstleverantörers, förmedlande

betaltjänstleverantörers, leverantörer av kryptotillgångstjänsters och förmedlande leverantörer av kryptotillgångstjänsters skyldigheter att avvisa eller avbryta överföringar av medel och överföringar av kryptotillgångar som strider mot en civilrättslig, förvaltningsrättslig eller straffrättslig bestämmelse.

- (50) För att säkerställa teknikneutralitet bör denna förordning inte föreskriva användning av en viss teknik för överföring av transaktionsinformation från leverantörer av kryptotillgångstjänster. För att säkerställa ett effektivt genomförande av krav som är tillämpliga på leverantörer av kryptotillgångstjänster enligt denna förordning kommer standardiseringsinitiativ som kryptotillgångsindustrin deltar i eller leder att vara av avgörande betydelse. De resulterande lösningarna bör vara interoperabla genom användning av internationella eller unionsomfattande standarder som möjliggör ett snabbt informationsutbyte.
- (51) I syfte att hjälpa betaltjänstleverantörer och leverantörer av kryptotillgångstjänster att inrätta effektiva förfaranden för att upptäcka fall där de tar emot överföringar av medel eller överföringar av kryptotillgångar som saknar uppgifter eller har ofullständiga uppgifter om betalaren, betalningsmottagaren, avsändaren eller mottagaren samt vidta effektiva uppföljningsåtgärder, bör EBA utfärda riktlinjer.
- (52) För att göra det möjligt att snabbt vidta åtgärder för bekämpning av penningtvätt och finansiering av terrorism bör betaltjänstleverantörerna och leverantörerna av kryptotillgångstjänster skyndsamt besvara en begäran om uppgifter om betalaren och betalningsmottagaren eller om avsändaren och mottagaren som kommer från myndigheter med ansvar för bekämpning av penningtvätt eller finansiering av terrorism i den medlemsstat där dessa betalningstjänstleverantörer är etablerade eller där dessa leverantörer av kryptotillgångstjänster har sitt säte.
- (53) Antalet arbetsdagar som förflutit i den medlemsstat där betalarens betaltjänstleverantör finns avgör antalet dagar för att besvara en begäran om uppgifter om betalaren.
- (54) Eftersom det inte alltid är möjligt i brottsutredningar att identifiera de uppgifter som behövs eller de personer som varit inblandade i en transaktion förrän flera månader eller till och med år efter den ursprungliga överföringen av medel eller överföringen av kryptotillgångar, och för att tillgängliggöra viktig bevisning i utredningar, är det lämpligt att kräva att betaltjänstleverantörerna eller leverantörerna av kryptotillgångstjänster bevarar uppgifterna om betalaren och betalningsmottagaren eller avsändaren och mottagaren under en tidsperiod i syfte att förebygga, upptäcka och utreda penningtvätt och finansiering av terrorism. Den perioden bör begränsas till fem år, varefter alla personuppgifter bör raderas, såvida inte annat föreskrivs i nationell rätt. Om det är nödvändigt för att förebygga, upptäcka eller utreda penningtvätt eller finansiering av terrorism, och efter att ha gjort en bedömning av åtgärdens nödvändighet och proportionalitet, bör medlemsstaterna kunna tillåta eller kräva att uppgifter lagras i ytterligare högst fem år, utan att det påverkar tillämpningen av nationell straffrätt om bevis som är tillämplig på pågående brottsutredningar och rättsliga förfaranden och i full överensstämmelse med Europaparlamentets och rådets direktiv (EU) 2016/680⁽²¹⁾. Dessa åtgärder kan ses över mot bakgrund av antagandet av Europaparlamentets och rådets förordning om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism.
- (55) För att förbättra efterlevnaden av denna förordning, och i enlighet med kommissionens meddelande av den 9 december 2010 med titeln *Reinforcing sanctioning regimes in the financial services sector*, bör de behöriga myndigheternas befogenheter att vidta tillsynsåtgärder och deras sanktionsbefogenheter stärkas. Administrativa sanktioner och åtgärder bör föreskrivas och mot bakgrund av hur viktig bekämpningen av penningtvätt och finansiering av terrorism är bör medlemsstaterna fastställa sanktioner och åtgärder som är effektiva, proportionella och avskräckande. Medlemsstaterna bör underrätta kommissionen samt den permanenta interna kommitté för bekämpning av penningtvätt och finansiering av terrorism som avses i artikel 9a.7 i förordning (EU) nr 1093/2010 om sanktionerna och åtgärderna.

⁽²¹⁾ Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89).

- (56) För att säkerställa enhetliga villkor för genomförandet av denna förordning, bör kommissionen tilldelas genomförandebefogenheter. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ⁽²²⁾.
- (57) Ett antal länder och territorier som inte utgör en del av unionens territorium ingår i en monetär union med en medlemsstat, tillhör en medlemsstats valutaområde eller har undertecknat ett monetärt avtal med unionen företrädd av en medlemsstat, och har betaltjänstleverantörer som direkt eller indirekt deltar i den medlemsstatens betalnings- och avvecklingssystem. För att tillämpningen av denna förordning på överföringar mellan berörda medlemsstater och dessa länder eller territorier inte ska medföra betydande negativa effekter på dessa länders eller territoriers ekonomier bör sådana överföringar av medel kunna behandlas som överföringar av medel inom de berörda medlemsstaterna.
- (58) Med tanke på de potentiellt höga riskerna förenade med fristående adresser och den tekniska och lagstiftningsmässiga komplexitet som de innebär, inbegripet avseende kontroll av uppgifterna om ägande, bör kommissionen senast den 1 juli 2026 bedöma behovet av ytterligare specifika åtgärder för att minska de risker som följer med överföringar till eller från fristående adresser eller till eller från enheter som inte är etablerade i unionen, inbegripet införandet av möjliga restriktioner, och bör bedöma om de mekanismer som används för att kontrollera riktigheten i uppgifter om ägande av fristående adresser är ändamålsenliga och proportionerliga.
- (59) För närvarande är direktiv (EU) 2015/849 endast tillämpligt på två kategorier av leverantörer av kryptotillgångstjänster, nämligen tillhandahållare av plånböcker för virtuella valutor och leverantörer som erbjuder växlings-tjänster mellan virtuella valutor och fiatvalutor. För att täppa till befintliga kryphål i regelverket för bekämpning av penningtvätt och finansiering av terrorism och för att anpassa unionsrätten till internationella rekommendationer bör direktiv (EU) 2015/849 ändras så att det omfattar alla kategorier av leverantörer av kryptotillgångstjänster enligt definitionen i förordning (EU) 2023/1114, som omfattar ett bredare spektrum av leverantörer av kryptotillgångstjänster. För att säkerställa att leverantörer av kryptotillgångstjänster omfattas av samma krav och tillsynsnivå som kreditinstitut och finansiella institut är det framför allt lämpligt att uppdatera förteckningen över ansvariga enheter genom att i kategorin finansiella institut inkludera leverantörer av kryptotillgångstjänster vid tillämpning av direktiv (EU) 2015/849. Med beaktande av att traditionella finansiella institut också omfattas av definitionen av leverantörer av kryptotillgångstjänster när de erbjuder sådana tjänster innebär identifieringen av leverantörer av kryptotillgångstjänster som finansiella institut dessutom att en enda konsekvent uppsättning regler kan tillämpas på enheter som tillhandahåller både traditionella finansiella tjänster och kryptotillgångstjänster. Direktiv (EU) 2015/849 bör också ändras för att säkerställa att leverantörer av kryptotillgångstjänster på lämpligt sätt kan minska de risker för penningtvätt och finansiering av terrorism som de är exponerade för.
- (60) Förbindelser som upprättats mellan leverantörer av kryptotillgångstjänster och enheter etablerade i tredjeländer i syfte att verkställa överföringar av kryptotillgångar eller tillhandahålla liknande kryptotillgångstjänster uppvisar likheter med korrespondentbankförbindelser som etablerats med ett tredjelands motpartsinstitut. Eftersom dessa förbindelser kännetecknas av en fortlöpande och upprepad karaktär bör de betraktas som en typ av korrespondentförbindelse och vara föremål för särskilda skärpta åtgärder för kundkännedom som i princip liknar dem som tillämpas i samband med banktjänster och finansiella tjänster. I synnerhet bör leverantörer av kryptotillgångstjänster, när de upprättar en ny korrespondentförbindelse med en motparts enhet, tillämpa särskilda skärpta åtgärder för kundkännedom för att identifiera och bedöma riskexponeringen avseende den motparten, på

⁽²²⁾ Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

grundval av motpartens anseende, tillsynens kvalitet och motpartens kontroller för bekämpning av penningtvätt och finansiering av terrorism. På grundval av de uppgifter som samlats in bör korrespondentleverantörerna av kryptotillgångstjänster vidta lämpliga riskreducerande åtgärder, med särskilt beaktande av den potentiellt högre risken för penningtvätt och finansiering av terrorism som är förenad med enheter som inte är registrerade eller inte har tillstånd. Det är särskilt relevant så länge genomförandet av FATF:s standarder avseende kryptotillgångar på global nivå fortfarande är ojämn, vilket innebär ytterligare risker och utmaningar. EBA bör ge vägledning om hur leverantörer av kryptotillgångstjänster bör genomföra de skärpta åtgärderna för kundkännedom och bör ange lämpliga riskreducerande åtgärder, inbegripet de minimiåtgärder som ska vidtas, när de interagerar med enheter som tillhandahåller kryptotillgångstjänster och som inte är registrerade eller inte har tillstånd.

- (61) Genom förordning (EU) 2023/1114 har ett omfattande regelverk för leverantörer av kryptotillgångstjänster inrättats, som harmoniserar reglerna för auktorisation och drift av leverantörer av kryptotillgångstjänster i hela unionen. För att undvika dubbla krav bör direktiv (EU) 2015/849 ändras så att registreringskraven tas bort för de kategorier av leverantörer av kryptotillgångstjänster som kommer att omfattas av en gemensam licensieringsordning enligt förordning (EU) 2023/1114.
- (62) Eftersom målen för denna förordning, som består i att bekämpa penningtvätt och finansiering av terrorism, inbegripet genom att följa internationella standarder och säkerställa att grundläggande uppgifter om betalare och betalningsmottagare vid överföring av medel, och avsändare och mottagare vid överföring av kryptotillgångar, är tillgängliga, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning eller verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå dessa mål.
- (63) Denna förordning omfattas av bestämmelserna i förordning (EU) 2016/679 och Europaparlamentets och rådets förordning (EU) 2018/1725 ⁽²³⁾. Den är förenlig med de grundläggande rättigheter och de principer som erkänns i Europeiska unionens stadga om de grundläggande rättigheterna, särskilt rätten till respekt för privatlivet och familjelivet (artikel 7), rätten till skydd av personuppgifter (artikel 8), rätten till ett effektivt rättsmedel och till en opartisk domstol (artikel 47) samt *ne bis in idem*-principen.
- (64) För att säkerställa överensstämmelse med förordning (EU) 2023/1114 bör den här förordningen tillämpas från och med den dag då den förordningen börjar tillämpas. Senast den dagen bör medlemsstaterna också införliva ändringarna av direktiv (EU) 2015/849.
- (65) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i förordning (EU) 2018/1725 och avgav ett yttrande den 22 september 2021 ⁽²⁴⁾.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Syfte, tillämpningsområde och definitioner

Artikel 1

Innehåll

I denna förordning fastställs regler om de uppgifter om betalare och betalningsmottagare som ska åtfölja överföringar av medel, i alla valutor, och de uppgifter om avsändare och mottagare som ska åtfölja överföringar av kryptotillgångar, i syfte att förebygga, upptäcka och utreda penningtvätt och finansiering av terrorism, när minst en av de betaltjänstleverantörer eller leverantörer av kryptotillgångstjänster som är involverade i överföringen av medel eller överföringen av kryptotillgångar är etablerad eller har sitt säte, beroende på vad som är tillämpligt, i unionen. I denna förordning fastställs dessutom regler om interna strategier, förfaranden och kontroller för att säkerställa att restriktiva åtgärder vidtas om minst en av de betaltjänstleverantörer eller leverantörer av kryptotillgångstjänster som medverkar i överföringen av medel eller överföringen av kryptotillgångar är etablerad eller har sitt säte, beroende på vad som är tillämpligt, i unionen.

⁽²³⁾ Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

⁽²⁴⁾ EUT C 524, 29.12.2021, s. 10.

Artikel 2

Tillämpningsområde

1. Denna förordning ska tillämpas på överföringar av medel, i alla valutor, som sänds eller tas emot av en betal-tjänstleverantör eller en förmedlande betaltjänstleverantör som är etablerad i unionen. Den ska också tillämpas på överföringar av kryptotillgångar, inbegripet överföringar av kryptotillgångar, som utförs med hjälp av kryptobankomater, om leverantören av kryptotillgångstjänster, eller den förmedlande leverantören av kryptotillgångstjänster, till antingen avsändaren eller mottagaren har sitt säte i unionen.

2. Denna förordning ska inte tillämpas på de tjänster som förtecknas i artikel 3 a–m och o i direktiv (EU) 2015/2366.

3. Denna förordning ska inte tillämpas på överföringar av medel eller på överföringar av e-pengartoken, enligt definitionen i artikel 3.1.7 i förordning (EU) 2023/1114, som utförs med hjälp av ett betalkort, ett instrument för elektroniska pengar, en mobiltelefon eller annan förbetald eller efterhandsbetald digital utrustning eller it-utrustning med liknande egenskaper, förutsatt att följande villkor är uppfyllda:

- a) Det kortet, det instrumentet eller den utrustningen används uteslutande för att betala för varor eller tjänster, och
- b) alla överföringar i samband med transaktionen åtföljs av numret på det kortet, det instrumentet eller den utrustningen.

Denna förordning ska dock tillämpas om ett betalkort, ett instrument för elektroniska pengar, en mobiltelefon eller annan förbetald eller efterhandsbetald digital utrustning eller it-utrustning med liknande egenskaper används för att verkställa en överföring av medel eller e-pengartoken mellan fysiska personer som agerar i egenskap av konsumenter för andra ändamål än handelsverksamhet, affärsverksamhet eller yrkesverksamhet.

4. Denna förordning ska inte tillämpas på personer som inte har någon annan verksamhet än att omvandla pappersdokument till elektroniska uppgifter och som gör detta i enlighet med ett avtal med en betaltjänstleverantör eller personer som inte har någon annan verksamhet än att tillhandahålla betaltjänstleverantörers meddelandesystem eller andra stödsystem för överföring av medel eller system för clearing och avveckling.

Denna förordning ska inte gälla för en överföring av medel där något av följande villkor är uppfyllt:

- a) Den involverar att betalaren tar ut kontanter från betalarens eget betalkonto.
- b) Den utgör en överföring av medel till en offentlig myndighet som betalning för skatter, böter eller andra avgifter inom en medlemsstat.
- c) Både betalaren och betalningsmottagaren är betaltjänstleverantörer som agerar för egen räkning.
- d) Den görs genom checkavbildningar, inklusive trunckerade checkar.

Denna förordning ska inte tillämpas på en överföring av kryptotillgångar där något av följande villkor är uppfyllt:

- a) Både avsändaren och mottagaren är leverantörer av kryptotillgångstjänster som agerar för egen räkning.
- b) Överföringen utgör en överföring av kryptotillgångar från person till person som utförs utan medverkan av en leverantör av kryptotillgångstjänster.

E-pengartoken enligt definitionen i artikel 3.1.7 i förordning (EU) 2023/1114 ska behandlas som kryptotillgångar enligt den här förordningen.

5. En medlemsstat kan besluta att inte tillämpa denna förordning på överföringar av medel inom dess territorium till en betalningsmottagares betalkonto som uteslutande möjliggör betalning för tillhandahållande av varor eller tjänster när samtliga följande villkor är uppfyllda:

- a) Betalningsmottagarens betaltjänstleverantör omfattas av direktiv (EU) 2015/849.
- b) Betalningsmottagarens betaltjänstleverantör har möjlighet att med hjälp av en unik transaktionsidentifierare via betalningsmottagaren spåra överföringar av medel från den person som har ingått ett avtal med betalningsmottagaren om tillhandahållande av varor eller tjänster.
- c) Överföringen av medel överskrider inte 1 000 EUR.

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

1. *finansiering av terrorism*: finansiering av terrorism i enlighet med definitionen i artikel 1.5 i direktiv (EU) 2015/849.
2. *penningtvätt*: penningtvätt i enlighet med artikel 1.3 och 1.4 i direktiv (EU) 2015/849.
3. *betalare*: en person som är betalkontoinnehavare och som godkänner en överföring av medel från detta betalkonto eller, om det inte finns något betalkonto, som lämnar en order om överföring av medel.
4. *betalningsmottagare*: en person som är den avsedda mottagaren av överföringen av medel.
5. *betaltjänstleverantör*: de kategorier av betaltjänstleverantörer som avses i artikel 1.1 i direktiv (EU) 2015/2366, fysiska eller juridiska personer som omfattas av ett undantag enligt artikel 32 i direktivet och juridiska personer som omfattas av ett undantag enligt artikel 9 i direktiv 2009/110/EG, vilka tillhandahåller överföringstjänster för medel.
6. *förmedlande betaltjänstleverantör*: en betaltjänstleverantör som inte är betalarens eller betalningsmottagarens betaltjänstleverantör och som tar emot och verkställer en överföring av medel på uppdrag av betalarens eller betalningsmottagarens betaltjänstleverantör eller en annan förmedlande betaltjänstleverantör.
7. *betalkonto*: ett betalkonto enligt definitionen i artikel 4.12 i direktiv (EU) 2015/2366.
8. *medel*: medel enligt definitionen i artikel 4.25 i direktiv (EU) 2015/2366.
9. *överföring av medel*: alla transaktioner som för en betalares räkning åtminstone delvis utförs på elektronisk väg genom en betaltjänstleverantör för att göra tillgångar tillgängliga för en betalningsmottagare genom en betaltjänstleverantör, oavsett om betalaren och betalningsmottagaren är en och samma person och oavsett om betalarens och betalningsmottagarens betaltjänstleverantör är en och samma person, inbegripet
 - a) en betalning enligt definitionen i artikel 4.24 i direktiv (EU) 2015/2366,
 - b) autogiro enligt definitionen i artikel 4.23 i direktiv (EU) 2015/2366,
 - c) en penningöverföring enligt definitionen i artikel 4.22 i direktiv (EU) 2015/2366, oavsett om den är nationell eller gränsöverskridande,

- d) en överföring som genomförts med ett betalkort, ett instrument för elektroniska pengar, en mobiltelefon eller någon annan förbetald eller efterhandsbetald digital utrustning eller it-utrustning med liknande egenskaper.
10. *överföring av kryptotillgångar*: alla transaktioner i syfte att flytta kryptotillgångar från en adress i den distribuerade liggaren, ett kryptotillgångskonto eller en annan utrustning som möjliggör lagringen av kryptotillgångar till annan sådan plats, som för antingen en avsändares eller en mottagares räkning utförs av minst en leverantör av kryptotillgångstjänster, oavsett om avsändaren och mottagaren är en och samma person och oavsett om avsändarens och mottagarens leverantör av kryptotillgångstjänster är en och samma person.
 11. *batchöverföring*: ett paket av flera enskilda överföringar av medel eller överföringar av kryptotillgångar som sammanförts för vidarebefordran.
 12. *unik transaktionsidentifierare*: en kombination av bokstäver, siffror eller symboler som betaltjänstleverantören fastställt i enlighet med protokollen för det betalnings- och avvecklingssystem eller meddelandesystem som används för överföringen av medel eller som fastställts av en leverantör av kryptotillgångstjänster, som gör det möjligt att spåra transaktionen tillbaka till betalaren och betalningsmottagaren eller att spåra överföringen av kryptotillgångar tillbaka till avsändaren och mottagaren.
 13. *överföring av kryptotillgångar från person till person*: en överföring av kryptotillgångar utan medverkan av någon leverantör av kryptotillgångstjänster.
 14. *kryptotillgång*: en kryptotillgång enligt definitionen i artikel 3.1.5 i förordning (EU) 2023/1114 utom när den ingår i de kategorier som förtecknas i artikel 2.2, 2.3 och 2.4 i den förordningen eller på annat sätt räknas som medel.
 15. *leverantör av kryptotillgångstjänster*: en leverantör av kryptotillgångstjänster enligt definitionen i artikel 3.1.15 i förordning (EU) 2023/1114, som utför en eller flera kryptotillgångstjänster enligt definitionen i artikel 3.1.16 i den förordningen.
 16. *förmedlande leverantör av kryptotillgångstjänster*: en leverantör av kryptotillgångstjänster som inte är avsändarens eller mottagarens leverantör av kryptotillgångstjänster och som tar emot och verkställer en överföring av kryptotillgångar på uppdrag av avsändarens eller mottagarens leverantör av kryptotillgångstjänster eller en annan förmedlande leverantör av kryptotillgångstjänster.
 17. *bankomater för kryptotillgångar eller kryptobankomater*: fysiska eller webbaserade elektroniska terminaler som gör det möjligt för en leverantör av kryptotillgångstjänster att i synnerhet utföra överföringstjänster för kryptotillgångar, i enlighet med artikel 3.1.16 j i förordning (EU) 2023/1114.
 18. *adress i distribuerad liggare*: en alfanumerisk kod som identifierar en adress på ett nätverk som använder teknik för distribuerade liggare (DLT) eller liknande teknik som kryptotillgångar kan sändas till eller tas emot från.
 19. *konto för kryptotillgångar*: ett konto som innehas av en leverantör av kryptotillgångstjänster för en eller flera fysiska eller juridiska personers räkning och som kan användas för att verkställa överföringar av kryptotillgångar.
 20. *fristående adress*: en adress för distribuerad liggare som inte är kopplad till något av följande:
 - a) en leverantör av kryptotillgångstjänster.
 - b) en enhet som inte är etablerad i unionen och som tillhandahåller tjänster liknande dem som tillhandahålls av en leverantör av kryptotillgångstjänster.

21. *avsändare*: en person som innehar ett konto för kryptotillgångar hos en leverantör av kryptotillgångstjänster, en adress i distribuerad liggare eller utrustning som möjliggör lagring av kryptotillgångar, och som tillåter en överföring av kryptotillgångar från det kontot, den adressen i en distribuerad liggare eller den utrustningen, eller, om det inte finns något sådant konto, någon adress i distribuerad liggare eller utrustning, en person som ger uppdrag om eller initierar en överföring av kryptotillgångar.
22. *mottagare*: en person som är den avsedda mottagaren av överföringen av kryptotillgångar.
23. *identifieringskod för juridiska personer eller LEI*: en unik alfanumerisk referenskod baserad på standarden ISO 17442 som tilldelats en juridisk person.
24. *teknik för distribuerade liggare eller DLT*: teknik för distribuerade liggare enligt definitionen i 3.1.1 i förordning (EU) 2023/1114.

KAPITEL II

Skyldigheter för betaltjänstleverantörer

Avsnitt 1

Skyldigheter för betalarens betaltjänstleverantör

Artikel 4

Uppgifter som ska åtfölja överföringar av medel

1. Betalarens betaltjänstleverantör ska se till att överföringar av medel åtföljs av följande uppgifter om betalaren:
 - a) Betalarens namn.
 - b) Betalarens betalkontonummer.
 - c) Betalarens adress, inbegripet landets namn, officiella personliga dokumentnummer, och kundnummer eller, alternativt, betalarens födelsedatum och födelseort.
 - d) Betalarens aktuella LEI-kod, under förutsättning att det nödvändiga fältet finns i det relevanta formatet för betalningsmeddelanden, och om betalaren tillhandahåller den koden till sin betaltjänstleverantör, eller, om sådan saknas, annan tillgänglig likvärdig officiell identifieringskod.
2. Betalarens betaltjänstleverantör ska se till att överföringar av medel åtföljs av följande uppgifter om betalningsmottagaren:
 - a) Betalningsmottagarens namn.
 - b) Betalningsmottagarens betalkontonummer.
 - c) Betalarens aktuella LEI-kod, förutsatt att det nödvändiga fältet finns i det relevanta formatet för betalningsmeddelanden, och om den uppges av betalaren till sin betaltjänstleverantör eller, om sådan saknas, annan tillgänglig likvärdig officiell identifieringskod.

3. Genom undantag från punkterna 1 b och 2 b, i fall där en överföring inte görs till eller från ett betalkonto, ska betalarens betaltjänstleverantör se till att överföringen av medel åtföljs av en unik transaktionsidentifierare i stället för betalkontonummer.

4. Innan betalarens betaltjänstleverantör överför medel ska denne kontrollera riktigheten i de uppgifter som avses i punkt 1, och om tillämpligt i punkt 3, på grundval av handlingar, uppgifter eller upplysningar från en tillförlitlig och oberoende källa.

5. Den kontroll som avses i punkt 4 i denna artikel ska anses ha ägt rum när något av följande tillämpas:

a) betalarens identitet har kontrollerats i enlighet med artikel 13 i direktiv (EU) 2015/849 och uppgifterna från kontrollen har lagrats i enlighet med artikel 40 i det direktivet,

b) betalaren omfattas av artikel 14.5 i direktiv (EU) 2015/849.

6. Utan att det påverkar de undantag som anges i artiklarna 5 och 6 ska betalarens betaltjänstleverantör inte verkställa en överföring av medel förrän kraven i den här artikeln har fullgjorts i sin helhet.

Artikel 5

Överföringar av medel inom unionen

1. Om alla betaltjänstleverantörer i betalningskedjan är etablerade inom unionen ska överföringar av medel, genom undantag från artikel 4.1 och 4.2, åtminstone åtföljas av både betalarens och betalningsmottagarens betalkontonummer eller, där artikel 4.3 är tillämplig, av den unika transaktionsidentifieraren, utan att detta i tillämpliga fall påverkar informationskraven i förordning (EU) nr 260/2012.

2. Utan hinder av punkt 1 ska betalarens betaltjänstleverantör, inom tre arbetsdagar efter att ha mottagit en begäran om information från betalningsmottagarens betaltjänstleverantör eller den förmedlande betaltjänstleverantören, lämna följande:

a) För överföringar av medel som överstiger 1 000 EUR, oavsett om sådana överföringar utförs i en enda transaktion eller i flera transaktioner som förefaller vara kopplade, de uppgifter om betalaren eller betalningsmottagaren som avses i artikel 4.

b) För överföringar av medel som uppgår till högst 1 000 EUR som inte förefaller vara sammankopplade till andra överföringar av medel som tillsammans med överföringen i fråga överstiger 1 000 EUR, åtminstone

i) betalarens och betalningsmottagarens namn, och

ii) betalarens och betalningsmottagarens betalkontonummer eller, där artikel 4.3 är tillämplig, den unika transaktionsidentifieraren.

3. Genom undantag från artikel 4.4 ska betalarens betaltjänstleverantör, vid överföringar av medel som avses i punkt 2 b i den här artikeln, inte vara skyldig att kontrollera uppgifterna om betalaren, såvida inte betalarens betaltjänstleverantör

a) har tagit emot de medel som ska överföras i kontanter eller i anonyma elektroniska pengar, eller

b) har rimliga skäl att misstänka penningtvätt eller finansiering av terrorism.

Artikel 6

Överföringar av medel från unionen till utanför unionen

1. Vid en batchöverföring från en enskild betalare där betalningsmottagarnas betaltjänstleverantörer är etablerade utanför unionen ska artikel 4.1 inte tillämpas på enskilda överföringar som sammanförts i batchöverföringen, under förutsättning att batchfilen innehåller de uppgifter som avses i artikel 4.1, 4.2 och 4.3 och att dessa uppgifter har kontrollerats i enlighet med artikel 4.4 och 4.5, och att de enskilda överföringarna åtföljs av betalarens betalkontonummer eller, där artikel 4.3 är tillämplig, den unika transaktionsidentifieraren.

2. Genom undantag från artikel 4.1 och, i tillämpliga fall, utan att det påverkar de uppgifter som krävs enligt förordning (EU) nr 260/2012, ska, om betalningsmottagarens betaltjänstleverantör är etablerad utanför unionen, överföringar av medel som inte överstiger 1 000 EUR och som inte förefaller vara sammankopplade till andra överföringar av medel som tillsammans med överföringen i fråga överstiger 1 000 EUR, åtföljas av åtminstone

- a) betalarens och betalningsmottagarens namn, och
- b) betalarens och betalningsmottagarens betalkontonummer eller, där artikel 4.3 är tillämplig, den unika transaktionsidentifieraren.

Genom undantag från artikel 4.4 ska betalarens betaltjänstleverantör inte vara skyldig att kontrollera de uppgifter om betalaren som avses i denna punkt, såvida inte betalarens betaltjänstleverantör

- a) har tagit emot de medel som ska överföras i kontanter eller i anonyma elektroniska pengar, eller
- b) har rimliga skäl att misstänka penningtvätt eller finansiering av terrorism.

Avsnitt 2

Skyldigheter för betalarens betaltjänstleverantör

Artikel 7

Upptäckt av saknade uppgifter om betalaren eller betalningsmottagaren

1. Betalningsmottagarens betaltjänstleverantör ska införa effektiva förfaranden för fastställande av huruvida fälten för uppgifter om betalaren och betalningsmottagaren inom det meddelande- eller betalnings- och avvecklingssystem som används för att verkställa överföringen av medel har fyllts i med hjälp av de vedertagna tecken eller inmatningsdata som är tillåtna i enlighet med det systemet.

2. Betalningsmottagarens betaltjänstleverantör ska införa effektiva förfaranden, inbegripet, om så är lämpligt, övervakning efter eller samtidigt med överföringarna, för fastställande av huruvida följande uppgifter om betalaren eller betalningsmottagaren saknas:

- a) Vid överföringar av medel där betalarens betaltjänstleverantör är etablerad inom unionen: de uppgifter som avses i artikel 5.
- b) Vid överföringar av medel där betalarens betaltjänstleverantör är etablerad utanför unionen: de uppgifter som avses i artikel 4.1 a, b och c, och 4.2 a och b.
- c) Vid batchöverföringar där betalarens betaltjänstleverantör är etablerad utanför unionen: de uppgifter som avses i artikel 4.1 a, b och c, och 4.2 a och b med avseende på den batchöverföringen.

3. Vid överföringar av medel som överstiger 1 000 EUR, oavsett om dessa överföringar utförs i en enda transaktion eller flera transaktioner som förefaller vara sammankopplade, ska betalningsmottagarens betaltjänstleverantör, innan denne krediterar betalningsmottagarens betalkonto eller gör medlen tillgängliga för betalningsmottagaren, kontrollera att de uppgifter om betalningsmottagaren som avses i punkt 2 i den här artikeln är riktiga, på grundval av handlingar, uppgifter eller upplysningar från en tillförlitlig och oberoende källa, utan att detta påverkar kraven i artiklarna 83 och 84 i direktiv (EU) 2015/2366.

4. Vid överföringar av medel som uppgår till högst 1 000 EUR och som inte förefaller vara sammankopplade till andra överföringar av medel som tillsammans med överföringen i fråga överstiger 1 000 EUR, ska betalningsmottagarens betaltjänstleverantör inte vara skyldig att kontrollera riktigheten i uppgifterna om betalningsmottagaren, såvida inte betalningsmottagarens betaltjänstleverantör

a) utbetalar medlen i kontanter eller i anonyma elektroniska pengar, eller

b) har rimliga skäl att misstänka penningtvätt eller finansiering av terrorism.

5. Den kontroll som avses i punkterna 3 och 4 i denna artikel ska anses ha ägt rum när något av följande tillämpas:

a) betalarens identitet har kontrollerats i enlighet med artikel 13 i direktiv (EU) 2015/849 och uppgifterna från kontrollen har lagrats i enlighet med artikel 40 i det direktivet,

b) betalaren omfattas av artikel 14.5 i direktiv (EU) 2015/849.

Artikel 8

Överföringar av medel där uppgifter om betalaren eller betalningsmottagaren saknas eller är ofullständig

1. Betalningsmottagarens betaltjänstleverantör ska genomföra effektiva riskbaserade förfaranden, bland annat förfaranden som grundar sig på den riskbedömning som avses i artikel 13 i direktiv (EU) 2015/849 för att avgöra om en överföring av medel som saknar erforderliga fullständiga uppgifter om betalaren och betalningsmottagaren ska verkställas, avvisas eller avbrytas samt för vidtagandet av lämpliga uppföljningsåtgärder.

Om betalningsmottagarens betaltjänstleverantör vid mottagandet av en överföring av medel får kännedom om att de uppgifter som avses i artikel 4.1 a, b och c, artikel 4.2 a och b, artikel 5.1 eller artikel 6 saknas eller är ofullständiga eller inte har fyllts i med hjälp av de vedertagna tecken eller inmatningsdata som är tillåtna enligt det meddelandesystem eller betalnings- och avvecklingssystem som avses i artikel 7.1, ska betalningsmottagarens betaltjänstleverantör på grundval av en riskbedömning

a) avvisa överföringen eller

b) begära de uppgifter som krävs om betalaren och betalningsmottagaren före eller efter krediteringen av betalningsmottagarens betalkonto eller tillgängliggörandet av tillgångar för betalningsmottagaren.

2. Om en betaltjänstleverantör upprepade gånger underlåter att tillhandahålla de erforderliga uppgifterna om en betalare eller en betalningsmottagare ska betalningsmottagarens betaltjänstleverantör

a) vidta åtgärder, som inledningsvis kan bestå i att utfärda varningar och fastställa tidsfrister, innan ett avvisande, en begränsning eller ett avslutande inleds i enlighet med led b om de erforderliga uppgifterna ännu inte tillhandahålls, eller

b) direkt avvisa alla framtida överföringar av medel från den betaltjänstleverantören eller begränsa eller avsluta sin affärsrelation med den betaltjänstleverantören.

Betalningsmottagarens betaltjänstleverantör ska meddela den underlåtenheten och de åtgärder som vidtagits till den behöriga myndighet som ansvarar för att övervaka efterlevnaden av bestämmelser som rör bekämpning av penningtvätt och finansiering av terrorism.

Artikel 9

Bedömning och rapportering

Betalningsmottagarens betaltjänstleverantör ska beakta saknade eller ofullständiga uppgifter om betalaren eller betalningsmottagaren som en faktor när den bedömer om överföringen av medel, eller därmed relaterade transaktioner, är misstänkt och om den ska rapporteras till finansunderrättelseenheten (FIU) i enlighet med direktiv (EU) 2015/849.

Avsnitt 3

Skyldigheter för förmedlande betaltjänstleverantörer

Artikel 10

Lagring av uppgifter om betalaren och betalningsmottagaren som åtföljer överföringen

Förmedlande betaltjänstleverantörer ska se till att alla mottagna uppgifter om betalaren och betalningsmottagaren som åtföljer en överföring av medel lagras med överföringen.

Artikel 11

Upptäckt av saknade uppgifter om betalaren eller betalningsmottagaren

1. Den förmedlande betaltjänstleverantören ska införa effektiva förfaranden för att fastställa om fälten för uppgifter om betalaren och betalningsmottagaren inom det meddelande- eller betalnings- och avvecklingssystem som används för att verkställa överföringen av medel har fyllts i med hjälp av de vedertagna tecken eller inmatningsdata som är tillåtna enligt detta system.
2. Den förmedlande betaltjänstleverantören ska införa effektiva förfaranden, inbegripet, om så är lämpligt, övervakning efter eller samtidigt med överföringarna, för fastställande av huruvida följande uppgifter om betalaren eller betalningsmottagaren saknas:
 - a) Vid överföringar av medel där betalarens och betalningsmottagarens betaltjänstleverantörer är etablerade inom unionen: de uppgifter som avses i artikel 5.
 - b) Vid överföringar av medel där betalarens eller betalningsmottagarens betaltjänstleverantör är etablerad utanför unionen: de uppgifter som avses i artikel 4.1 a, b och c och 4.2 a och b.
 - c) Vid batchöverföringar där betalarens betaltjänstleverantör är etablerad utanför unionen: de uppgifter som avses i artikel 4.1 a, b och c, och artikel 4.2 a och b, med avseende på den batchöverföringen.

Artikel 12

Överföringar av medel där uppgifter om betalaren eller betalningsmottagaren saknas

1. Den förmedlande betaltjänstleverantören ska inrätta effektiva riskbaserade förfaranden för att avgöra om en överföring av medel som saknar erforderliga uppgifter om betalaren och betalningsmottagaren ska verkställas, avvisas eller avbrytas samt för att vidta lämpliga uppföljningsåtgärder.

Om den förmedlande betaltjänstleverantören vid mottagandet av en överföring av medel får kännedom om att de uppgifter som avses i artikel 4.1 a, b och c, artikel 4.2 a och b, artikel 5.1 eller artikel 6 saknas eller är ofullständiga eller inte har fyllts i med hjälp av de vedertagna tecken eller inmatningsdata som är tillåtna enligt det meddelandesystem eller betalnings- och avvecklingssystem som avses i artikel 7.1, ska den förmedlande betaltjänstleverantören på grundval av en riskbedömning.

- a) avvisa överföringen, eller
- b) begära de uppgifter som krävs om betalaren och betalningsmottagaren före eller efter det att överföringen av medel gjorts.

2. Om en betaltjänstleverantör upprepade gånger underlåter att tillhandahålla erforderliga uppgifter om betalaren eller betalningsmottagaren ska den förmedlande betaltjänstleverantören

- a) vidta åtgärder som inledningsvis kan bestå i att utfärda varningar och fastställa tidsfrister, innan ett avvisande, en begränsning eller ett avslutande inleds i enlighet med led b om de erforderliga uppgifterna ännu inte tillhandahålls, eller
- b) direkt avvisa alla framtida överföringar av medel från den betaltjänstleverantören eller begränsa eller avsluta sin affärsrelation med den betaltjänstleverantören.

Den förmedlande betaltjänstleverantören ska meddela den underlåtenheten och de åtgärder som vidtagits till den behöriga myndighet som ansvarar för att övervaka efterlevnaden av bestämmelser som rör bekämpning av penningtvätt och finansiering av terrorism.

Artikel 13

Bedömning och rapportering

Den förmedlande betaltjänstleverantören ska beakta saknade uppgifter om betalaren eller betalningsmottagaren som en faktor när den bedömer om en överföring av medel, eller därmed relaterade transaktioner, är misstänkt och om den ska rapporteras till FIU i enlighet med direktiv (EU) 2015/849.

KAPITEL III

Skyldigheter för leverantörer av kryptotillgångstjänster

Avsnitt 1

Skyldigheter för avsändarens leverantör av kryptotillgångstjänster

Artikel 14

Uppgifter som ska åtfölja överföringar av kryptotillgångar

1. Avsändarens leverantör av kryptotillgångstjänster ska se till att överföringar av kryptotillgångar åtföljs av följande uppgifter om avsändaren:
 - a) Avsändarens namn.
 - b) Avsändarens adress i den distribuerade liggaren, i de fall där en överföring av kryptotillgångar registreras på ett nätverk som använder DLT eller liknande teknik, och avsändarens kontonummer för kryptotillgångar om ett sådant konto finns och används för transaktionen.
 - c) Avsändarens kontonummer för kryptotillgångar i de fall där en överföring av kryptotillgångar inte registreras på ett nätverk som använder DLT eller liknande teknik.
 - d) Avsändarens adress, inbegripet landets namn, officiella personliga dokumentnummer, kundnummer eller, alternativt, avsändarens födelsedatum och födelseort.
 - e) Avsändarens aktuella LEI-kod, under förutsättning att det nödvändiga fältet finns i det relevanta meddelandeformatet, och om avsändaren tillhandahåller sin leverantör av kryptotillgångstjänster den koden, eller, om en sådan saknas, annan tillgänglig likvärdig officiell identifieringskod för avsändaren.

2. Avsändarens leverantör av kryptotillgångstjänster ska se till att överföringar av kryptotillgångar åtföljs av följande uppgifter om mottagaren:

- a) Mottagarens namn.
- b) Mottagarens adress i den distribuerade liggaren, i de fall där en överföring av kryptotillgångar registreras på ett nätverk som använder DLT eller liknande teknik, och mottagarens kontonummer för kryptotillgångar om ett sådant konto finns och används för transaktionen.
- c) Mottagarens kontonummer för kryptotillgångar i de fall där en överföring av kryptotillgångar inte registreras på ett nätverk som använder DLT eller liknande teknik.
- d) Den aktuella LEI-koden, under förutsättning att det nödvändiga fältet finns i det relevanta meddelandeformatet, och om avsändaren tillhandahåller sin leverantör av kryptotillgångstjänster den koden, eller, om en sådan saknas, annan tillgänglig likvärdig officiell identifieringskod för mottagaren.

3. Genom undantag från punkterna 1 c och 2 c, i fall där en överföring av kryptotillgångar inte registrerats på ett nätverk som använder DLT eller liknande teknik och inte görs till eller från ett konto för kryptotillgångar, ska avsändarens leverantör av kryptotillgångstjänster säkerställa att överföringen av kryptotillgångar åtföljs av en unik transaktionsidentifierare.

4. De uppgifter som avses i punkterna 1 och 2 ska lämnas på ett säkert sätt, och i enlighet med förordning (EU) 2016/679, före, samtidigt som eller i samband med överföringen av kryptotillgångar.

De uppgifter som avses i punkterna 1 och 2 får inte krävas direkt medfölja, eller ingå i, överföringen av kryptotillgångar.

5. Vid överföring av kryptotillgångar till en fristående adress ska avsändarens leverantör av kryptotillgångstjänster inhämta och bevara de uppgifter som avses i punkterna 1 och 2 och ska säkerställa att överföringen av kryptotillgångar kan identifieras individuellt.

Utan att det påverkar särskilda riskreducerande åtgärder som vidtagits i enlighet med artikel 19b i direktiv (EU) 2015/849 ska, vid en överföring av ett belopp som överstiger 1 000 EUR till en fristående adress, avsändarens leverantör av kryptotillgångstjänster vidta lämpliga åtgärder för att bedöma om huruvida den adressen ägs eller kontrolleras av avsändaren.

6. Innan avsändarens leverantör av kryptotillgångstjänster överför kryptotillgångarna ska denne kontrollera riktigheten i de uppgifter som avses i punkt 1, på grundval av handlingar, uppgifter eller upplysningar från en tillförlitlig och oberoende källa.

7. Den kontroll som avses i punkt 6 i denna artikel ska anses ha ägt rum när något av följande tillämpas:

- a) avsändarens identitet har kontrollerats i enlighet med artikel 13 i direktiv (EU) 2015/849 och uppgifterna från kontrollen har lagrats i enlighet med artikel 40 i det direktivet,
- b) avsändaren omfattas av artikel 14.5 i direktiv (EU) 2015/849.

8. Avsändarens leverantör av kryptotillgångstjänster ska inte möjliggöra initiering av eller verkställa någon överföring av kryptotillgångar förrän kraven i den här artikeln har fullgjorts i sin helhet.

Artikel 15

Batchöverföringar av kryptotillgångar

Vid en batchöverföring av kryptotillgångar från en enskild avsändare ska artikel 14.1 inte tillämpas på enskilda överföringar som sammanförts i batchöverföringen, under förutsättning att batchfilen innehåller de uppgifter som avses i artikel 14.1, 14.2 och 14.3, att dessa uppgifter har kontrollerats i enlighet med artikel 14.6 och 14.7, och att de enskilda överföringarna åtföljs av avsändarens adress i den distribuerade liggaren, om artikel 14.2 b är tillämplig, avsändarens kontonummer för kryptotillgångar, om artikel 14.2 c är tillämplig, eller den unika transaktionsidentifieraren, om artikel 14.3 är tillämplig.

Avsnitt 2

Skyldigheter för mottagarens leverantör av kryptotillgångstjänster

Artikel 16

Upptäckt av saknade uppgifter om avsändaren eller mottagaren

1. Mottagarens leverantör av kryptotillgångstjänster ska införa effektiva förfaranden, inbegripet, när så är lämpligt, övervakning efter eller samtidigt med överföringarna, för att upptäcka om de uppgifter som avses i artikel 14.1 och 14.2 om avsändaren och mottagaren ingår i, eller följer, överföringen eller batchöverföringen av kryptotillgångar.

2. Vid en överföring av kryptotillgångar som genomförs från en fristående adress ska mottagarens leverantör av kryptotillgångstjänster inhämta och bevara de uppgifter som avses i artikel 14.1 och 14.2 och ska säkerställa att överföringen av kryptotillgångar kan identifieras individuellt.

Utan att det påverkar särskilda riskreducerande åtgärder som vidtagits i enlighet med artikel 19b i direktiv (EU) 2015/849 ska, vid en överföring av ett belopp som överstiger 1 000 EUR från en fristående adress, mottagarens leverantör av kryptotillgångstjänster vidta lämpliga åtgärder för att bedöma om huruvida den adressen ägs eller kontrolleras av mottagaren.

3. Innan avsändarens leverantör av kryptotillgångstjänster överför kryptotillgångarna till mottagaren ska den kontrollera riktigheten i de uppgifter om mottagaren som avses i artikel 14.2, på grundval av handlingar, uppgifter eller upplysningar från en tillförlitlig och oberoende källa.

4. Den kontroll som avses i punkterna 2 och 3 i denna artikel ska anses ha ägt rum när något av följande gäller:

a) mottagarens identitet har kontrollerats i enlighet med artikel 13 i direktiv (EU) 2015/849 och uppgifterna från kontrollen har lagrats i enlighet med artikel 40 i det direktivet,

b) mottagaren omfattas av artikel 14.5 i direktiv (EU) 2015/849.

Artikel 17

Överföringar av kryptotillgångar där uppgifter om avsändaren eller mottagaren saknas eller är ofullständiga

1. Mottagarens leverantör av kryptotillgångstjänster ska genomföra effektiva riskbaserade förfaranden, bland annat förfaranden som grundar sig på den riskbedömning som avses i artikel 13 i direktiv (EU) 2015/849 för att avgöra om en överföring av kryptotillgångar som saknar erforderliga fullständiga uppgifter om avsändaren och mottagaren ska verkställas, avvisas, återsändas eller avbrytas samt för vidtagandet av lämpliga uppföljningsåtgärder.

Om mottagarens leverantör av kryptotillgångstjänster får kännedom om att de uppgifter som avses i artikel 14.1 eller 14.2 eller artikel 15 saknas eller är ofullständiga, ska den leverantören av kryptotillgångstjänster på grundval av en riskbedömning och utan onödigt dröjsmål,

- a) avvisa överföringen eller återsända de överförda kryptotillgångarna till avsändarens kryptotillgångskonto eller
- b) begära erforderliga uppgifter om avsändaren och mottagaren före det att kryptotillgångarna görs tillgängliga för mottagaren.

2. Om en leverantör av kryptotillgångstjänster upprepade gånger underlåter att tillhandahålla de erforderliga uppgifterna om avsändaren eller mottagaren, ska mottagarens leverantör av kryptotillgångstjänster

- a) vidta åtgärder som inledningsvis kan bestå i att utfärda varningar och fastställa tidsfrister, i innan ett avvisande, en begränsning eller ett avslutande inleds i enlighet med led b om de erforderliga uppgifterna ännu inte tillhandahålls, eller
- b) direkt avvisa alla framtida överföringar av kryptotillgångar till eller från, eller begränsa eller avsluta affärsförbindelserna med, den leverantören av kryptotillgångstjänster.

Mottagarens leverantör av kryptotillgångstjänster ska meddela den underlåtenheten och de åtgärder som vidtagits till den behöriga myndighet som ansvarar för att övervaka efterlevnaden av bestämmelser som rör bekämpning av penningtvätt och finansiering av terrorism.

Artikel 18

Bedömning och rapportering

Mottagarens leverantör av kryptotillgångstjänster ska beakta saknade eller ofullständiga uppgifter om avsändaren eller mottagaren som en faktor när den bedömer om en överföring av kryptotillgångar, eller någon därmed relaterad transaktion, är mistänkt och om den ska rapporteras till FIU i enlighet med direktiv (EU) 2015/849.

Avsnitt 3

Skyldigheter för förmedlande leverantörer av kryptotillgångstjänster

Artikel 19

Lagring av uppgifter om avsändaren och mottagaren som åtföljer överföringen

Förmedlande leverantörer av kryptotillgångstjänster ska säkerställa att alla mottagna uppgifter om avsändaren och mottagaren som åtföljer en överföring av kryptotillgångar översänds i samband med överföringen och att förteckningen över sådana uppgifter lagras och på begäran görs tillgänglig för de behöriga myndigheterna.

Artikel 20

Upptäckt av saknade uppgifter om avsändaren eller mottagaren

Den förmedlande leverantören av kryptotillgångstjänster ska införa effektiva förfaranden, inbegripet, när så är lämpligt, övervakning efter eller i samband med överföringarna, för att upptäcka om de uppgifter om avsändaren eller mottagaren som avses i artikel 14.1 a, b och c och artikel 14.2 a, b och c har lämnats före, samtidigt eller i samband med överföringen eller batchöverföringen av kryptotillgångar, inbegripet om överföringen görs till eller från en fristående adress.

Artikel 21

Överföringar av kryptotillgångar där uppgifter om avsändaren eller mottagaren saknas

1. Den förmedlande leverantören av kryptotillgångstjänster ska fastställa effektiva riskbaserade förfaranden, bland annat förfaranden som grundar sig på den riskbedömning som avses i artikel 13 i direktiv (EU) 2015/849 för att avgöra om en överföring av kryptotillgångar som saknar erforderliga uppgifter om avsändaren och mottagaren ska verkställas, avvisas, återsändas eller avbrytas samt för vidtagandet av lämpliga uppföljningsåtgärder.

Om den förmedlande leverantören av kryptotillgångstjänster vid mottagande av en överföring av kryptotillgångar får kännedom om att de uppgifter som avses i artikel 14.1 a, b och c och artikel 14.2 a, b och c eller artikel 15.1 saknas eller är ofullständiga, ska den förmedlande leverantören av kryptotillgångstjänster, på grundval av en riskbedömning och utan onödigt dröjsmål,

- a) avvisa överföringen eller återsända de överförda kryptotillgångarna eller
- b) begära erforderliga uppgifter om avsändaren och mottagaren före det att överföringen av kryptotillgångarna utförs.

2. Om leverantören av kryptotillgångstjänster upprepade gånger underlåter att tillhandahålla de erforderliga uppgifterna om avsändaren eller mottagaren, ska den förmedlande leverantören av kryptotillgångstjänster

- a) vidta åtgärder som inledningsvis kan bestå i att utfärda varningar och fastställa tidsfrister, innan ett avvisande, en begränsning eller ett avslutande inleds i enlighet med led b om de erforderliga uppgifterna ännu inte tillhandahålls, eller
- b) direkt avvisa alla framtida överföringar av kryptotillgångar till eller från, eller begränsa eller avsluta affärsförbindelserna med, den leverantören av kryptotillgångstjänster.

Den förmedlande leverantören av kryptotillgångstjänster ska meddela den underlåtenheten och de åtgärder som vidtagits till den behöriga myndighet som ansvarar för att övervaka efterlevnaden av bestämmelser som rör bekämpning av penningtvätt och finansiering av terrorism.

Artikel 22

Bedömning och rapportering

Den förmedlande leverantören av kryptotillgångstjänster ska beakta saknade uppgifter om avsändaren eller mottagaren som en faktor när den bedömer om en överföring av kryptotillgångar, eller därmed relaterade transaktioner, är misstänkt och om den ska rapporteras till FIU i enlighet med direktiv (EU) 2015/849.

KAPITEL IV

Gemensamma åtgärder som ska tillämpas av betaltjänstleverantörer och leverantörer av kryptotillgångstjänster

Artikel 23

Interna strategier, förfaranden och kontroller för att säkerställa genomförandet av restriktiva åtgärder

Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster ska ha infört interna strategier, förfaranden och kontroller för att säkerställa genomförandet av unionens restriktiva åtgärder och nationella restriktiva åtgärder vid överföringar av medel och kryptotillgångar enligt denna förordning.

Europeiska bankmyndigheten (EBA) ska senast den 30 december 2024 utfärda riktlinjer som specificerar de åtgärder som avses i denna artikel.

KAPITEL V

Uppgifter, uppgiftsskydd och lagring

Artikel 24

Tillhandahållande av information

Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster ska till fullo och utan dröjsmål, inbegripet genom en central kontaktpunkt i enlighet med artikel 45.9 i direktiv (EU) 2015/849, om en sådan kontaktpunkt har inrättats, och i enlighet med formella krav som anges i nationell rätt i den medlemsstat där de är etablerade eller har sitt säte, beroende på vad som är tillämpligt, besvara förfrågningar angående de uppgifter som krävs enligt denna förordning uteslutande från de myndigheter som ansvarar för bekämpning av penningtvätt eller finansiering av terrorism i den medlemsstaten.

Artikel 25

Dataskydd

1. Behandling av personuppgifter enligt denna förordning omfattas av förordning (EU) 2016/679. Personuppgifter som behandlas enligt den här förordningen av kommissionen eller av EBA omfattas av förordning (EU) 2018/1725.

2. Personuppgifter ska behandlas av betaltjänstleverantörer och leverantörer av kryptotillgångstjänster på grundval av denna förordning endast i syfte att förebygga penningtvätt och finansiering av terrorism och får inte senare behandlas på ett sätt som är oförenligt med dessa syften. Behandling av personuppgifter på grundval av denna förordning för kommersiella ändamål ska vara förbjuden.

3. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster ska tillhandahålla nya kunder den information som krävs enligt artikel 13 i förordning (EU) 2016/679 innan en affärsrelation ingås eller en enstaka transaktion genomförs. Den informationen ska tillhandahållas i en koncis, klar och tydlig, begriplig och lätt tillgänglig form i enlighet med artikel 12 i förordning (EU) 2016/679, och ska särskilt innehålla allmän information om betaltjänstleverantörernas och leverantörernas av kryptotillgångstjänsternas rättsliga förpliktelser enligt den här förordningen när personuppgifter behandlas i syfte att förebygga penningtvätt och finansiering av terrorism.

4. Betaltjänstleverantörerna och leverantörerna av kryptotillgångstjänster ska alltid säkerställa att alla personuppgifter om de medverkande parterna i en överföring av medel eller en överföring av kryptotillgångar översänds i enlighet med förordning (EU) 2016/679.

Europeiska dataskyddsstyrelsen ska, efter samråd med EBA, utfärda riktlinjer för det praktiska genomförandet av dataskyddskrav för överföring av personuppgifter till tredjeländer i samband med överföringar av kryptotillgångar. EBA ska utfärda riktlinjer om lämpliga förfaranden för att avgöra om en överföring av kryptotillgångar ska verkställas, avvisas, återsändas eller avbrytas i situationer då överensstämmelse med dataskyddskraven för överföring av personuppgifter till tredjeländer inte kan säkerställas.

Artikel 26

Lagring av uppgifter

1. Uppgifter om betalaren och betalningsmottagaren eller avsändaren och mottagaren, ska inte lagras längre än vad som är absolut nödvändigt. Betalarens och betalningsmottagarens betaltjänstleverantörer ska lagra de uppgifter som avses i artiklarna 4–7, och avsändarens och mottagarens leverantörer av kryptotillgångstjänster ska lagra de uppgifter som avses i artiklarna 14–16, under en period på fem år.

2. Vid utgången av den lagringsperiod som avses i punkt 1 ska betaltjänstleverantörer och leverantörer av kryptotillgångstjänster säkerställa att personuppgifterna raderas, om inte annat föreskrivs i nationell rätt som avgör under vilka omständigheter betaltjänstleverantörer och leverantörer av kryptotillgångstjänster får eller ska fortsätta att lagra sådana uppgifter. Medlemsstaterna får endast tillåta eller kräva ytterligare lagringstid efter att de har genomfört en grundlig bedömning av nödvändigheten och proportionaliteten av en sådan fortsatt lagring och om de anser att det är nödvändigt för att förebygga, upptäcka eller utreda penningtvätt eller finansiering av terrorism. Den ytterligare lagringstiden får inte vara längre än fem år.

3. Om det den 25 juni 2015 pågår rättsliga förfaranden som rör förebyggande, upptäckt, utredning eller lagföring av misstänkt penningtvätt eller finansiering av terrorism i en medlemsstat, och en betaltjänstleverantör innehar uppgifter eller handlingar som rör dessa pågående förfaranden, får betaltjänstleverantören lagra dessa uppgifter eller handlingar i enlighet med nationell rätt i fem år från och med den 25 juni 2015. Medlemsstaterna får, utan att det påverkar nationell straffrätt om bevis som är tillämpliga på pågående brottsutredningar och rättsliga förfaranden, tillåta eller kräva att sådana uppgifter eller handlingar lagras i ytterligare fem år, om det har fastställts att en sådan ytterligare lagringstid är nödvändig och proportionerlig för att förebygga, upptäcka, utreda eller lagföra misstänkt penningtvätt eller finansiering av terrorism.

Artikel 27

Samarbete med behöriga myndigheter

Informationsutbytet mellan behöriga myndigheter och med relevanta myndigheter i tredjeländer enligt denna förordning ska omfattas av direktiv (EU) 2015/849.

KAPITEL VI

Sanktioner och övervakning

Artikel 28

Administrativa sanktioner och åtgärder

1. Medlemsstaterna ska, utan att det påverkar rätten att föreskriva och påföra straffrättsliga påföljder, fastställa regler för administrativa sanktioner och åtgärder vid överträdelser av bestämmelserna i denna förordning och vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna och åtgärderna ska vara effektiva, proportionella och avskräckande och ska vara förenliga med dem som fastställs i enlighet med kapitel VI avsnitt 4 i direktiv (EU) 2015/849.

Medlemsstaterna får besluta att inte fastställa regler för administrativa sanktioner eller åtgärder vid överträdelser av de bestämmelser i denna förordning som omfattas av straffrättsliga påföljder i deras nationella rätt. I det fallet ska medlemsstaterna informera kommissionen om de relevanta straffrättsliga bestämmelserna.

2. Då betaltjänstleverantörer och leverantörer av kryptotillgångstjänster omfattas av skyldigheter ska medlemsstaterna, vid överträdelse av bestämmelserna i denna förordning och om ingenting annat föreskrivs i nationell rätt, se till att sanktioner eller åtgärder kan tillämpas på ledamöterna i styrelsen för den relevanta tjänstleverantören och på alla andra fysiska personer som enligt nationell rätt bär ansvar för överträdelsen.

3. Medlemsstaterna ska anmäla de regler som avses i punkt 1 till kommissionen och till den permanenta interna kommitté för bekämpning av penningtvätt och finansiering av terrorism som avses i artikel 9a.7 i förordning (EU) nr 1093/2010. Medlemsstaterna ska utan onödigt dröjsmål anmäla till kommissionen och den permanenta interna kommittén alla eventuella senare ändringar av dem.

4. I enlighet med artikel 58.4 i direktiv (EU) 2015/849 ska de behöriga myndigheterna ges lämpliga resurser och alla de tillsyns- och undersökningsbefogenheter som de behöver för att utföra sina uppgifter. När de behöriga myndigheterna utövar sina befogenheter att påföra administrativa sanktioner och åtgärder ska de i nära samarbete se till att dessa administrativa sanktioner eller åtgärder får önskad effekt och samordna sina åtgärder när de hanterar gränsöverskridande fall.

5. Medlemsstaterna ska se till att juridiska personer kan ställas till ansvar för de överträdelser som avses i artikel 29 och som begås till förmån för dem av en person som agerar antingen enskilt eller som en del av den juridiska personens organisation och har en ledande ställning inom den juridiska personen, på grundval av någon av följande befogenheter:

- a) Befogenhet att företräda den juridiska personen.
- b) Befogenhet att fatta beslut på den juridiska personens vägnar,
- c) Befogenhet att utöva kontroll inom den juridiska personen.

6. Medlemsstaterna ska också se till att juridiska personer kan ställas till ansvar när brister i den övervakning eller kontroll som utförs av en person som avses i punkt 5 i denna artikel har gjort det möjligt att begå någon av de överträdelser som avses i artikel 29 till förmån för den juridiska personen av en person under dess ledning.

7. De behöriga myndigheterna ska utöva sina befogenheter att påföra administrativa sanktioner och åtgärder i enlighet med denna förordning på något av följande sätt:

- a) Direkt.
- b) I samarbete med andra myndigheter.
- c) På eget ansvar genom delegering till sådana andra myndigheter.
- d) Genom hänvändelse till de behöriga rättsliga myndigheterna.

När de behöriga myndigheterna utövar sina befogenheter att påföra administrativa sanktioner och åtgärder, ska de göra detta i ett nära samarbete för att säkerställa att dessa administrativa sanktioner eller åtgärder får önskad effekt och samordna sina åtgärder när de hanterar gränsöverskridande fall.

Artikel 29

Särskilda bestämmelser

Medlemsstaterna ska säkerställa att deras administrativa sanktioner och åtgärder åtminstone omfattar de som fastställs i artikel 59.2 och 59.3 i direktiv (EU) 2015/849 vid följande överträdelser av denna förordning:

- a) Upprepad eller systematisk underlåtenhet från en betaltjänstleverantörs sida att låta överföringen av medel åtföljas av erforderliga uppgifter om betalare eller betalningsmottagare, i strid med artikel 4, 5 eller 6, eller från en leverantör av kryptotillgångstjänsters sida att låta överföringen av kryptotillgångar åtföljas av erforderliga uppgifter om avsändare och mottagare i strid med artiklarna 14 eller 15.
- b) Upprepad, systematisk eller allvarlig underlåtenhet från en betaltjänstleverantörs eller leverantör av kryptotillgångstjänsters sida att lagra uppgifter i strid med artikel 26.
- c) Underlåtenhet från en betaltjänstleverantörs sida att genomföra effektiva riskbaserade förfaranden, i strid med artikel 8 eller 12, eller från en leverantör av kryptotillgångstjänsters sida att införa effektiva riskbaserade förfaranden i strid med artikel 17.
- d) Allvarligt åsidosättande av artikel 11 eller 12 från en förmedlande betaltjänstleverantörs sida eller av artikel 19, 20 eller 21 från en förmedlande leverantör av kryptotillgångstjänster.

Artikel 30

Offentliggörande av sanktioner och åtgärder

I enlighet med artikel 60.1, 60.2 och 60.3 i direktiv (EU) 2015/849 ska de behöriga myndigheterna offentliggöra administrativa sanktioner och åtgärder som påförts i de fall som avses i artiklarna 28 och 29 i denna förordning utan onödigt dröjsmål, inklusive uppgifter om överträdelsens art och slag samt identiteten på de personer som är ansvariga för överträdelsen, om nödvändigt och proportionellt efter en bedömning i det enskilda fallet.

Artikel 31

Behöriga myndigheters tillämpning av sanktioner och åtgärder

1. När de behöriga myndigheterna ska fastställa vilken typ av administrativa sanktioner eller åtgärder som ska tillämpas, och storleken på sanktionsavgifterna, ska de beakta alla relevanta omständigheter, inklusive dem som förtecknas i artikel 60.4 i direktiv (EU) 2015/849.
2. Artikel 62 i direktiv (EU) 2015/849 ska tillämpas vad gäller administrativa sanktioner och åtgärder.

Artikel 32

Rapportering av överträdelser

1. Medlemsstaterna ska inrätta effektiva mekanismer som uppmuntrar rapportering till de behöriga myndigheterna av överträdelser av denna förordning.

De mekanismerna ska åtminstone omfatta de som avses i artikel 61.2 i direktiv (EU) 2015/849.

2. Betaltjänstleverantörerna och leverantörerna av kryptotillgångstjänster ska i samarbete med behöriga myndigheter fastställa lämpliga interna rutiner för att deras anställda, eller personer i jämförbar ställning, internt ska kunna rapportera om överträdelser genom en säker, oberoende, särskild och anonym kanal, som står i proportion till den berörda betaltjänstleverantörens eller leverantören av kryptotillgångstjänsters typ och storlek.

Artikel 33

Övervakning

1. Medlemsstaterna ska kräva att de behöriga myndigheterna effektivt övervakar och vidtar de åtgärder som krävs för att säkerställa att kraven i denna förordning uppfylls, och för att, genom effektiva mekanismer, uppmuntra rapportering till de behöriga myndigheterna av överträdelser av bestämmelserna i denna förordning.
2. Senast den 31 december 2026 och vart tredje år därefter ska kommissionen överlämna en rapport till Europaparlamentet och rådet om tillämpningen av kapitel VI med särskild hänsyn till gränsöverskridande fall.

KAPITEL VII

Genomförandebefogenheter

Artikel 34

Kommittéförfarande

1. Kommissionen ska biträdas av kommittén för förebyggande av penningtvätt och finansiering av terrorism. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.
2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

KAPITEL VIII

Undantag

Artikel 35

Överenskommelser med länder och territorier som inte utgör en del av unionens territorium

1. Kommissionen kan bemyndiga en medlemsstat att ingå överenskommelser med ett tredjeland eller med ett territorium utanför det territoriella tillämpningsområdet för fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt (EUF-fördraget) enligt artikel 355 i EUF-fördraget (*det berörda landet eller territoriet*), som innehåller undantag från denna förordning, varigenom det blir möjligt att behandla överföringar av medel mellan det landet eller territoriet och den berörda medlemsstaten som överföringar av medel inom den medlemsstaten.

Sådana överenskommelser får bemyndigas endast när samtliga följande villkor är uppfyllda:

- a) Det berörda landet eller territoriet ingår i en monetär union med den berörda medlemsstaten eller utgör en del av den medlemsstatens valutaområde eller har undertecknat ett monetärt avtal med unionen företrädd av en medlemsstat.
- b) Betaltjänstleverantörer i det berörda landet eller territoriet deltar direkt eller indirekt i den medlemsstatens betalnings- och avvecklingssystem.
- c) Det berörda landet eller territoriet kräver att betaltjänstleverantörer som verkar inom dess jurisdiktion ska tillämpa samma regler som de som fastställs i denna förordning.

2. En medlemsstat som önskar ingå en sådan överenskommelse som avses i punkt 1 ska lämna in en begäran till kommissionen och tillhandahålla den alla uppgifter som krävs för att bedöma begäran.

3. När kommissionen tagit emot en sådan begäran ska överföringar av medel mellan denna medlemsstat och det berörda landet eller territoriet provisoriskt behandlas som överföringar av medel inom den medlemsstaten fram till dess att ett beslut har fattats i enlighet med denna artikel.

4. Om kommissionen inom två månader efter mottagandet av begäran inte anser sig ha alla uppgifter som krävs för att bedöma begäran, ska den kontakta den berörda medlemsstaten och specificera vilka ytterligare uppgifter som krävs.

5. Inom en månad efter det att den har mottagit alla uppgifter som den anser krävs för att bedöma begäran, ska kommissionen underrätta den ansökande medlemsstaten om detta och vidarebefordra kopior av begäran till de övriga medlemsstaterna.

6. Inom tre månader efter den underrättelse som avses i punkt 5 i den här artikeln ska kommissionen genom en genomförandeakt i enlighet med artikel 34.2 besluta om den ska bemyndiga den berörda medlemsstaten att ingå det avtal som är föremål för begäran.

Kommissionen ska i alla händelser anta ett beslut enligt första stycket i denna punkt inom 18 månader efter att ha tagit emot begäran.

KAPITEL IX

Övriga bestämmelser

Artikel 36

Riktlinjer

EBA ska utfärda riktlinjer till de behöriga myndigheterna och betaltjänstleverantörerna i enlighet med artikel 16 i förordning (EU) nr 1093/2010 om åtgärder som ska vidtas i enlighet med den här förordningen, särskilt när det gäller genomförandet av artiklarna 7, 8, 11 och 12 i den här förordningen. Senast den 30 juni 2024 ska EBA till behöriga myndigheter och till leverantörer av kryptotillgångstjänster utfärda riktlinjer om de åtgärder som ska vidtas för tillämpningen av artiklarna 14–17 och 19–22 i den här förordningen.

EBA ska utfärda riktlinjer som specificerar tekniska aspekter för tillämpningen av denna förordning på autogirering liksom de åtgärder som ska vidtas av leverantörer av betalningsinitieringstjänster, enligt definitionen i artikel 4.18 i direktiv (EU) 2015/2366, enligt denna förordning, med beaktande av deras begränsade roll i betalningstransaktionen.

EBA ska utfärda riktlinjer, riktade till behöriga myndigheter, om egenskaperna hos en riskbaserad metod för tillsyn av leverantörer av kryptotillgångstjänster och om de steg som ska tas vid genomförande av sådan tillsyn.

EBA ska säkerställa en regelbunden dialog med berörda parter om utvecklingen av interoperabla tekniska lösningar i syfte att underlätta genomförandet av de krav som fastställs i denna förordning.

Artikel 37

Översyn

1. Senast 12 månader efter den dag då en förordning om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism trätt i kraft ska kommissionen se över den här förordningen och ska vid behov föreslå ändringar för att säkerställa samstämmighet med och anpassning till förordningen om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism.
2. Senast den 1 juli 2026 ska kommissionen, efter samråd med EBA, utfärda en rapport i vilken riskerna med överföringar till eller från fristående adresser eller enheter som inte är etablerade i unionen bedöms, samt behovet av särskilda åtgärder för att minska dessa risker, och vid behov föreslå ändringar av denna förordning.
3. Senast den 30 juni 2027 bör kommissionen till Europaparlamentet och rådet överlämna en rapport om tillämpningen och efterlevnaden av denna förordning, vid behov åtföljd av ett lagstiftningsförslag.

Den rapport som avses i första stycket ska innehålla följande:

- a) En bedömning av hur effektiva de åtgärder som föreskrivs i denna förordning är och av hur betaltjänstleverantörerna och leverantörerna av kryptotillgångstjänster efterlever denna förordning.
- b) En bedömning av de tekniska lösningarna för att uppfylla de skyldigheter som åläggs leverantörer av kryptotillgångstjänster enligt denna förordning, inbegripet av den senaste utvecklingen av tekniskt sunda och interoperabla lösningar för att efterleva denna förordning och av användningen av DLT-analysverktyg för att identifiera ursprung och destination för överföringar av kryptotillgångar och för att göra en bedömning av transaktionskännetecknet.
- c) En bedömning av hur effektiva och lämpliga *de minimis*-trösklarna för överföringar av medel är, särskilt med avseende på tillämpningsområdet och uppsättningen uppgifter som ska åtfölja överföringar, samt en bedömning av behovet av att sänka eller ta bort sådana trösklar.
- d) En bedömning av kostnaderna och fördelarna med att införa *de minimis*-trösklar för den uppsättning uppgifter som åtföljer överföringar av kryptotillgångar, inbegripet en bedömning av de relaterade riskerna för penningtvätt och finansiering av terrorism.
- e) En analys av trenderna i samband med användningen av fristående adresser för att utföra överföringar utan inblandning av en tredje part, tillsammans med en bedömning av de relaterade riskerna för penningtvätt och finansiering av terrorism och en bedömning av behovet, effektiviteten och verkställbarheten av ytterligare riskreducerande åtgärder, såsom specifika skyldigheter för leverantörer av hårdvaru- och mjukvaruplånböcker och begränsning och kontroll av eller förbud mot överföringar som inbegriper fristående adresser.

Den rapporten ska beakta ny utveckling inom området bekämpning av penningtvätt och finansiering av terrorism, samt relevanta utvärderingar, bedömningar eller rapporter inom det området som utarbetats av internationella organisationer och normgivare, brottsbekämpande myndigheter och underrättelsetjänster, leverantörer av kryptotillgångstjänster eller andra tillförlitliga källor.

KAPITEL X

Slutbestämmelser

Artikel 38

Ändring av direktiv (EU) 2015/849

Direktiv (EU) 2015/849 ska ändras på följande sätt:

1. I artikel 2.1.3 ska leden g och h utgå.

2. Artikel 3 ska ändras på följande sätt:

a) I punkt 2 ska följande led läggas till:

”g) leverantörer av kryptotillgångstjänster.”.

b) Punkt 8 ska ersättas med följande:

”8. korrespondentförbindelse:

a) tillhandahållande av banktjänster från en bank som korrespondent till en annan bank som motpart, inbegripet tillhandahållande av ett löpande konto eller annat passivkonto och härtill knutna tjänster, t. ex. likviditetsförvaltning, internationella överföringar av medel, checkavräkning, payable-through-konton och valutatjänster,

b) förbindelserna mellan kreditinstitut och finansiella institut, inbegripet där liknande tjänster tillhandahålls av ett korrespondentinstitut till ett motpartsinstitut, och inbegripet förbindelser som etablerats för värdepapperstransaktioner eller överföring av medel eller förbindelser som etablerats för kryptotillgångstransaktioner eller överföringar av kryptotillgångar.”.

c) Punkterna 18 och 19 ska ersättas med följande:

”18. *kryptotillgång*: en kryptotillgång enligt definitionen i artikel 3.1.5 i Europaparlamentets och rådets förordning (EU) 2023/1114 (*) utom när den ingår i de kategorier som förtecknas i artikel 2.2, 2.3 och 2.4 i den förordningen eller på annat sätt räknas som medel.

19. *leverantör av kryptotillgångstjänster*: en leverantör av kryptotillgångstjänster enligt definitionen i artikel 3.1.15 i förordning (EU) 2023/1114, som utför en eller flera kryptotillgångstjänster enligt definitionen i artikel 3.1.16 i den förordningen, med undantag för rådgivning om kryptotillgångar som avses i artikel 3.1.16 h i den förordningen.

(*) Europaparlamentets och rådets förordning (EU) 2023/1114 av den 31 maj 2023 om marknader för kryptotillgångar och om ändring av förordningarna (EU) nr 1093/2010 och (EU) nr 1095/2010 samt direktiven 2013/36/EU och (EU) 2019/1937 (EUT L 150, 9.6.2023, s. 40).”.

d) Följande led ska läggas till:

”20. *fristående adress*: en fristående adress enligt definitionen i artikel 3.20 i Europaparlamentets och rådets förordning (EU) 2023/1113 (*).

(*) Europaparlamentets och rådets förordning (EU) 2023/1113 av den 31 maj 2023 om uppgifter som ska åtfölja överföringar av medel och vissa kryptotillgångar och ändring av direktiv (EU) 2015/849 (EUT L 150, 9.6.2023, s. 1).”.

3. I artikel 18 ska följande punkter läggas till:

”5. Senast 30 December 2024 ska EBA utfärda riktlinjer om riskvariabler och riskfaktorer som leverantörer av kryptotillgångstjänster ska beakta när de ingår affärsförbindelser eller utför transaktioner med kryptotillgångar.

6. EBA ska särskilt klargöra hur de riskfaktorer som anges i bilaga III ska tas i beaktande av leverantörer av kryptotillgångstjänster, inbegripet när de utför transaktioner med personer och enheter som inte omfattas av detta direktiv. EBA ska i detta syfte särskilt uppmärksamma produkter, transaktioner och teknik som har potential att underlätta anonymitet, såsom privata plånböcker, mixertjänster eller tumlartjänster.

Om situationer med högre risk identifieras ska de riktlinjer som avses i punkt 5 omfatta skärpta åtgärder för kundkännedom som ansvariga enheter ska överväga att vidta för att minska dessa risker, inbegripet införande av lämpliga förfaranden för att bestämma kryptotillgångarnas ursprung eller destination.”.

4. Följande artiklar ska införas:

”Artikel 19a

1. Medlemsstaterna ska kräva att leverantörer av kryptotillgångstjänster identifierar och bedömer risken för penningtvätt och finansiering av terrorism i samband med överföringar av kryptotillgångar som riktas till eller härrör från en fristående adress. Leverantörer av kryptotillgångstjänster ska därför ha infört interna strategier, förfaranden och kontroller för detta ändamål. Medlemsstaterna ska kräva att leverantörer av kryptotillgångstjänster vidtar riskreducerande åtgärder som motsvarar de identifierade riskerna. Dessa riskreducerande åtgärder ska inbegripa en eller flera av följande åtgärder:

a) Vidta riskbaserade åtgärder för att identifiera och kontrollera identiteten på avsändaren eller mottagaren av en överföring till eller från en fristående adress eller avsändarens eller mottagarens verkliga huvudman, inbegripet genom att förlita sig på tredje parter.

b) Kräva ytterligare information om de överförda kryptotillgångarnas ursprung och destination.

c) Genomföra en skärpt fortlöpande övervakning av dessa transaktioner.

d) Andra åtgärder för att minska och hantera riskerna för penningtvätt och finansiering av terrorism samt risken för att riktade ekonomiska sanktioner och riktade ekonomiska sanktioner som rör finansiering av spridning av vapen inte genomförs eller kringgås.

2. Senast 30 December 2024 ska EBA utfärda riktlinjer för att specificera vilka åtgärder som avses i denna artikel, inbegripet kriterier och medel för identifiering och kontroll av identiteten på avsändaren eller mottagaren av en överföring till eller från en fristående adress, särskilt genom att förlita sig på tredje parter, med beaktande av den senaste tekniska utvecklingen.

Artikel 19b

1. Vid gränsöverskridande korrespondentförbindelser som inbegriper verkställandet av kryptotillgångstjänster enligt definitionen i artikel 3.1.16 i förordning (EU) 2023/1114, med undantag för led h i den punkten, med en motpartsenhet som inte är etablerad i unionen och som tillhandahåller liknande tjänster, inbegripet överföringar av kryptotillgångar, ska medlemsstaterna, genom undantag från artikel 19, utöver de åtgärder för kundkännedom som fastställs i artikel 13 i detta direktiv, kräva att leverantörer av kryptotillgångstjänster, när de ingår en affärsförbindelse med en sådan enhet, gör följande:

- a) Fastställer om motpartsenheten har tillstånd eller är registrerad.
- b) Samlar in så mycket information om motpartsenheten att de får full insikt i dess affärsverksamhet och utifrån offentligt tillgänglig information kan bedöma dess anseende och övervakningens kvalitet.
- c) Bedömer de kontroller för bekämpning av penningtvätt och finansiering av terrorism som motpartsenheten har infört.
- d) Inhämtar godkännande från sin ledning innan de ingår nya korrespondentförbindelser.
- e) Dokumenterar respektive ansvarsområden för varje part i korrespondentförbindelsen.
- f) När det gäller "payable-through"-konton för kryptotillgångar, försäkras sig om att motpartsenheten har kontrollerat identiteten på och fortlöpande vidtagit åtgärder för kundkännedom med avseende på de kunder som har direkt tillgång till konton hos korrespondentenheten, och att den på begäran kan tillhandahålla relevant kundkännedom till korrespondentenheten.

Om leverantörer av kryptotillgångstjänster beslutar att avsluta korrespondentförbindelser av skäl som rör strategin för bekämpning av penningtvätt och finansiering av terrorism, ska de dokumentera sitt beslut.

Leverantörer av kryptotillgångstjänster ska uppdatera kundkännedomsuppgifterna för korrespondentförbindelsen regelbundet eller när nya risker uppstår i förhållande till motpartsenheten.

2. Medlemsstaterna ska säkerställa att leverantörer av kryptotillgångstjänster beaktar de uppgifter som avses i punkt 1 för att på grundval av en riskbedömning fastställa vilka lämpliga åtgärder som ska vidtas för att minska de risker som är förknippade med motpartsenheten.

3. Senast 30 juni 2024 ska EBA utfärda riktlinjer för att specificera de kriterier och aspekter som leverantörer av kryptotillgångstjänster ska ta i beaktande i den bedömning som avses i punkt 1 och de riskreducerande åtgärder som avses i punkt 2, inbegripet de minimiåtgärder som leverantörer av kryptotillgångstjänster ska vidta om motparts-enheten inte är registrerad eller har tillstånd.”.

5. Följande artikel ska införas:

”Artikel 24a

Senast den 1 januari 2024 ska EBA utfärda riktlinjer som specificerar hur de skärpta åtgärderna för kundkännedom i detta avsnitt ska tillämpas när ansvariga enheter utför kryptotillgångstjänster enligt definitionen i artikel 3.1.16 i förordning (EU) 2023/1114, med undantag för led h i den punkten, samt överföringar av kryptotillgångar enligt definitionen i artikel 3.10 i förordning (EU) 2023/1113. EBA ska särskilt ange hur och när dessa ansvariga enheter ska inhämta ytterligare uppgifter om avsändaren och mottagaren.”.

6. I artikel 45 ska punkt 9 ersättas med följande:

”9. Medlemsstaterna får kräva att utgivare av elektroniska pengar enligt definitionen i artikel 2.3 i direktiv 2009/110/EG, betaltjänstleverantörer enligt definitionen i artikel 4.11 i direktiv (EU) 2015/2366 och leverantörer av kryptotillgångstjänster som är etablerade på deras territorium i en annan form än en filial och vars huvudkontor är beläget i en annan medlemsstat, utser en central kontaktpunkt på deras territorium. Denna kontaktpunkt ska, som företrädare för enheten med gränsöverskridande verksamhet, säkerställa att reglerna för bekämpning av penningtvätt och finansiering av terrorism följs och underlätta för tillsynsmyndigheterna att utöva tillsyn, bland annat genom att på begäran förse tillsynsmyndigheterna med dokument och information.”.

7. I artikel 47 ska punkt 1 ersättas med följande:

”1. Medlemsstaterna ska säkerställa att valutaväxlings- och checkinlösningskontor samt leverantörer av tjänster till trustar eller bolag har tillstånd eller är registrerade och att tillhandahållare av speltjänster ska regleras.”.

8. I artikel 67 ska följande punkt läggas till:

”3. Medlemsstaterna ska senast den 30 december 2024 anta och offentliggöra de bestämmelser i lagar och andra författningar som är nödvändiga för att följa artikel 2.1.3, artikel 3.2 g, artikel 3.8, 3.18, 3.19 och 3.20, artikel 19a.1, artikel 19b.1 och 19b.2, artikel 45.9 och artikel 47.1. De ska genast underrätta kommissionen om texten till dessa bestämmelser.

De ska tillämpa dessa bestämmelser från och med 30 december 2024.”.

Artikel 39

Upphävande

Förordning (EU) 2015/847 ska upphöra att gälla med verkan den dag då den här förordningen börjar tillämpas.

Hänvisningar till den upphävda förordningen ska anses som hänvisningar till den här förordningen och läsas i enlighet med jämförelsetabellen i bilaga II.

*Artikel 40***Ikraftträdande**

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Den ska tillämpas från och med den 30 december 2024.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 31 maj 2023.

På Europaparlamentets vägnar

R. METSOLA

Ordförande

På rådets vägnar

P. KULLGREN

Ordförande

BILAGA I

UPPHÄVD FÖRORDNING OCH ÄNDRINGEN AV DENNA

Europaparlamentets och rådets förordning (EU) 2015/847 (EUT L 141, 5.6.2015, s. 1)	
Europaparlamentets och rådets förordning (EU) 2019/2175 (EUT L 334, 27.12.2019, s. 1)	[endast artikel 6]

BILAGA II

JÄMFÖRELSETABELL

Förordning (EU) 2015/847	Denna förordning
Artikel 1	Artikel 1
Artikel 2.1, 2.2 och 2.3	Artikel 2.1, 2.2 och 2.3
Artikel 2.4 första och andra styckena	Artikel 2.4 första och andra styckena
—	Artikel 2.4 tredje och fjärde styckena
Artikel 2.5	Artikel 2.5
Artikel 3 inledningsfrasen	Artikel 3 inledningsfrasen
Artikel 3.1–3.9	Artikel 3.1–3.9
—	Artikel 3.10
Artikel 3.10	Artikel 3.11
Artikel 3.11	Artikel 3.12
Artikel 3.12	—
—	Artikel 3.13–3.24
Artikel 4.1 inledningsfrasen	Artikel 4.1 inledningsfrasen
Artikel 4.1 a, b och c	Artikel 4.1 a, b och c
—	Artikel 4.1 d
Artikel 4.2 inledningsfrasen	Artikel 4.2 inledningsfrasen
Artikel 4.2 a och b	Artikel 4.2 a och b
—	Artikel 4.2 c
Artikel 4.3–4.6	Artikel 4.3–4.6
Artiklarna 5–13	Artiklarna 5–13
—	Artiklarna 14–23
Artikel 14	Artikel 24

Förordning (EU) 2015/847	Denna förordning
Artikel 15.1, 15.2 och 15.3	Artikel 25.1, 25.2 och 25.3
Artikel 15.4 enda stycket	Artikel 25.4 första stycket
—	Artikel 25.4 andra stycket
Artikel 16	Artikel 26
—	Artikel 27
Artikel 17	Artikel 28
Artikel 18	Artikel 29
Artikel 19	Artikel 30
Artikel 20	Artikel 31
Artikel 21	Artikel 32
Artikel 22	Artikel 33
Artikel 23	Artikel 34
Artikel 24.1–24.6	Artikel 35.1–35.6
Artikel 24.7	—
Artikel 25 enda stycket	Artikel 36 första stycket
—	Artikel 36 andra, tredje och fjärde styckena
—	Artikel 37
—	Artikel 38
Artikel 26	Artikel 39
Artikel 27	Artikel 40
Bilaga	—
—	Bilaga I
—	Bilaga II