EBA/GL/2024/14

14 november 2024

Riktlinjer

för interna strategier, förfaranden och kontroller för att säkerställa genomförandet av unionens restriktiva åtgärder och nationella restriktiva åtgärder

1. Efterlevnads- och rapporteringsskyldigheter

Riktlinjernas status

1. Detta dokument innehåller riktlinjer som har utfärdats i enlighet med artikel 16 i förordning (EU) nr 1093/2010[1]. I enlighet med artikel 16.3 i förordning (EU) nr 1093/2010 ska de behöriga myndigheterna och de finansiella instituten med alla tillgängliga medel söka följa dessa riktlinjer.

2. I riktlinjerna fastställs EBA:s syn på lämplig tillsynspraxis inom det europeiska systemet för finansiell tillsyn och hur unionsrätten bör tillämpas inom ett särskilt område. Behöriga myndigheter enligt definitionen i artikel 4.2 i förordning (EU) nr 1093/2010 som berörs av riktlinjerna bör följa dem genom att på lämpligt sätt införliva dem i sin praxis (till exempel genom att ändra sina rättsliga ramar eller tillsynsprocesser), även när riktlinjerna i första hand riktas till finansiella institut.

Rapporteringskrav

3. Enligt artikel 16.3 i förordning (EU) nr 1093/2010 måste de behöriga myndigheterna meddela EBA om de följer eller avser att följa dessa riktlinjer, alternativt ange skälen till att de inte gör det, senast 11.04.2025. Om någon sådan anmälan inte inkommer inom denna tidsfrist kommer EBA anse att de behöriga myndigheterna inte följer riktlinjerna. Anmälningarna ska lämnas in via det formulär som tillhandahålls på EBA:s webbplats, med hänvisningen EBA/GL/2024/14. Anmälningarna bör lämnas in av personer som på sina behöriga myndigheters vägnar har befogenhet att rapportera om hur riktlinjerna tillämpas. Alla förändringar i graden av efterlevnad måste också rapporteras till EBA.

4. Anmälningarna kommer att offentliggöras på EBA:s webbplats i enlighet med artikel 16.3.

[1] 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).

2. Syfte, tillämpningsområde och definitioner

Syfte och tillämpningsområde

5. I dessa riktlinjer specificeras de interna strategier, förfaranden och kontroller som finansiella institut som är föremål för reglering och tillsyn enligt direktiv 2013/36/EU, direktiv (EU) 2015/2366 och direktiv 2009/110/EG bör införa, i enlighet med artikel 74.1 i direktiv 2013/36/EU, artikel 11.4 i direktiv (EU) 2015/2366 och artikel 3.1 i direktiv 2009/110/EG, för att säkerställa ett effektivt genomförande av unionens restriktiva åtgärder och nationella restriktiva åtgärder.

Målgrupp

6. Dessa riktlinjer riktar sig till

   (i) behöriga myndigheter enligt definitionen i de rättsakter som avses i artikel 4.2 i) i förordning (EU) nr 1093/2010,

   (ii) behöriga myndigheter enligt definitionen i artikel 4.2 vi) i förordning (EU) nr 1093/2010 med avseende på direktiv (EU) 2015/2366 och direktiv 2009/110/EG,

   (iii) finansiella institut som är föremål för reglering och tillsyn i enlighet med direktiv 2013/36/EU, direktiv (EU) 2015/2366 och direktiv 2009/110/EG.

7. Behöriga myndigheter som ansvarar för att bedöma interna strategier, förfaranden och kontroller som antagits av finansiella institut för att säkerställa genomförandet av unionens restriktiva åtgärder och nationella restriktiva åtgärder, i enlighet med den nationella rättsliga ramen, kan använda dessa riktlinjer vid bedömningen av sådana interna strategier, förfaranden och kontroller.

Definition

Om inget annat anges har de termer som används och definieras i direktiv 2013/36/EU, direktiv (EU) 2015/2366 och direktiv 2009/110/EG samma innebörd i riktlinjerna. I dessa riktlinjer gäller dessutom följande definition:

restriktiva åtgärder	unionens restriktiva åtgärder enligt definitionen i artikel 2.1 i direktiv (EU) 2024/1226 och nationella restriktiva åtgärder som antagits av medlemsstaterna i enlighet med deras nationella rättsordning (i den mån de är tillämpliga på finansiella institut).

3. Genomförande

Datum för tillämpning

8. Dessa riktlinjer gäller från den 30 december 2025.

4. Riktlinjer för interna strategier, förfaranden och kontroller för att säkerställa genomförandet av unionens restriktiva åtgärder och nationella restriktiva åtgärder

Allmänna bestämmelser

1. Finansiella institut bör identifiera och bedöma de verksamhetsområden som är särskilt utsatta eller exponerade för restriktiva åtgärder och för kringgående av restriktiva åtgärder. På grundval av detta bör de införa och genomföra strategier, förfaranden och kontroller, samt se till att dessa hålls uppdaterade, för att säkerställa att de effektivt kan följa systemen för restriktiva åtgärder.

2. Dessa strategier, förfaranden och kontroller bör vara effektiva och stå i proportion till det finansiella institutets storlek, art och komplexitet samt till dess exponering för restriktiva åtgärder.

4.1 Ram för styrning och ledningsorganets roll

3. Finansiella institut bör inrätta en ram för styrning för att säkerställa att strategier, förfaranden och kontroller för genomförandet av restriktiva åtgärder är adekvata och genomförs effektivt.

4. Det finansiella institutets ledningsorgan bör ansvara för att godkänna det finansiella institutets strategi för efterlevnad av restriktiva åtgärder och för att övervaka dess genomförande genom de strategier, förfaranden och kontroller som krävs för att säkerställa genomförandet av restriktiva åtgärder. Alla ledamöter i ledningsorganet bör vara medvetna om det finansiella institutets exponering för restriktiva åtgärder och dess utsatthet för kringgående av restriktiva åtgärder.

5. Om det finansiella institutets verksamhet leds av en enda person får denna person utse en senior befattningshavare för att utföra ledningsorganets uppgifter i enlighet med punkt 4.

6. Om det finansiella institutet är moderföretag i en koncern enligt definitionerna i artikel 2.9 och 2.11 i direktiv 2013/34/EU [2], bör moderföretagets ledningsorgan säkerställa att varje ledningsorgan, affärsområde och intern enhet, inbegripet varje intern kontrollfunktion i koncernens dotterföretag, har den information som krävs för att kunna följa restriktiva åtgärder. Det yttersta ansvaret för efterlevnaden av restriktiva åtgärder ligger hos varje enhet i koncernen.

7. Om ett finansiellt institut är moderföretag i en koncern bör moderföretagets ledningsorgan säkerställa att koncernens dotterföretag genomför en egen exponeringsbedömning avseende restriktiva åtgärder, enligt vad som anges i avsnitt 4.2, på ett samordnat sätt och på grundval av en gemensam metod som återspeglar koncernens särdrag.

4.1.1 Ledningsorganets tillsynsfunktion

8. I sin tillsynsfunktion bör ledningsorganet ansvara för att kontrollera och övervaka ramen för intern kontroll och styrning som det finansiella institutet har inrättat för att följa restriktiva åtgärder, för att säkerställa att den är effektiv, i enlighet med avsnitt 4.3.

9. Utöver bestämmelserna i riktlinjerna EBA/GL/2021/05 [3], bör ledningsorganet i sin tillsynsfunktion

    a. informeras om resultaten av den senaste exponeringsbedömningen avseende restriktiva åtgärder, i enlighet med avsnitt 4.2,
    b. kontrollera och övervaka, genom funktionen för intern kontroll, i vilken utsträckning strategierna och förfarandena för restriktiva åtgärder är adekvata och effektiva, i enlighet med avsnitt 4.3, mot bakgrund av exponeringen för restriktiva åtgärder och de risker för kringgående av restriktiva åtgärder som det finansiella institutet är exponerat för, samt vidta lämpliga åtgärder för att säkerställa att korrigerande åtgärder vidtas vid behov,
    c. minst en gång om året bedöma huruvida funktionen för efterlevnad av restriktiva åtgärder, inbegripet interna strategier, förfaranden och kontroller, fungerar på ett effektivt sätt, inbegripet huruvida de personalresurser och tekniska resurser som avsatts för efterlevnad av restriktiva åtgärder är lämpliga.

10. Om ett finansiellt institut är moderföretag i en koncern bör ledningsorganet för det moderföretaget också utföra alla de uppgifter som avses i punkt 9 på koncernnivå. Det yttersta ansvaret för efterlevnaden av restriktiva åtgärder ligger hos varje enhet i koncernen.

[2] Europaparlamentets och rådets direktiv 2013/34/EU av den 26 juni 2013 om årsbokslut, koncernredovisning och rapporter i vissa typer av företag, om ändring av Europaparlamentets och rådets direktiv 2006/43/EG och om upphävande av rådets direktiv 78/660/EEG och 83/349/EEG.

[3] Riktlinjer (EBA/GL/2021/05) för intern styrning enligt direktiv 2013/36/EU.

4.1.2 Ledningsorganets ledningsfunktion

11. Utöver bestämmelserna i riktlinjerna EBA/GL/2021/05, bör ledningsorganet i sin ledningsfunktion

    a. säkerställa att det informeras om resultaten av den senaste exponeringsbedömningen avseende restriktiva åtgärder, i enlighet med avsnitt 4.2,
    b. anta en lämplig ram för riskhantering och ett system för intern kontroll som är tillräckligt oberoende av den verksamhet som kontrolleras,
    c. godkänna strategier, förfaranden och kontroller som står i proportion till det finansiella institutets exponering för restriktiva åtgärder och är adekvata för att säkerställa det finansiella institutets efterlevnad av restriktiva åtgärder,
    d. säkerställa ett effektivt genomförande av det finansiella institutets processer för efterlevnad av restriktiva åtgärder,
    e. genomföra den organisatoriska och operativa struktur som krävs för att på ett effektivt sätt följa den strategi för restriktiva åtgärder som antagits av ledningsorganet,
    f. säkerställa att de personalresurser och tekniska resurser som avsatts för efterlevnad av restriktiva åtgärder är lämpliga och står i proportion till institutets exponering för restriktiva åtgärder,
    g. om operativa funktioner avseende efterlevnad av restriktiva åtgärder utkontrakteras, säkerställa att dessa arrangemang överensstämmer med riktlinjerna EBA/GL/2019/02[4], och regelbundet få rapporter från tjänsteleverantören om systemets effektivitet för att informera ledningsorganet.

12. Om det finansiella institutet är moderföretag i en koncern bör ledningsorganet för det moderföretaget säkerställa att alla de uppgifter som avses i punkt 11 också utförs på dotterföretagsnivå och att de strategier och förfaranden som införts är förenliga med koncernens förfaranden och strategier, i den utsträckning det är tillåtet enligt tillämplig nationell lagstiftning.

4.1.3 Rollen för den seniora tjänsteman som ansvarar för efterlevnaden av restriktiva åtgärder

4.1.3.1 Utnämning av den seniora tjänstemannen

13. Finansiella institut bör utse en senior tjänsteman som ansvarar för att utföra de funktioner och uppgifter som anges i punkterna 19–21. Ledningsorganet bör se till att den seniora tjänstemannen har den kunskap och förståelse avseende restriktiva åtgärder som krävs för att kunna fullgöra sina uppgifter på ett effektivt sätt.

[4] Riktlinjer (EBA/GL/2019/02) för utkontraktering, som ska ersättas av riktlinjer (EBA/GL/XXXX/XX) för sund hantering av tredjepartsrisker.

14. Ledningsorganet får tilldela denna roll till en senior tjänsteman som redan har andra uppgifter eller funktioner inom det finansiella institutet (såsom den ansvarige för regelefterlevnad för bekämpning av penningtvätt och finansiering av terrorism eller chefen för regelefterlevnad), förutsatt att

    a. detta motiveras av det finansiella institutets storlek och komplexitet och resultatet av exponeringsbedömningen avseende restriktiva åtgärder,
    b. detta inte påverkar den seniora tjänstemannens förmåga att utföra sina uppgifter eller funktioner på ett effektivt sätt,
    c. denna kombination av uppgifter inte ger upphov till några intressekonflikter, såsom konflikter mellan den seniora tjänstemannens operativa uppgifter och kontrolluppgifter.

15. Ledningsorganet bör göra det möjligt för den seniora tjänstemannen att tilldela och delegera de uppgifter som anges i punkterna 19–21 till annan personal som agerar under den seniora tjänstemannens ledning och överinseende, förutsatt att det yttersta ansvaret för att dessa uppgifter utförs på ett effektivt sätt ligger kvar hos den seniora tjänstemannen.

16. Oberoende av de institutionella arrangemangen bör finansiella institut se till att

    a. den seniora tjänstemannen kan samordna arbetet och samarbeta på ett effektivt sätt med funktionerna för intern kontroll,
    b. den seniora tjänstemannen kan rapportera och har direkt tillgång till ledningsorganet i dess lednings- och tillsynsfunktion.

17. Om det finansiella institutet ingår i en koncern bör ledningsorganet för moderföretaget utse en senior tjänsteman på koncernnivå.

4.1.3.2 Den seniora tjänstemannens roll

18. Den seniora tjänstemannen bör utveckla, införa och upprätthålla strategier, förfaranden och kontroller som är adekvata för att säkerställa att det finansiella institutet följer de restriktiva åtgärderna och som står i proportion till det finansiella institutets exponering för restriktiva åtgärder.

19. Den seniora tjänstemannen bör göra följande:

    a. Vidta de åtgärder som är nödvändiga för att säkerställa efterlevnad av avsnitt 4.2 om exponeringsbedömningen avseende restriktiva åtgärder.
    b. Vidta de åtgärder som är nödvändiga för att säkerställa efterlevnad av avsnitt 4.3 om effektiva strategier och förfaranden för restriktiva åtgärder.
    c. Förse ledningsorganet med regelbunden och adekvat information så att det kan utföra sina uppgifter enligt avsnitt 4.1.1 och avsnitt 4.1.2. Sådan information bör åtminstone omfatta följande:

i) Förändringar gällande det finansiella institutets exponering för restriktiva åtgärder och resultatet av det finansiella institutets exponeringsbedömning avseende restriktiva åtgärder.

ii) Förändringar gällande system för restriktiva åtgärder och deras inverkan på det finansiella institutet.

iii) Statistik och information avseende

- antalet genererade larm,
- antalet larm som ska analyseras,
- antalet rapporter som lämnats till den relevanta nationella myndighet som är behörig att genomföra restriktiva åtgärder [5] och/eller till den behöriga tillsynsmyndigheten enligt tillämplig lagstiftning,
- den genomsnittliga tiden mellan en sann positiv matchning och rapporteringen till den relevanta nationella myndighet som är behörig att genomföra restriktiva åtgärder och/eller till den behöriga tillsynsmyndigheten enligt tillämplig lagstiftning,
- värdet av de frysta penningmedel och de frysta ekonomiska resurser [6], samt dessa tillgångars karaktär, som innehas av det finansiella institutet.

iv) Information om personalresurser och tekniska resurser och om huruvida dessa resurser är tillräckliga mot bakgrund av det finansiella institutets exponering för restriktiva åtgärder.

v) Brister eller tillkortakommanden som identifierats avseende det finansiella institutets strategier, förfaranden och kontroller för genomförandet av restriktiva åtgärder, inbegripet iakttagelser som gjorts av behöriga myndigheter avseende tillsyn av strategier, förfaranden och kontroller för genomförandet av restriktiva åtgärder.

vi) Överträdelser och kringgående av restriktiva åtgärder samt skälen till detta.

vii) Förslag om hur man kan åtgärda eventuella förändringar avseende lagstadgade krav eller exponeringen för restriktiva åtgärder, eller eventuella brister eller tillkortakommanden i det finansiella institutets strategier, förfaranden eller kontroller för genomförandet av restriktiva åtgärder som har identifierats samt överträdelser och kringgående av restriktiva åtgärder som har identifierats.

d. Rapportera alla överträdelser av restriktiva åtgärder till de relevanta nationella myndigheter som är behöriga att genomföra restriktiva åtgärder och/eller till den behöriga tillsynsmyndigheten enligt tillämplig lagstiftning.

e. Samarbeta på ett effektivt och konstruktivt sätt med de relevanta nationella myndigheter som är behöriga att genomföra restriktiva åtgärder och den behöriga tillsynsmyndigheten enligt tillämplig lagstiftning.

[5] https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/overview-sanctions-and-related-resources_en#contact.

[6] Se artikel 2.5 och 2.6 i direktiv (EU) 2024/1226.

20. Om det finansiella institutet ingår i en koncern bör den seniora tjänstemannen på koncernnivå bedöma effektiviteten hos strategier, förfaranden och kontroller gällande efterlevnad av relevanta restriktiva åtgärder med avseende på filialer, dotterföretag, förmedlare, distributörer och ombud, i förekommande fall. Det yttersta ansvaret för efterlevnaden av restriktiva åtgärder ligger hos varje enhet i koncernen.

21. Den seniora tjänstemannen bör övervaka utarbetandet och genomförandet av utbildningsprogrammet i enlighet med avsnitt 4.4.

4.2 Genomförande av en exponeringsbedömning avseende restriktiva åtgärder

22. Finansiella instituts interna förfaranden bör omfatta en exponeringsbedömning avseende restriktiva åtgärder för att de ska få en uppfattning om i vilken utsträckning deras olika verksamhetsområden är exponerade för restriktiva åtgärder och är utsatta för kringgående av restriktiva åtgärder.

23. Exponeringsbedömningen avseende restriktiva åtgärder bör göra det möjligt för de finansiella instituten att identifiera och bedöma följande:

    a. Vilka system för restriktiva åtgärder som är tillämpliga på dem.
    b. Sannolikheten för att de restriktiva åtgärderna inte genomförs.
    c. Sannolikheten för kringgående av restriktiva åtgärder.
    d. Konsekvenserna av eventuella överträdelser av restriktiva åtgärder.
    e. Följande riskfaktorer:

    a) Geografisk risk, inbegripet

        i. där det finansiella institutet bedriver sin verksamhet, dvs. de jurisdiktioner och territorier där det finansiella institutet är etablerat eller verksamt,
        ii. i vilken utsträckning dessa jurisdiktioner och territorier är exponerade för restriktiva åtgärder eller är kända för att användas för att kringgå restriktiva åtgärder,
        iii. transaktionernas ursprung och destination.

    b) Kundrelaterad risk, inbegripet

        i. kunders och, i tillämpliga fall, deras verkliga huvudmäns och kontrollerande aktieägares kopplingar till länder för vilka restriktiva åtgärder har införts på grund av en situation som påverkar dessa länder, eller till länder som är kända för att användas för att kringgå restriktiva åtgärder,
        ii. antalet kunder och typen av kunder samt dessa kunders komplexitet, såsom problem att identifiera den verkliga huvudmannen,
        iii. kundbasens verksamhet och verksamhetens komplexitet, inbegripet eventuella kopplingar till branscher eller sektorer som kan vara föremål för ekonomiska eller

andra restriktiva åtgärder, samt frekvens och typer med avseende på transaktioner,

c) Produkt- och tjänsterelaterad risk, inbegripet

   i. karaktären på det finansiella institutets produkter och tjänster,
   ii. i vilken utsträckning tillhandahållandet av dessa produkter och tjänster exponerar det finansiella institutet för risken för överträdelse av restriktiva åtgärder och kringgående av restriktiva åtgärder.

d) Distributionskanalsrelaterad risk, inbegripet huruvida användningen av förmedlare, ombud, tredje parter, korrespondentbankförbindelser eller andra distributionskanaler leder till utsatthet, bland annat genom att

   i. begränsa det finansiella institutets exponering i förhållande till de berörda parterna,
   ii. göra det finansiella institutet beroende av tredje parters screeningsprocesser,
   iii. öka det finansiella institutets exponering för geografiska risker eftersom de bedriver verksamhet i, eller är baserade i, länder för vilka restriktiva åtgärder har införts på grund av en situation som påverkar dessa länder, eller till länder som är kända för att användas för att kringgå restriktiva åtgärder.

24. Den bedömning som avses i punkt 22 bör baseras på ett tillräckligt brett spektrum av informationskällor, inbegripet åtminstone följande:

   a. Information som erhållits som en del av tillämpningen av det finansiella institutets åtgärder för kundkännedom, i enlighet med bestämmelserna i artikel 13 i direktiv (EU) 2015/849.
   b. Information från internationella organ, myndigheter, nationella behöriga myndigheter, inbegripet tillsynsmyndigheter för bekämpning av penningtvätt och finansiering av terrorism, finansunderrättelseenheter och brottsbekämpande myndigheter, till exempel uppdaterade typologier om kringgående av restriktiva åtgärder.
   c. Information från trovärdiga och tillförlitliga öppna källor, såsom rapporter i ansedda tidningar och andra ansedda mediekanaler.
   d. Information från trovärdiga och tillförlitliga kommersiella organisationer, till exempel riskrapporter.
   e. I förekommande fall, en analys av tidigare larm för restriktiva åtgärder om sanna positiva och falska positiva matchningar för att identifiera i vilka situationer det är mest sannolikt att sanna positiva matchningar inträffar.

25. När finansiella institut gör en exponeringsbedömning avseende restriktiva åtgärder bör de överväga huruvida det vore användbart och proportionerligt att göra en retroaktiv screening av sin kunddatabas och sina tidigare transaktionsregister. Detta kan vara fallet om finansiella institut har fastställt eller har rimliga skäl att misstänka att deras tidigare screeningssystem var otillräckliga eller ineffektiva.

26. Finansiella institut bör säkerställa att exponeringsbedömningen avseende restriktiva åtgärder förblir aktuell och relevant. Av denna anledning bör finansiella institut se över bedömningen minst en gång om året och vid behov uppdatera den. Dessutom bör finansiella institut i förekommande fall se över sin exponeringsbedömning avseende restriktiva åtgärder i följande situationer:

    a. Vid antagande av nya restriktiva åtgärder och betydande förändringar avseende befintliga restriktiva åtgärder.
    b. Innan institutet tillhandahåller nya produkter, erbjuder nya kanaler för produktleveranser, betjänar nya kundgrupper eller tar sig in på marknaden i nya geografiska områden.
    c. Vid betydande förändringar avseende institutets verksamhetsprofil, kundbas, organisationsstruktur eller affärsmodell.
    d. Vid identifiering av underlåtenhet att genomföra restriktiva åtgärder och kringgående av restriktiva åtgärder, vilket visar att exponeringsbedömningen avseende restriktiva åtgärder är olämplig.
    e. Vid brister i den befintliga exponeringsbedömningen avseende restriktiva åtgärder som identifierats av det finansiella institutet eller den behöriga myndighet som ansvarar för tillsynen av interna strategier, förfaranden och kontroller för att säkerställa genomförandet av unionens restriktiva åtgärder och nationella restriktiva åtgärder.

27. Finansiella institut bör dokumentera sin metod för att genomföra och se över sin exponeringsbedömning avseende restriktiva åtgärder och resultatet av denna bedömning och på begäran göra dokumentationen tillgänglig för den behöriga myndigheten.

28. Om det finansiella institutet är moderföretag i en koncern bör koncernens ledningsorgan säkerställa att koncernens dotterföretag genomför en egen exponeringsbedömning avseende restriktiva åtgärder, på ett samordnat sätt och på grundval av en gemensam metod, samtidigt som bedömningen återspeglar de egna särdragen.

4.3 Säkerställa löpande effektivitet avseende strategier, förfaranden och kontroller för genomförandet av restriktiva åtgärder

29. För att vara effektiva bör ett finansiellt instituts strategier, förfaranden och kontroller för genomförandet av restriktiva åtgärder göra det möjligt för institutet att fullt ut och på ett korrekt sätt genomföra alla tillämpliga restriktiva åtgärder utan dröjsmål.

30. Strategier, förfaranden och kontroller bör åtminstone omfatta följande:

    a. Processer för att säkerställa att de finansiella instituten har all aktuell information om de tillämpliga restriktiva åtgärderna.
    b. Processer för att säkerställa att förteckningar och krav gällande tillämpliga restriktiva åtgärder uppdateras så snart de träder i kraft.
    c. Processer för att säkerställa att exponeringsbedömningen avseende restriktiva åtgärder förblir relevant och aktuell.
    d. Processer för att säkerställa att strategier, förfaranden och kontroller står i proportion till exponeringsbedömningen avseende restriktiva åtgärder.
    e. Processer för att säkerställa att strategier och förfaranden för restriktiva åtgärder
        i. regelbundet ses över,
        ii. regelbundet ändras och uppdateras vid behov,
        iii. genomförs effektivt,
        iv. utformas på ett sådant sätt att de utlöser nödvändiga åtgärder när brister har identifierats.
    f. Förfaranden för att utan dröjsmål börja undersöka alla potentiella matchningar.
    g. Vid sanna positiva matchningar, förfaranden som påkallar uppföljningsåtgärder för att säkerställa efterlevnad av tillämpliga restriktiva åtgärder, inbegripet omedelbara beslut om avvisning, tillfälligt avbrott, eller frysning, samt rapportering till relevanta nationella myndigheter som är behöriga att genomföra restriktiva åtgärder eller till den behöriga tillsynsmyndigheten enligt tillämplig lagstiftning, inom de tidsfrister som anges av dessa myndigheter eller i förordningen om tillämpliga restriktiva åtgärder.
    h. En dokumenterad intern organisation som tydligt anger uppgifter och ansvar i samband med restriktiva åtgärder, även vid utkontraktering.
    i. Andra aspekter som anges i riktlinjerna (EBA/GL/2024/15) för interna strategier, förfaranden och kontroller för att säkerställa genomförandet av restriktiva åtgärder enligt förordning (EU) 2023/1113.

4.4 Utbildning

31. Finansiella institut bör regelbundet tillhandahålla utbildning till sina anställda för att säkerställa att de är och håller sig underrättade om

    a. tillämpliga restriktiva åtgärder,
    b. resultatet av exponeringsbedömningen avseende restriktiva åtgärder,
    c. strategier, förfaranden och kontroller för att följa tillämpliga restriktiva åtgärder.

32. Utbildningen bör anpassas till de anställda och deras specifika roller. Den bör anordnas på ett adekvat sätt och inom lämpliga tidsramar för att göra det möjligt för det finansiella institutet att följa restriktiva åtgärder. Inom en koncern kan detta – helt eller delvis – genomföras av moderföretaget.

33. Finansiella institut bör dokumentera sin utbildningsplan och vara beredda att på begäran kunna visa för den behöriga myndigheten att utbildningen är adekvat och effektiv.

EBA/GL/2024/15

14 november 2024

Riktlinjer

för interna strategier, förfaranden och kontroller för att säkerställa genomförandet av unionens restriktiva åtgärder och nationella restriktiva åtgärder enligt förordning (EU) 2023/1113

1. Efterlevnads- och rapporteringsskyldigheter

Riktlinjernas status

1. Detta dokument innehåller riktlinjer som har utfärdats i enlighet med artikel 16 i förordning (EU) nr 1093/2010[7]. I enlighet med artikel 16.3 i förordning (EU) nr 1093/2010 ska de behöriga myndigheterna, betaltjänstleverantörer och leverantörer av kryptotillgångstjänster med alla tillgängliga medel söka följa dessa riktlinjer.

2. I riktlinjerna fastställs EBA:s syn på lämplig tillsynspraxis inom det europeiska systemet för finansiell tillsyn och hur unionsrätten bör tillämpas inom ett särskilt område. Behöriga myndigheter enligt definitionen i artikel 4.2 i förordning (EU) nr 1093/2010 som berörs av riktlinjerna bör följa dem genom att på lämpligt sätt införliva dem i sin praxis (till exempel genom att ändra sina rättsliga ramar eller tillsynsprocesser), även när riktlinjerna i första hand riktas till finansiella institut.

Rapporteringskrav

3. Enligt artikel 16.3 i förordning (EU) nr 1093/2010 måste de behöriga myndigheterna meddela EBA om de följer eller avser att följa dessa riktlinjer, alternativt ange skälen till att de inte gör det, senast 11.04.2025. Om någon sådan anmälan inte inkommer inom denna tidsfrist kommer EBA att anse att de behöriga myndigheterna inte följer riktlinjerna. Anmälningarna ska lämnas in via det formulär som tillhandahålls på EBA:s webbplats, med hänvisningen EBA/GL/2024/15. Anmälningarna bör lämnas in av personer som på sina behöriga myndigheters vägnar har befogenhet att rapportera om hur riktlinjerna tillämpas. Alla förändringar i graden av efterlevnad måste också rapporteras till EBA.

4. Anmälningarna kommer att offentliggöras på EBA:s webbplats i enlighet med artikel 16.3.

[7] 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).

2. Syfte, tillämpningsområde och definitioner

Syfte och tillämpningsområde

5. I dessa riktlinjer anges de interna strategier, förfaranden och kontroller som betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör införa för att säkerställa ett effektivt genomförande av unionens restriktiva åtgärder och nationella restriktiva åtgärder vid överföringar av medel och kryptotillgångar i enlighet med Europaparlamentets och rådets förordning (EU) 2023/1113[8].

Målgrupp

6. Dessa riktlinjer riktar sig till

   a. behöriga myndigheter som ansvarar för tillsynen av betaltjänstleverantörer och leverantörer av kryptotillgångstjänster med avseende på efterlevnad av deras skyldigheter enligt förordning (EU) 2023/1113,

   b. finansiella institut enligt definitionen i artikel 4.1 i förordning (EU) nr 1093/2010 som är betaltjänstleverantörer enligt definitionen i artikel 3.5 i förordning (EU) 2023/1113 och leverantörer av kryptotillgångstjänster enligt definitionen i artikel 3.15 i förordning (EU) 2023/1113.

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

Definitioner

7. Termer som används och definieras i förordning (EU) 2023/1113 har samma betydelse i dessa riktlinjer. I dessa riktlinjer gäller dessutom följande definitioner:

restriktiva åtgärder	unionens restriktiva åtgärder enligt definitionen i artikel 2.1 i direktiv (EU) 2024/1226 och nationella restriktiva åtgärder som antagits av medlemsstaterna i enlighet med deras nationella rättsordning (i den mån de är tillämpliga på finansiella institut).
riktade ekonomiska sanktioner	frysning av tillgångar och förbud mot att ställa medel eller andra tillgångar till förfogande, direkt eller indirekt, till förmån för förtecknade personer och enheter enligt rådsbeslut som antas på grundval av artikel 29 i EU-fördraget och rådsförordningar som antas på grundval av artikel 215 i EUF-fördraget.
sektoriella sanktioner	restriktiva åtgärder såsom embargon på vapen och tillhörande utrustning eller ekonomiska och finansiella åtgärder (till exempel import- och exportrestriktioner och restriktioner för tillhandahållande av vissa tjänster, såsom banktjänster).

3. Genomförande

Datum för tillämpning

8. Dessa riktlinjer gäller från den 30 december 2025.

4. Riktlinjer för interna strategier, förfaranden och kontroller för att säkerställa genomförandet av unionens restriktiva åtgärder och nationella restriktiva åtgärder enligt förordning (EU) 2023/1113

Allmänna bestämmelser

1. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör införa strategier, förfaranden och kontroller för att kunna följa restriktiva åtgärder. Sådana strategier, förfaranden och kontroller bör följa EBA:s riktlinjer för interna strategier, förfaranden och kontroller för att säkerställa genomförandet av unionens restriktiva åtgärder och nationella restriktiva åtgärder (EBA/GL/2024/14).

2. Dessa strategier, förfaranden och kontroller bör göra det möjligt för betaltjänstleverantörer och leverantörer av kryptotillgångstjänster att identifiera personer som är föremål för restriktiva åtgärder. De bör också göra det möjligt för betaltjänstleverantörer och leverantörer av kryptotillgångstjänster att vidta nödvändiga åtgärder för att säkerställa att de inte ställer några medel eller kryptotillgångar till dessa personers förfogande, att de inte utför finansiella transaktioner eller tjänster som är förbjudna enligt restriktiva åtgärder och att de hanterar risker för kringgående av restriktiva åtgärder.

4.1 Screening av restriktiva åtgärder

3. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör införa ett effektivt screeningssystem för att på ett tillförlitligt sätt identifiera dem som är föremål för restriktiva åtgärder, vilket specificeras närmare i avsnitt 4.4.

4.1.1 Val av screeningssystem

4. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör använda sin exponeringsbedömning avseende restriktiva åtgärder för att besluta vilket screeningssystem som de kommer att använda, eller för att validera det screeningssystem som de använder, för att följa tillämpliga restriktiva åtgärder. Screeningssystemet bör anpassas till storleken, arten

och komplexiteten i den verksamhet som betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bedriver och dess exponering för restriktiva åtgärder.

5. När betaltjänstleverantörer och leverantörer av kryptotillgångstjänster fattar beslut om sina screeningssystem bör de överväga om de har tillgång till de resurser som krävs för att använda det valda systemet på ett effektivt sätt.

6. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör regelbundet se över screeningssystemets prestanda för att säkerställa att det förblir effektivt och fortsätter att på ett tillförlitligt sätt identifiera dem som är föremål för restriktiva åtgärder. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör genomföra en översyn av det använda screeningssystemet minst en gång per år och omedelbart om de misstänker att systemet inte är ändamålsenligt.

7. Enligt artikel 8 i förordning (EU) 2022/2554 bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster förstå och dokumentera screeningssystemets kapacitet och begränsningar. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör kunna visa för sin behöriga myndighet att deras screeningssystem fungerar på ett tillfredsställande sätt.

4.1.2 Förteckningshantering

8. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör i sina strategier och förfaranden ange vilka restriktiva åtgärder som de måste tillämpa.

9. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör ha strategier och förfaranden för att

    a. identifiera när en ny uppsättning restriktiva åtgärder antas eller en befintlig restriktiv åtgärd uppdateras eller upphävs,
    b. uppdatera sina interna dataset som ska screenas i enlighet med avsnitt 4.1.3 omedelbart efter det att en ny restriktiv åtgärd träder i kraft eller en befintlig restriktiv åtgärd uppdateras eller upphävs.

4.1.3 Fastställande av den uppsättning data som ska screenas

10. I sina strategier och förfaranden bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster fastställa vilka typer av data som de kommer att screena för varje typ av restriktiv åtgärd, med beaktande av resultatet av deras exponeringsbedömning avseende restriktiva åtgärder och de restriktiva åtgärder som de måste tillämpa.

11. När betaltjänstleverantörer och leverantörer av kryptotillgångstjänster fattar beslut om den uppsättning data som ska screenas i enlighet med typen av tillämplig restriktiv åtgärd bör de beakta alla data som de innehar om sina kunder, inbegripet information som erhållits

a. vid tillämpning av åtgärder för kundkännedom i enlighet med unionsrätten och nationell rätt som införlivar unionsrätten,
b. i enlighet med förordning (EU) 2023/1113.

12. I enlighet med kraven i förordning (EU) 2023/1113 bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bedöma huruvida de data som de innehar är tillräckligt korrekta, aktuella och detaljerade för att de ska kunna avgöra om en part i överföringen, deras verkliga huvudman eller en person som påstår sig ha eller har tillstånd att agera på deras vägnar, är föremål för restriktiva åtgärder.

13. För att undvika upprepade falska larm om fysiska eller juridiska personer, enheter eller organ som inte är föremål för restriktiva åtgärder men som felaktigt har fastställts vara det av det befintliga screeningssystemet, får betaltjänstleverantörer och leverantörer av kryptotillgångstjänster besluta att inkludera sådana personer, enheter eller organ i en särskild intern förteckning (vitlistning). Skälen för ett sådant beslut ska dokumenteras. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör se över en sådan förteckning omedelbart efter det att en ny eller ändrad restriktiv åtgärd har trätt i kraft, eller om kundinformationen har ändrats.

4.1.4 Screening av kundbasen

14. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör i sina strategier och förfaranden ange hur de kommer att screena sin kundbas.

15. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör regelbundet screena hela sin kunddatabas och fastställa frekvensen för denna kundscreening på grundval av sin exponeringsbedömning avseende restriktiva åtgärder.

16. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör i ett internt beslut fastställa vilka händelser som alltid bör leda till kundscreening och se till att sådana beslut hålls uppdaterade. Sådana händelser bör åtminstone omfatta följande:

a. Vid ändring av någon av de befintliga förteckningsuppföringarna eller restriktiva åtgärderna, en ny förteckningsuppföring eller ikraftträdandet av en ny restriktiv åtgärd.
b. Vid etablering av affärsförbindelser med nya kunder eller innan en affärsförbindelse har upprättats.
c. Vid väsentliga ändringar i en befintlig kunds data gällande åtgärder för kundkännedom, till exempel ändring av namn, hemvist, nationalitet eller affärsverksamhet.
d. Om det finns rimliga skäl att misstänka att kunden, eller någon person som påstår sig ha eller har tillstånd att agera på kundens vägnar, försöker kringgå de restriktiva åtgärderna.

17. I linje med de tillämpliga restriktiva åtgärderna bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster åtminstone screena följande kundinformation:

a. När det gäller fysiska personer:

   a. För- och efternamn, i originalform och/eller translittererad form.
   b. Födelsedatum.
b. När det gäller juridiska personer: den juridiska personens namn, i originalform och/eller translittererad form.
c. När det gäller fysiska eller juridiska personer, enheter eller organ: alla andra namn, alias, företagsnamn, plånboksadresser, om sådana finns tillgängliga, i förteckningarna över restriktiva åtgärder. Genom exponeringsbedömningen avseende restriktiva åtgärder bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster motivera valet att inte screena sådan information om den finns tillgänglig.

18. Vid screening av kunder som är juridiska eller fysiska personer, organ eller enheter bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster, i den mån denna information är tillgänglig, även screena

    a. verkliga huvudmän genom ägarintresse,
    b. verkliga huvudmän genom kontroll,
    c. varje person som påstår sig ha eller har tillstånd att agera på kundens vägnar.

4.1.5 Screening av överföringar av medel och kryptotillgångar

19. Utom i de fall som omfattas av artikel 5d i förordning (EU) nr 260/2012 bör betaltjänstleverantörer screena överföringar av medel innan de gör medlen tillgängliga för betalningsmottagaren, och leverantörer av kryptotillgångstjänster bör screena alla överföringar av kryptotillgångar innan de gör kryptotillgångarna tillgängliga för mottagaren, oavsett om de utförs som en del av en affärsförbindelse eller som en del av en engångstransaktion.

20. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör screena alla parter i överföringar av medel eller kryptotillgångar mot tillämpliga restriktiva åtgärder. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör i sin exponeringsbedömning avseende restriktiva åtgärder ägna särskild uppmärksamhet åt sundheten och tillförlitligheten hos de strategier och förfaranden för restriktiva åtgärder som införts av betaltjänstleverantörer och leverantörer av kryptotillgångstjänster, med vilka de bedriver affärsverksamhet, för att säkerställa att de restriktiva åtgärderna efterlevs.

21. Alla data som kan vara relevanta för bedömningen av huruvida en transaktion kan påverkas av tillämpliga restriktiva åtgärder bör screenas mot tillämpliga restriktiva åtgärder. De data som ska screenas bör åtminstone omfatta följande:

    a. Uppgifter om betalaren och betalningsmottagaren i enlighet med artikel 4 i förordning (EU) 2023/1113.
    b. Uppgifter om avsändaren och mottagaren i enlighet med artikel 14 i förordning (EU) 2023/1113.
    c. Syftet med överföringen av medel eller kryptotillgångar och, om uppgifter finns tillgängliga och om de omfattas av exponeringsbedömningen avseende restriktiva

åtgärder, andra fritextfält som ger ytterligare information om den faktiska avsändaren/mottagaren av medel eller kryptotillgångar.

d. Uppgifter om de betaltjänstleverantörer och leverantörer av kryptotillgångstjänster som deltar i överföringen av medel eller kryptotillgångar, inbegripet förmedlande institut och korrespondenter, med screening av identifieringskoder såsom BIC, Swift och andra.
e. Andra uppgifter om överföringen av medel eller kryptotillgångar, beroende på transaktionens art och typ samt de styrkande handlingar som mottagits, om uppgifter finns tillgängliga och om de omfattas av exponeringsbedömningen avseende restriktiva åtgärder.
f. Plånboksadresser för avsändaren och mottagaren av en överföring av kryptotillgångar, i den mån denna information finns tillgänglig i officiella förteckningar över plånboksadresser kopplade till restriktiva åtgärder.

22. I enlighet med bestämmelserna i avsnitt 4.6 i EBA:s riktlinjer (EBA/GL/2024/11) om informationskrav i samband med överföringar av medel och vissa överföringar av kryptotillgångar enligt förordning (EU) 2023/1113 (”riktlinjer för reseregeln”), bör all ny information som erhålls i ett senare skede, före eller efter det att överföringen verkställs, också screenas.

23. När så är lämpligt, på grundval av volym och antal gällande överföringar av kryptotillgångar, bör leverantörer av kryptotillgångstjänster överväga att införliva blockkedjeanalys för transaktionsövervakningsändamål i den befintliga ramen.

4.1.6 Kalibrering

24. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör fastställa hur inställningarna i ett automatiskt screeningssystem ska kalibreras för maximal larmkvalitet och otvetydig identifiering, samtidigt som efterlevnaden av restriktiva åtgärder säkerställs. På grundval av exponeringsbedömningen avseende restriktiva åtgärder och regelbundna tester bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster åtminstone göra följande:

a. För varje tillämplig restriktiv åtgärd fastställa lämpliga parametrar för matchning, vilka sannolikt kommer att generera ett rimligt larm som gör det möjligt för betaltjänstleverantörer och leverantörer av kryptotillgångstjänster att fullgöra sina skyldigheter vad gäller restriktiva åtgärder, genom att kontrollera tröskelvärdena för sanna positiva resultat i samband med olika matchningsprocentandelar. Kalibreringens känslighetsnivå bör varken vara för hög, vilket leder till ett stort antal falska positiva matchningar, eller för låg, vilket leder till att förtecknade personer, enheter och organ inte upptäcks eller till att information i fritext inte används för andra restriktiva åtgärder.
b. Använda ett screeningssystem som möjliggör algoritmbaserad teknik som kan matcha ett namn eller en ordsträng, där innehållet i den information som screenas inte är

identiskt, men dess stavning, mönster eller ljud stämmer nära överens med innehållet i det dataset som används för screening (tekniker för ”fuzzy matching” [ungefärlig matchning]) och kalibrera graden av fuzzy matching i sina screeningssystem.

25. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör besluta om kalibreringen både innan de utvecklar ett nytt screeningssystem och sedan på regelbunden basis, i linje med exponeringsbedömningen avseende restriktiva åtgärder. De bör dokumentera sin motivering och på begäran göra den tillgänglig för behöriga myndigheter.

4.1.7 Anlitande av tredje parter och utkontraktering

26. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör i sina strategier och förfaranden ange vilka åtgärder som ska vidtas av betaltjänstleverantörerna, av leverantörerna av kryptotillgångstjänster eller av tjänsteleverantörer till vilka tjänster har utkontrakterats, för att säkerställa efterlevnad av tillämpliga restriktiva åtgärder. Vid utkontraktering av tjänster bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster, med beaktande av riktlinjerna EBA/GL/2019/02 i tillämpliga fall[9], tillämpa följande huvudprinciper:

    a. Det yttersta ansvaret för efterlevnaden av restriktiva åtgärder, oavsett om specifika funktioner utkontrakteras eller inte, ligger hos betaltjänstleverantörerna eller leverantörerna av kryptotillgångstjänster.
    b. Rättigheterna och skyldigheterna för betaltjänstleverantörerna eller leverantörerna av kryptotillgångstjänster samt för tjänsteleverantören bör vara tydligt fördelade och fastställda i skriftlig form.
    c. De betaltjänstleverantörer eller leverantörer av kryptotillgångstjänster som förlitar sig på ett utkontrakteringsavtal bör förbli ansvariga för att övervaka och kontrollera kvaliteten på den tjänst som tillhandahålls av tjänsteleverantören.
    d. Koncernintern utkontraktering bör omfattas av samma regelverk som om utkontraktering skett till tjänsteleverantörer utanför koncernen.

27. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör införa och tillämpa de kontroller som krävs för att säkerställa att utkontraktering av tjänster till tjänsteleverantörer inte utsätter dem för risken för överträdelse av restriktiva åtgärder, och dokumentera dessa kontroller i utkontrakteringsavtalet.

28. Om tjänsteleverantörer ansvarar för att uppdatera data som ska användas av betaltjänstleverantörer och leverantörer av kryptotillgångstjänster om fysiska eller juridiska personer, enheter och organ som omfattas av tillämpliga restriktiva åtgärder, bör betaltjänstleverantörerna och leverantörerna av kryptotillgångstjänster säkerställa att ett tjänsteavtal minimerar risken för att de bryter mot restriktiva åtgärder.

29. När utkontrakteringsavtal ingåtts bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster regelbundet kontrollera att tjänsteleverantören fullgör de skyldigheter

[9] EBA:s riktlinjer för utkontraktering (EBA/GL/2019/02).

som följer av avtalet, bedöma effektiviteten hos de tjänster som omfattas av avtalet och vidta nödvändiga riskreducerande åtgärder, inbegripet omförhandling av avtalet.

30. Bestämmelserna i detta avsnitt påverkar inte de skyldigheter och uppgifter som betaltjänstleverantörer och leverantörer av kryptotillgångstjänster tillskrivs när det gäller digital operativ motståndskraft enligt förordning (EU) 2022/2554[10].

4.2 Åtgärder för tillbörlig aktsamhet (due diligence) och verifieringsåtgärder för analys av larm

4.2.1 Strategier och förfaranden för hantering och analys av larm

31. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör ha strategier och förfaranden för att utreda larm i samband med restriktiva åtgärder. Dessa strategier och förfaranden bör göra det möjligt för betaltjänstleverantörer och leverantörer av kryptotillgångstjänster att bekräfta huruvida ett larm utgör en sann positiv matchning och, om så är fallet, fastställa vilka åtgärder som krävs för att följa den tillämpliga restriktiva åtgärden.

32. Sådana strategier och förfaranden bör omfatta följande:

    a. Åtgärder för att utan dröjsmål börja utreda alla potentiella matchningar, för varje överföring av medel eller överföring av kryptotillgångar.
    b. Regler i enlighet med de allmänna riktlinjer för dokumentation som gäller för betaltjänstleverantörerna och leverantörerna av kryptotillgångstjänster, för dokumentation av alla beslut som fattas avseende larm.
    c. Åtgärder för att följa avsnitt 4.2.2 i dessa riktlinjer.
    d. Olika nivåer av översyn som ska genomföras i linje med exponeringsbedömningen avseende restriktiva åtgärder, där situationer med högre exponering ska vara föremål för översyn av minst två personer.

4.2.2 Åtgärder för tillbörlig aktsamhet vid analys av larm

33. Det larm som genereras av screeningssystemet bör ange vilken del i den respektive restriktiva åtgärden som den avser. Larmen bör analyseras av personal som har nödvändig expertis och som har fått tillräcklig utbildning[11].

34. Om det råder tvivel om huruvida en matchning är korrekt bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster använda ytterligare uppgifter som står till deras förfogande och/eller som de kan erhålla till stöd för analysen av larmen, i den mån dessa uppgifter finns tillgängliga, såsom

[10] Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (Text av betydelse för EES), EUT L 333, 27.12.2022, s. 1.

[11] Se avsnitt 4.4 i riktlinjerna för interna strategier, förfaranden och kontroller för att säkerställa genomförandet av unionens restriktiva åtgärder och nationella restriktiva åtgärder.

a. identifieringsuppgifter för fysiska eller juridiska personer, enheter eller organ som inte använts i screeningsstadiet,
b. uppgifter om fysiska personers hemvist och uppgifter om säte eller registrerad adress för juridiska personer, enheter eller organ som inte använts i screeningsstadiet,
c. uppgifter om nationalitet och medborgarskap för fysiska personer som inte använts i screeningsstadiet,
d. uppgifter om företrädare, ledning och organisationsstruktur för juridiska personer som inte använts i screeningsstadiet,
e. kontaktuppgifter som inte använts i screeningsstadiet.

35. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör i sina strategier och förfaranden ange hur de ska hantera fall där det inte är möjligt att efter ytterligare tillbörlig aktsamhet otvetydigt fastställa att en matchning är sant positiv eller falskt positiv, eller om det rör sig om en situation med homonymer. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör avstå från att tillhandahålla finansiella tjänster till en part i en överföring innan de har fattat ett välgrundat beslut.

4.2.3 Bedömning av om en enhet ägs eller kontrolleras av en förtecknad person

36. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör i sina strategier och förfaranden ange hur de kommer att bedöma om en juridisk person eller enhet ägs eller kontrolleras av en förtecknad person eller enhet.

37. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör

a. tillämpa de kriterier som anges i rådets riktlinjer för sanktioner[12] och i avsnitt VIII i rådets bästa praxis[13] för att avgöra om en juridisk person ägs eller kontrolleras av en annan person eller enhet,
b. tillämpa de kriterier som används för att identifiera en verklig huvudman enligt tillämplig lagstiftning[14],
c. använda tillgängliga offentliga informationskällor, såsom register över ägda och kontrollerade enheter och register över verkliga huvudmän.

38. Om en bedömning förblir ofullständig bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster överväga att samarbeta med den nationella myndighet som är behörig att genomföra restriktiva åtgärder. Det yttersta ansvaret för efterlevnaden av restriktiva åtgärder ligger hos betaltjänstleverantörerna och leverantörerna av kryptotillgångstjänster.

4.2.4 Kontroller och åtgärder för tillbörlig aktsamhet för att följa sektoriella sanktioner

[12] https://data.consilium.europa.eu/doc/document/ST-11618-2024-INIT/en/pdf, Bryssel, 2 juli 2024, 11618/24 (uppdatering).

[13] Uppdatering av EU:s bästa praxis för effektivt genomförande av restriktiva åtgärder (dok. 11623/24).

[14] Artikel 3.6 i direktiv (EU) 2015/849.

39. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör ta hänsyn till exponeringsbedömningen avseende restriktiva åtgärder när de fastställer vilka typer av kontroller som de kommer att tillämpa för att följa restriktiva åtgärder. Som en del av detta bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster fastställa vilka tillgängliga uppgifter med anknytning till en transaktion som kommer att screenas.

40. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör vara särskilt uppmärksamma på sektoriella sanktioner som kan kopplas till en viss jurisdiktion eller ett visst territorium. Inom ramen för sådana restriktiva åtgärder bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster screena alla underliggande uppgifter avseende överföringen av medel eller kryptotillgångar till eller från den specifika jurisdiktionen eller det specifika territoriet, eller avseende överföringar av medel eller kryptotillgångar som initierats av kunder som bedriver verksamhet i den specifika jurisdiktionen eller på det specifika territoriet. I den mån detta är tillgängligt bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster screena

    a. uppgifter om medborgarskapsland samt uppgifter om födelseort,
    b. uppgifter om stadigvarande hemvist eller huvudsakligt verksamhetsställe på grundval av andra adresser, i enlighet med exponeringsbedömningen avseende restriktiva åtgärder,
    c. uppgifter om det land till eller från vilket överföringen av medel genomförs, om överföringen av medel har verkställts,
    d. syftet med överföringen av medel eller kryptotillgångar och andra fritextfält som ger ytterligare information om varor, fartyg och destinationsland eller ursprungsland för de varor som betalningen omfattar, i enlighet med exponeringsbedömningen avseende restriktiva åtgärder.

41. Om det är motiverat av exponeringsbedömningen avseende restriktiva åtgärder bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster i sina screeningssystem överväga att införliva geolokaliseringsverktyg och verktyg för att upptäcka användningen av proxytjänster, för att identifiera och förhindra att IP-adresser som härrör från ett land som omfattas av restriktiva åtgärder, på grund av en situation som påverkar det landet, får åtkomst till deras webbplatser och tjänster, med avseende på en verksamhet som är förbjuden enligt systemen för restriktiva åtgärder.

42. I enlighet med exponeringsbedömningen avseende restriktiva åtgärder kan betaltjänstleverantörer och leverantörer av kryptotillgångstjänster överväga att tillämpa särskilda kontroller, såsom att

    a. vid upprättande av en affärsförbindelse, inhämta relevanta uppgifter om kundens typ av verksamhet och de länder där kunden bedriver verksamhet,
    b. begära ytterligare uppgifter från kunden, såsom en beskrivning av varor med dubbla användningsområden eller varor som omfattas av sektoriella sanktioner, uppgifter om lämpliga tillstånd för att hantera varor med dubbla användningsområden samt uppgifter om varornas ursprungsland och slutanvändare,

c. begära mer detaljerade uppgifter från kunden om syftet med en överföring av medel eller kryptotillgångar,
d. använda följande data: fartygsregister, fastighetsregister och andra dataset som är allmänt tillgängliga (i förekommande fall).

43. Om betaltjänstleverantörer och leverantörer av kryptotillgångstjänster använder funktioner för att automatiskt läsa information från dokument som rör överföringen av medel eller kryptotillgångar, såsom algoritmer för optisk teckenigenkänning eller maskinläsbara verifieringsfält, bör de vidta nödvändiga åtgärder för att säkerställa att dessa verktyg samlar in information på ett korrekt och konsekvent sätt.

4.2.5 Åtgärder för tillbörlig aktsamhet för upptäckt av försök till kringgående av restriktiva åtgärder

44. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör hålla sig informerade om typologier och trender när det gäller kringgående av restriktiva åtgärder. Relevanta informationskällor som betaltjänstleverantörer och leverantörer av kryptotillgångstjänster alltid bör hänvisa till omfattar åtminstone rapporter som delas av

a. relevanta nationella myndigheter som är behöriga att genomföra restriktiva åtgärder[15] och/eller nationella tillsynsmyndigheter,
b. finansunderrättelseenheter och brottsbekämpande myndigheter,
c. relevanta offentlig-privata partnerskap på nationell nivå eller EU-nivå,
d. EU-myndigheter[16].

45. Strategier och förfaranden för tillbörlig aktsamhet bör göra det möjligt för betaltjänstleverantörer och leverantörer av kryptotillgångstjänster att upptäcka eventuella försök att kringgå restriktiva åtgärder, såsom försök att

a. utelämna, radera eller ändra information i betalningsmeddelanden,
b. göra överföringar genom personer med anknytning till en kund som är föremål för restriktiva åtgärder,
c. strukturera överföringar av medel eller kryptotillgångar för att dölja en förtecknad parts inblandning,
d. dölja den verkliga huvudmannen eller kontrollen av tillgångar,
e. använda förfalskad eller bedräglig bakgrundsdokumentation för överföring av medel eller kryptotillgångar.

46. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster som är särskilt utsatta för risken att användas för kringgående bör också överväga att genomföra en aggregerad analys

[15] https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/overview-sanctions-and-related-resources_en#contact.

[16] Se exempelvis https://finance.ec.europa.eu/news/sanctions-commission-publishes-guidance-help-european-operators-assess-sanctions-circumvention-risks-2023-09-07_en.

av betalningsflödena till eller från länder som är föremål för restriktiva åtgärder och länder som är kända för att användas för att kringgå restriktiva åtgärder.

4.3 Åtgärder för frysning och rapportering

4.3.1 Avbryta genomförandet av överföringar av medel och frysning av tillgångar

47. Betaltjänstleverantörer bör ha strategier och förfaranden för att utan dröjsmål avbryta verksamhet som utlöser ett larm med en eventuell matchning som avser en förtecknad person eller enhet, eller en person eller enhet som ägs, innehas eller kontrolleras av en förtecknad person eller enhet, eller där den verkliga huvudmannen är en förtecknad person.

48. Om betaltjänstleverantörernas interna analys av ett sådant larm bekräftar att den eventuella matchningen avser en förtecknad person eller enhet, eller en person eller enhet som ägs, innehas eller kontrolleras av en förtecknad person eller enhet, eller att den verkliga huvudmannen är en förtecknad person, bör betaltjänstleverantörerna omedelbart

    a. frysa motsvarande medel,
    b. stoppa överföringar av medel som skulle innebära en överträdelse av restriktiva åtgärder.

4.3.2 Frysning av överföringar av kryptotillgångar

49. Leverantörer av kryptotillgångstjänster bör ha strategier och förfaranden för de situationer då deras interna analys av ett larm bekräftar att den eventuella matchningen avser en förtecknad person eller enhet, eller en person eller enhet som ägs, innehas eller kontrolleras av en förtecknad person eller enhet, eller att den verkliga huvudmannen är en förtecknad person, i syfte att omedelbart kunna frysa och blockera tillgångarna på ett bevakningskonto tills den relevanta nationella myndighet som är behörig att genomföra restriktiva åtgärder ger leverantören av kryptotillgångstjänster vidare instruktioner om vilka åtgärder som ska vidtas för dessa medel. Det yttersta ansvaret för efterlevnaden av restriktiva åtgärder ligger hos leverantören av kryptotillgångstjänster.

4.3.3 Åtgärder för rapportering

50. Enligt tillämpliga unionskrav och nationella krav bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster ha tydliga processer för att till den relevanta nationella myndighet som är behörig att genomföra restriktiva åtgärder och/eller till den behöriga tillsynsmyndigheten, utan dröjsmål eller inom en angiven tidsfrist, rapportera om följande:

    a. Alla åtgärder som vidtagits för en specifik överföring i samband med en restriktiv åtgärd.
    b. Upptäckten av en överträdelse av restriktiva åtgärder.
    c. Genomförandet av överföringar av medel eller kryptotillgångar som innebär en överträdelse av en tillämplig restriktiv åtgärd, genom att tillhandahålla information om omständigheterna, såsom en incident avseende screeningssystemets funktion i samband med en sådan överföring.

51. Vid misstanke om ett eventuellt kringgående av restriktiva åtgärder eller vid upptäckt av ett försök att överföra medel eller kryptotillgångar av eller till fysiska eller juridiska personer, enheter eller organ, bör betaltjänstleverantörer och leverantörer av kryptotillgångstjänster

    a. rapportera detta till den relevanta nationella myndighet som är behörig att genomföra restriktiva åtgärder, om detta särskilt krävs i en EU-förordning om restriktiva åtgärder,
    b. lämna in en rapport om den misstänkta transaktionen om så krävs enligt tillämplig lagstiftning.

4.3.4 Förfaranden för undantag eller upphävande av restriktiva åtgärder

52. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör ha strategier och förfaranden för att kunna avgöra om dispenser, tillståndssystem eller undantag är tillämpliga och, om så är fallet, hur de ska gå vidare för att följa tillämplig unionsrätt eller nationell rätt. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör i sina strategier och förfaranden ange vilken information de kommer att ge till kunder som lämnar in en begäran om undantag att använda sina frysta tillgångar, om sådana undantag är tillåtna enligt den

tillämpliga rättsliga ramen. Denna information bör innehålla uppgifter om kundens rättigheter i en sådan situation.

53. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör ha strategier och förfaranden där det fastställs hur medel och kryptotillgångar som omfattas av särskilda restriktiva åtgärder ska hanteras då en sådan åtgärd upphävs.

4.4 Säkerställa löpande effektivitet avseende strategier, förfaranden och system för screening av restriktiva åtgärder

54. För att vara effektiva bör de strategier, förfaranden och system som betaltjänstleverantörer och leverantörer av kryptotillgångstjänster har för screening av restriktiva åtgärder göra det möjligt att

    a. på ett tillförlitligt sätt upptäcka positiva matchningar,
    b. vid bekräftelse av positiva matchningar, omedelbart avbryta genomförandet av alla överföringar av medel, blockera alla inkommande överföringar och deponera dem på ett bevakningskonto, frysa tillgångarna eller kryptotillgångarna utan dröjsmål och rapportera detta till den relevanta nationella myndighet som är behörig att genomföra restriktiva åtgärder för ytterligare anvisningar,
    c. rapportera frysta tillgångar till de relevanta nationella myndigheter som är behöriga att genomföra restriktiva åtgärder och/eller till den behöriga tillsynsmyndigheten enligt tillämplig lagstiftning, utan dröjsmål eller inom de tidsfrister som fastställs i tillämplig unionsrätt eller nationell rätt,
    d. rapportera misstanke om kringgående eller försök till kringgående av restriktiva åtgärder till den relevanta nationella myndighet som är behörig att genomföra restriktiva åtgärder eller till den nationella finansunderrättelseenheten, om så krävs enligt tillämplig lagstiftning.

55. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör regelbundet testa inställningarna i screeningssystemet för att avgöra om det fortfarande är lämpligt mot bakgrund av exponeringsbedömningen avseende restriktiva åtgärder, och att det fortfarande är effektivt. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör fastställa kontrollfrekvensen på grundval av exponeringsbedömningen avseende restriktiva åtgärder och föra in detta i sina strategier och förfaranden.

56. När betaltjänstleverantörer och leverantörer av kryptotillgångstjänster testar sina screeningssystem bör de

    a. testa kalibreringen av screeningssystemet i enlighet med avsnitt 4.1.6,
    b. bedöma förteckningshanteringens korrekthet utifrån tillämpliga och aktuella restriktiva åtgärder,
    c. bedöma om alla kunder och överföringar av medel och kryptotillgångar screenas när så krävs,

d. bedöma lämpligheten och relevansen hos de informationsfält som används i screeningssystemet, såsom omfattningen av de överföringar av medel eller kryptotillgångar som matas in i screeningssystemet,
e. bedöma om det automatiska verksamhetsavbrottet sker i rätt tid,
f. bedöma om de processer och resurser som finns tillgängliga för analys av larm gör det möjligt att skyndsamt rapportera matchningar som är sant positiva.

57. Betaltjänstleverantörer och leverantörer av kryptotillgångstjänster bör till ledningsorganet rapportera betydande svagheter eller brister som identifierats i screeningssystemet och utan dröjsmål vidta korrigerande åtgärder.