ABE/GL/2022/15

22/11/2022

Orientamenti

sull'utilizzo di soluzioni di onboarding a distanza del cliente per le finalità di cui all'articolo 13, paragrafo 1, della direttiva (UE) 2015/849

1. Conformità e obblighi di notifica

Status giuridico degli orientamenti

1. Il presente documento contiene orientamenti emanati in applicazione dell'articolo 16 del regolamento (UE) n. 1093/2010 ([1]). Conformemente all'articolo 16, paragrafo 3, del regolamento (UE) n. 1093/2010, le autorità competenti e gli enti creditizi e gli istituti finanziari compiono ogni sforzo per conformarsi ai presenti orientamenti.

2. Gli orientamenti definiscono la posizione dell'ABE in merito alle prassi di vigilanza adeguate all'interno del Sistema europeo di vigilanza finanziaria o alle modalità di applicazione del diritto dell'Unione in un particolare settore. Le autorità competenti di cui all'articolo 4, punto 2), del regolamento (UE) n. 1093/2010 cui si applicano gli orientamenti dovrebbero conformarsi agli orientamenti integrandoli opportunamente nelle rispettive prassi (ad esempio modificando il proprio quadro giuridico o le proprie procedure di vigilanza), anche quando gli orientamenti sono diretti principalmente agli enti.

Obblighi di notifica

3. Ai sensi dell'articolo 16, paragrafo 3, del regolamento (UE) n. 1093/2010, le autorità competenti devono notificare all'ABE entro il 30.05.2023 se sono conformi o se intendono conformarsi agli orientamenti in questione; in alternativa sono tenute a indicare le ragioni della mancata conformità. Qualora entro il termine indicato non sia pervenuta alcuna notifica da parte delle autorità competenti, queste sono ritenute dall'ABE non conformi. Le notifiche dovrebbero essere inviate trasmettendo il modulo disponibile sul sito web dell'ABE con il riferimento «EBA/GL/2022/15» da persone debitamente autorizzate a segnalare la conformità per conto delle rispettive autorità competenti. Ogni eventuale variazione dello status di conformità deve essere altresì comunicata all'ABE.

4. Le notifiche sono pubblicate sul sito web dell'ABE ai sensi dell'articolo 16, paragrafo 3.

([1]) Regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità bancaria europea), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/78/CE della Commissione (GU L 331 del 15.12.2010, pag. 12).

2. Oggetto, ambito di applicazione e definizioni

Oggetto e ambito di applicazione

5. I presenti orientamenti illustrano le misure che gli enti creditizi e gli istituti finanziari dovrebbero assumere al momento di adottare o rivedere soluzioni per adempiere gli obblighi di cui all'articolo 13, paragrafo 1, lettere a), b) e c), della direttiva (UE) 2015/849 ([2]) laddove acquisiscano nuovi clienti a distanza. Inoltre, indicano le misure che gli enti creditizi e finanziari dovrebbero adottare allorché ricorrono a terzi ai sensi del capo II, sezione 4, della direttiva (UE) 2015/849, nonché le politiche, i controlli e le procedure che gli enti creditizi e gli istituti finanziari dovrebbero porre in essere in relazione all'adeguata verifica della clientela di cui all'articolo 8, paragrafo 3, e paragrafo 4, lettera a), della direttiva (UE) 2015/849 nelle situazioni in cui le misure di adeguata verifica della clientela sono eseguite a distanza.

6. Le autorità competenti dovrebbero tenere conto dei presenti orientamenti nel valutare se le misure adottate dagli enti creditizi e gli istituti finanziari per adempiere gli obblighi di cui alla direttiva (UE) 2015/849 ai fini dell'adeguata verifica a distanza della clientela siano adeguate ed efficaci.

Destinatari

7. I presenti orientamenti sono destinati alle autorità competenti di cui all'articolo 4, paragrafo 2 del regolamento (UE) n. 1093/2010, nonché agli operatori del settore finanziario di cui all'articolo 4, paragrafo 1, punto a), di tale regolamento, che sono enti creditizi e istituti finanziari ai sensi dell'articolo 3, paragrafi 1 e 2, della direttiva (UE) 2015/849.

[2] Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio o finanziamento del terrorismo.

Definizioni

8. Se non diversamente specificato, i termini utilizzati e definiti nella direttiva (UE) 2015/849 hanno lo stesso significato nei presenti orientamenti. Inoltre, ai fini dei presenti orientamenti, si applicano le definizioni riportate di seguito.

Dati biometrici	Dati personali relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali immagini del volto o dati dattiloscopici, ottenuti e trattati con mezzi tecnici.

3. Attuazione

Data di applicazione

I presenti orientamenti si applicano a decorrere dal 02.10.2023.

4. Orientamenti sull'utilizzo di soluzioni di onboarding a distanza del cliente per le finalità di cui all'articolo 13, paragrafo 1, della direttiva (UE) 2015/849

4.1 Politiche e procedure interne

4.1.1 Politiche e procedure relative all'onboarding a distanza del cliente

9. Gli enti creditizi e gli istituti finanziari dovrebbero porre in essere e mantenere politiche e procedure per adempiere gli obblighi di cui all'articolo 13, paragrafo 1, lettere a) e c), della direttiva (UE) 2015/849 nelle situazioni in cui l'onboarding del cliente è eseguita a distanza. Tali politiche e procedure dovrebbero essere commisurate al rischio e includere almeno:

    a) una descrizione generale della soluzione che gli enti creditizi e gli istituti finanziari hanno posto in essere per raccogliere, verificare e conservare le informazioni nel corso di tutto il processo di onboarding a distanza del cliente. Tale descrizione dovrebbe includere una spiegazione delle caratteristiche e del funzionamento della soluzione;

    b) le situazioni in cui è possibile utilizzare la soluzione di onboarding a distanza del cliente, tenendo conto dei fattori di rischio individuati e valutati ai sensi dell'articolo 8, paragrafo 1, della direttiva (UE) 2015/849 e dell'auto valutazione del rischio di riciclaggio connesso alla propria area di attività, compresa una descrizione della categoria di clienti, prodotti e servizi per i quali è ammissibile l'onboarding a distanza;

    c) le fasi che sono completamente automatizzate e quelle che richiedono l'intervento umano;

    d) i controlli in essere per assicurare che la prima operazione con un nuovo cliente sia eseguita solo dopo l'applicazione di tutte le misure di adeguata verifica iniziale della clientela;

    e) una descrizione dei programmi di preparazione e formazione periodica tesi ad assicurare la sensibilizzazione e l'aggiornamento delle conoscenze del personale in merito al funzionamento della soluzione di onboarding a distanza del cliente, ai rischi

associati e alle politiche e procedure di onboarding a distanza del cliente volte a mitigare tali rischi.

10. Le politiche e le procedure, una volta attuate, dovrebbero consentire agli enti creditizi e agli istituti finanziari di assicurare la conformità del proprio operato alle disposizioni di cui alle sezioni da 4.2 a 4.7 dei presenti orientamenti.

4.1.2 Governance

11. In aggiunta ai compiti di cui alla sezione 4.2.4 degli orientamenti dell'ABE sul ruolo e compiti del responsabile antiriciclaggio ([3]), il responsabile antiriciclaggio ([4]), investito del dovere generale di preparare politiche e procedure per ottemperare ai requisiti di adeguata verifica della clientela, dovrebbe assicurare che le politiche e le procedure per l'onboarding a distanza del cliente siano attuate in modo efficace, riesaminate periodicamente e modificate se necessario.

12. L'organo di gestione dell'ente creditizio e dell'istituto finanziario dovrebbe approvare le politiche e le procedure di onboarding a distanza del cliente e vigilare sulla loro corretta attuazione.

4.1.3 La valutazione preliminare all'attuazione della soluzione di onboarding a distanza del cliente

13. Al momento di considerare la possibilità di adottare una nuova soluzione per l'onboarding a distanza del cliente, gli enti creditizi e gli istituti finanziari dovrebbero effettuare una valutazione preliminare all'attuazione di tale soluzione.

14. Gli enti creditizi e gli istituti finanziari dovrebbero definire l'ambito, le fasi e i requisiti di conservazione dei documenti della valutazione preliminare all'attuazione nelle loro politiche e procedure, che dovrebbe comprendere almeno:

    a) una valutazione dell'adeguatezza della soluzione in termini di completezza e accuratezza dei dati e dei documenti raccolti, nonché dell'affidabilità e dell'indipendenza delle fonti di informazione utilizzate;

    b) una valutazione dell'impatto dell'utilizzo della soluzione di onboarding a distanza del cliente sull'esposizione al rischio dell'ente o dell'istituto in relazione alla loro area di attività, compreso l'impatto sui rischi ML/TF, operativi, reputazionali e legali;

    c) l'individuazione di possibili misure di mitigazione e azioni correttive per ciascun rischio individuato nella valutazione di cui alla lettera b);

([3]) Progetto di orientamenti sulle politiche e le procedure in relazione alla gestione della conformità e al ruolo e alle responsabilità del responsabile AML/CFT ai sensi dell'articolo 8 e del capo VI della direttiva.

([4]) In conformità dei criteri di proporzionalità di cui alla sezione 4.2.2 degli orientamenti per il responsabile AML/CFT.

d) test per valutare i rischi di frode, compresi i rischi di sostituzione di persona e altri rischi legati alle tecnologie dell'informazione e della comunicazione (ICT) e alla sicurezza, in conformità con il paragrafo 43 degli orientamenti dell'ABE sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione e di sicurezza ([5]);

e) un test end-to-end del funzionamento della soluzione rispetto al cliente/ai clienti, al prodotto/ai prodotti e al servizio/ai servizi per i quali la soluzione di onboarding a distanza può essere utilizzata, secondo quanto definito nelle politiche e nelle procedure di onboarding a distanza del cliente.

15. Gli enti creditizi e gli istituti finanziari dovrebbero considerare soddisfatti i criteri di cui al paragrafo 14, lettere (a), (d) ed (e), se la soluzione utilizza uno dei seguenti elementi:

    a) regimi di identificazione elettronica notificati ai sensi dell'articolo 9 del regolamento (UE) n. 910/2014 che soddisfano i requisiti relativi a livelli di garanzia «significativi» o «elevati» ai sensi dell'articolo 8 di tale regolamento;

    b) servizi fiduciari qualificati pertinenti che soddisfano i requisiti del regolamento (UE) n. 910/2014, in particolare il capo III, sezione 3 e l'articolo 24, paragrafo 1, comma 2, lettera b), di tale regolamento.

16. Gli enti creditizi e gli istituti finanziari dovrebbero essere in grado di illustrare alla loro autorità competente di riferimento quali valutazioni abbiano effettuato prima dell'attuazione della soluzione di onboarding a distanza del cliente e il risultato delle loro valutazioni e dimostrarle che l'utilizzo della soluzione è adeguato rispetto ai rischi ML/TF individuati per i tipi di cliente/clienti, servizio/servizi, aree geografiche e prodotto/prodotti che rientrano nell'ambito di applicazione della soluzione stessa.

17. Gli enti creditizi e gli istituti finanziari dovrebbero iniziare a utilizzare una soluzione di onboarding a distanza del cliente solo dopo avere accertato la possibilità di integrarla nel loro più ampio sistema di controlli interni, consentendo loro così di gestire adeguatamente i rischi ML/TF che potrebbero derivare dall'utilizzo di tale soluzione.

4.1.4 Monitoraggio continuo della soluzione di onboarding a distanza del cliente

18. Gli enti creditizi e gli istituti finanziari dovrebbero monitorare costantemente la soluzione di onboarding a distanza del cliente per assicurare che sia in linea con le attese. Dovrebbero includere nelle politiche e le procedure di cui al paragrafo 9 una descrizione di almeno:

    a) le misure che adotteranno per accertarsi della qualità, della completezza, dell'accuratezza e dell'adeguatezza dei dati raccolti durante il processo di

([5]) EBA/GL/2019/04.

onboarding a distanza del cliente, che dovrebbero essere commisurate ai rischi ML/TF cui l'ente creditizio e finanziario è esposto;

b) l'ambito e la frequenza di tali verifiche periodiche; e

c) le circostanze che attiveranno revisioni ad hoc, che dovrebbero includere almeno:

   a. modifiche dell'esposizione ai rischi ML/TF dell'ente creditizio e finanziario;

   b. carenze nel funzionamento della soluzione rilevate nel corso di attività di monitoraggio, audit o vigilanza;

   c. un aumento percepibile dei tentativi di frode;

   d. modifiche del quadro normativo o regolamentare.

19. Gli enti creditizi e gli istituti finanziari dovrebbero definire nei propri processi e procedure misure correttive per il caso in cui si sia concretizzato un rischio o siano stati individuati errori con un impatto sull'efficienza e sull'efficacia della soluzione generale di onboarding a distanza del cliente. Tali misure dovrebbero includere almeno:

    a) una revisione di tutti i rapporti d'affari interessati, per valutare se gli enti creditizi e gli istituti finanziari hanno adottato misure di adeguata verifica iniziale della clientela sufficienti per conformarsi all'articolo 13, paragrafo 1, lettere a), b) e c), della direttiva antiriciclaggio (AML/CFT). Gli enti creditizi e gli istituti finanziari dovrebbero dare priorità ai rapporti d'affari che comportano il rischio ML/TF più elevato;

    b) tenendo conto delle informazioni ottenute nella suddetta revisione, una valutazione dell'opportunità che i rapporti continuativi interessati siano:

       a. sottoposti a ulteriori misure di adeguata verifica;

       b. sottoposti a limitazioni, ad esempio limiti al volume delle operazioni richiedibili, ove consentito dal diritto nazionale, fino a quando non sia stata effettuata una revisione;

       c. chiusi;

       d. oggetto di una segnalazione all'unità di informazione finanziaria (UIF);

       e. riclassificati in un diverso profilo di rischio.

20. Gli enti creditizi e gli istituti finanziari dovrebbero considerare il modo più efficace per monitorare nel continuo l'adeguatezza e l'affidabilità delle soluzioni di onboarding a distanza del cliente. Dovrebbero considerare, a titolo esemplificativo ma non esaustivo, uno o più dei seguenti strumenti:

i. test di garanzia della qualità;

ii. segnalazioni e notifiche automatizzate di criticità;

iii. relazioni periodiche automatizzate sulla qualità;

iv. test a campione;

v. revisioni manuali.

21. Questa sezione si applica anche nel caso in cui siano utilizzate soluzioni di onboarding a distanza del cliente completamente automatizzate che dipendono in larga misura da algoritmi automatizzati, con intervento umano limitato o assente.

22. Gli enti creditizi e gli istituti finanziari dovrebbero essere in grado di dimostrare alla rispettiva autorità competente le revisioni effettuate e le misure correttive adottate per ovviare alle eventuali carenze individuate durante l'intero ciclo di vita della soluzione di onboarding a distanza del cliente.

4.2 Acquisizione di informazioni

4.2.1 Identificazione del cliente

23. In aggiunta a quanto indicato nel paragrafo 9, gli enti creditizi e gli istituti finanziari dovrebbero definire nelle loro politiche e procedure le informazioni necessarie per identificare il cliente, i tipi di documenti, dati o informazioni che utilizzeranno per verificare l'identità del cliente e le modalità di verifica di tali informazioni.

24. Gli enti creditizi e gli istituti finanziari dovrebbero assicurare che:

a) le informazioni ottenute attraverso la soluzione di onboarding a distanza del cliente siano aggiornate e adeguate a soddisfare le norme giuridiche e regolamentari applicabili all'adeguata verifica iniziale della clientela;

b) tutte le immagini, i video, i suoni e i dati siano acquisiti in un formato leggibile e con una qualità sufficiente ad assicurare il riconoscimento inequivocabile del cliente;

c) il processo di identificazione non prosegua se vengono rilevate carenze tecniche o interruzioni impreviste della connessione.

25. Gli enti creditizi o gli istituti finanziari dovrebbero considerare soddisfatti i criteri di cui al paragrafo 24 se la soluzione utilizza uno dei seguenti elementi:

a) regimi di identificazione elettronica notificati ai sensi dell'articolo 9 del regolamento (UE) n. 910/2014 che soddisfano i requisiti relativi a livelli di garanzia «significativi» o «elevati» ai sensi dell'articolo 8 di tale regolamento;

b) servizi fiduciari qualificati pertinenti che soddisfano i requisiti del regolamento (UE) n. 910/2014, in particolare il capo III, sezione 3 e l'articolo 24, paragrafo 1, comma 2, lettera b), di tale regolamento.

26. I documenti e le informazioni raccolti durante il processo di identificazione a distanza, che devono essere conservati in conformità dell'articolo 40, paragrafo 1, lettera a), della direttiva (UE) 2015/849, dovrebbero essere orodatati e conservati in modo sicuro dall'ente creditizio e finanziario. Il contenuto dei documenti conservati, compresi immagini, video, suoni e dati, dovrebbe essere disponibile in un formato leggibile e consentire verifiche ex post.

4.2.2 Identificazione di persone fisiche

27. Gli enti creditizi e gli istituti finanziari dovrebbero stabilire nelle rispettive politiche, come indicato nella sezione 4.1.1, paragrafo 9, le informazioni che devono ottenere per identificare i clienti a distanza, in conformità dell'articolo 13, paragrafo 1, lettere a) e c), della direttiva (UE) 2015/849. Inoltre, gli enti creditizi e gli istituti finanziari dovrebbero definire quali informazioni:

a) sono inserite manualmente dal cliente;

b) sono estratte in modo automatico dalla documentazione fornita dal cliente;

c) sono raccolte utilizzando altre fonti interne o esterne.

28. Gli enti creditizi e gli istituti finanziari dovrebbero porre in essere e mantenere meccanismi appropriati per assicurare che le informazioni acquisite in modo automatico in linea con il paragrafo 27 siano affidabili. Dovrebbero applicare controlli per gestire i rischi associati, compresi i rischi legati all'acquisizione automatica di dati, quali l'offuscamento dell'ubicazione del dispositivo del cliente, indirizzi di protocollo Internet (IP) alterati o servizi come reti private virtuali (VPN).

4.2.3 Identificazione di persone giuridiche

29. In caso di onboarding a distanza di clienti che sono persone giuridiche, gli enti creditizi e gli istituti finanziari dovrebbero definire nelle loro politiche e procedure, come indicato nella sezione 4.1.1, paragrafo 9, per quali categoria di persone giuridiche sarà utilizzato l'onboarding a distanza, tenendo conto del livello di rischio ML/TF associato a ciascuna categoria e del livello di intervento umano necessario per convalidare le informazioni di identificazione.

30. Gli enti creditizi e gli istituti finanziari dovrebbero assicurare che la soluzione di onboarding a distanza del cliente disponga di funzioni per la raccolta di:

a) tutti i dati e tutta la documentazione pertinenti per l'identificazione e la verifica della persona giuridica;

b) tutti i dati e tutta la documentazione pertinenti per verificare che la persona fisica che agisce per conto della persona giuridica sia giuridicamente legittimato ad agire in tale qualità;

c) le informazioni relative ai titolari effettivi in conformità della disposizione 4.12 degli orientamenti dell'ABE in materia di fattori di rischio ([6]).

31. Per la persona fisica che agisce per conto di una persona giuridica, gli enti creditizi e gli istituti finanziari dovrebbero applicare la procedura di identificazione di cui alla sezione 4.2.2.

4.2.4 Natura e scopo del rapporto d'affari

32. Al momento di valutare e, se del caso, acquisire informazioni sullo scopo e sulla natura prevista del rapporto d'affari in conformità dell'articolo 13, paragrafo 1, lettera c), della direttiva (UE) 2015/849, come ulteriormente specificato nella sezione 4.38 degli orientamenti dell'ABE in materia di fattori di rischio, gli enti creditizi e gli istituti finanziari, ai fini dei presenti orientamenti, dovrebbero avere completato le azioni pertinenti prima della fine del processo di onboarding a distanza del cliente.

4.3 Autenticità e integrità dei documenti

33. Laddove gli enti creditizi e gli istituti finanziari accettino riproduzioni di un documento originale e non esaminino il documento originale, essi dovrebbero adottare misure per accertare che la riproduzione sia affidabile. Gli enti creditizi e gli istituti finanziari dovrebbero verificare almeno quanto segue:

a) se la riproduzione include caratteristiche di sicurezza incorporate nel documento originale e se le specifiche del documento originale riprodotte sono valide e accettabili, in particolare il tipo, la dimensione dei caratteri e la struttura del documento, confrontandole con banche dati ufficiali, come PRADO ([7]);

b) se i dati personali sono stati alterati o altrimenti manomessi o, se del caso, se l'immagine del cliente incorporata nel documento è stata sostituita;

c) l'integrità dell'algoritmo utilizzato per generare il numero di identificazione unico del documento originale, nel caso in cui il documento ufficiale sia stato emesso con zona a lettura ottica;

d) se la riproduzione fornita è di qualità e definizione sufficienti ad assicurare l'univocità delle informazioni rilevanti;

([6]) EBA/GL/2021/02.

[7] https://www.consilium.europa.eu/prado/en/prado-start-page.html

e) che la riproduzione visualizzata su uno schermo non sia a sua volta la riproduzione di una fotografia o una scansione del documento d'identità originale.

34. Se gli enti creditizi e gli istituti finanziari utilizzano strumenti di lettura automatica delle informazioni dai documenti, come algoritmi di riconoscimento ottico dei caratteri o verifiche delle zone a lettura ottica, dovrebbero adottare le misure necessarie per assicurare che tali strumenti acquisiscano le informazioni in modo accurato e coerente.

35. Nelle situazioni in cui il dispositivo utilizzato dai clienti per dimostrare la propria identità consente la raccolta dei dati rilevanti, ad esempio perché i dati sono contenuti nel chip di una carta d'identità nazionale, ed è tecnicamente possibile per gli enti creditizi e gli istituti finanziari accedere a tali dati, gli enti creditizi e gli istituti finanziari dovrebbero prendere in considerazione la possibilità di utilizzare tali informazioni per verificarne la coerenza con le informazioni ottenute attraverso altre fonti, come i dati o altri documenti presentati dal cliente.

36. Se disponibili, durante il processo di verifica, gli enti creditizi e gli istituti finanziari dovrebbero verificare i dispositivi di sicurezza incorporate nel documento ufficiale, ad esempio gli ologrammi, come prova di autenticità.

37. Gli enti creditizi e finanziari dovrebbero indicare nelle rispettive politiche e procedure come adegueranno le loro richieste di fornire documentazione per finalità di inclusione finanziaria. Qualora si accettino forme di documentazione meno affidabili o non tradizionali, gli enti creditizi e gli istituti finanziari dovrebbero prevedere, oltre alle misure di cui al paragrafo 4.10 degli orientamenti dell'ABE in materia di fattori di rischio, controlli o un maggiore intervento umano per accertarsi di comprendere il rischio ML/TF associato al rapporto d'affari.

4.4 Accertamento della corrispondenza dell'identità del cliente nel quadro del processo di verifica

38. Le soluzioni di onboarding a distanza del cliente poste in essere dagli enti creditizi e gli istituti finanziari dovrebbero, come minimo, consentire di accertare quanto segue, nel quadro del processo di verifica:

a) che vi sia una corrispondenza tra le informazioni visibili della persona fisica e la documentazione fornita;

b) nel caso in cui il cliente sia una persona giuridica, che sia registrato presso un'autorità pubblica, se applicabile;

c) nel caso in cui il cliente sia una persona giuridica, che la persona fisica che lo rappresenta sia autorizzata ad agire per suo conto.

39. Se la soluzione di onboarding remoto del cliente prevede il ricorso a dati biometrici per verificare l'identità del cliente, gli enti creditizi e gli istituti finanziari dovrebbero assicurare che i dati biometrici siano sufficientemente univoci da essere inequivocabilmente collegati a un'unica persona fisica. Gli enti creditizi e gli istituti finanziari dovrebbero utilizzare algoritmi efficaci e affidabili per verificare la corrispondenza tra i dati biometrici indicati nel documento d'identità presentato e il cliente oggetto di onboarding. Laddove la soluzione non fornisca il livello di garanzia necessario, dovrebbero essere effettuati controlli aggiuntivi.

40. Qualora le informazioni fornite siano di qualità insufficiente, con una conseguente ambiguità o incertezza tali da compromettere la corretta esecuzione dei controlli a distanza, il singolo processo di onboarding a distanza del cliente dovrebbe essere interrotto e riavviato o reindirizzato a una verifica de visu.

41. Se gli enti creditizi e gli istituti finanziari utilizzano soluzioni di onboarding a distanza non presenziate, in cui il cliente non interagisce con un dipendente per l'esecuzione del processo di verifica, essi dovrebbero:

    a) assicurare che le fotografie o i video siano realizzati in condizioni di illuminazione adeguate e che le caratteristiche richieste siano acquisite con la necessaria chiarezza per consentire la corretta verifica dell'identità del cliente;

    b) assicurare che le fotografie o i video siano realizzati nel momento in cui l'acquirente esegue il processo di verifica;

    c) eseguire verifiche per accertare che il cliente sia un essere umano vivo, che possono includere procedure in cui è richiesta un'azione specifica da parte del cliente per verificare la sua presenza nella sessione di comunicazione o che possono essere basate sull'analisi dei dati ricevuti e non richiedere un'azione specifica da parte del cliente;

    d) utilizzare algoritmi efficaci e affidabili per verificare se la/le fotografia/fotografie o i video realizzati corrispondono alla/alle immagine/immagini ottenute dai documenti ufficiali del cliente.

42. Se gli enti creditizi e gli istituti finanziari utilizzano soluzioni di onboarding a distanza del cliente assistite, in cui il cliente interagisce con un dipendente per l'esecuzione del processo di verifica, essi dovrebbero:

    a) assicurare che la qualità dell'immagine e dell'audio sia sufficiente a consentire la corretta verifica dell'identità del cliente e che siano utilizzati sistemi tecnologici affidabili;

    b) prevedere la partecipazione di un dipendente che abbia una conoscenza sufficiente della normativa AML/CFT applicabile e degli aspetti di sicurezza della verifica a distanza e che abbia una formazione sufficiente per essere in grado di prevedere ed

evitare l'uso intenzionale o deliberato di tecniche di inganno associate alla verifica a distanza, nonché per individuarle e reagire in caso siano utilizzate;

c) elaborare una guida al colloquio che definisca le fasi successive del processo di verifica a distanza e le azioni che il dipendente dovrebbe intraprendere. La guida al colloquio dovrebbe includere indicazioni sull'osservazione e sull'individuazione di fattori psicologici o di altri elementi che potrebbero caratterizzare un comportamento sospetto durante la verifica a distanza.

43. Ove possibile, gli enti creditizi e gli istituti finanziari dovrebbero utilizzare soluzioni di onboarding a distanza del cliente che includano la casualità nella sequenza di azioni che il cliente deve compiere ai fini della verifica, per proteggersi da rischi quali l'uso di identità sintetiche o la coercizione. Ove possibile, gli enti creditizi e gli istituti finanziari dovrebbero anche prevedere l'assegnazione casuale degli incarichi al dipendente responsabile del processo di verifica a distanza, al fine di evitare la collusione tra il cliente e il dipendente responsabile.

44. In aggiunta a quanto sopra, e se commisurato al rischio ML/TF associato al rapporto d'affari, gli enti creditizi e gli istituti finanziari dovrebbero utilizzare uno o più dei seguenti controlli o una misura analoga per aumentare l'affidabilità del processo di verifica. Tali controlli o misure possono includere, a titolo esemplificativo ma non esaustivo, quanto segue:

a) esecuzione del primo pagamento a valere su un conto intestato o cointestato al cliente presso un ente creditizio o finanziario regolamentato in un paese dello Spazio economico europeo o in un paese terzo nel quale vigono obblighi di AML/CFT di livello analogo a quelli previsti dalla direttiva (UE) 2015/849;

b) invio al cliente di un codice di accesso generato in modo casuale per confermare la presenza durante il processo di verifica a distanza. Il codice di accesso dovrebbe essere monouso e limitato nel tempo;

c) acquisizione di dati biometrici per confrontarli con i dati raccolti attraverso altre fonti indipendenti e affidabili;

d) contatti telefonici con il cliente;

e) invio diretto di comunicazioni (per via sia elettronica che postale) al cliente.

45. Gli enti creditizi e gli istituti finanziari dovrebbero considerare soddisfatti i criteri di cui ai paragrafi da 38 a 43 se la soluzione utilizza uno dei seguenti elementi:

a) regimi di identificazione elettronica notificati ai sensi dell'articolo 9 del regolamento (UE) n. 910/2014 che soddisfano i requisiti relativi a livelli di garanzia «significativi» o «elevati» ai sensi dell'articolo 8 di tale regolamento;

b) servizi fiduciari qualificati pertinenti che soddisfano i requisiti del regolamento (UE) n. 910/2014, in particolare il capo III, sezione 3 e l'articolo 24, paragrafo 1, comma 2, lettera b), di tale regolamento.

4.5 Ricorso a terzi ed esternalizzazione

46. Oltre ai punti di cui al paragrafo 9, gli enti creditizi e gli istituti finanziari dovrebbero specificare nelle loro politiche e procedure quali funzioni e attività di onboarding a distanza del cliente saranno svolte o eseguite dall'ente creditizio o istituto finanziario, quali da terzi o da un altro prestatore di servizi esterno.

4.5.1 Ricorso a terzi in conformità del capo II, sezione 4, della direttiva (UE) 2015/849

47. Oltre agli orientamenti dell'ABE in materia di fattori di rischio ([8]), in particolare i paragrafi 2.20, 2.21 e dal 4.32 al 4.37 di tali orientamenti, essi dovrebbero applicare i seguenti criteri:

a) adottare le misure necessarie per accertarsi che i processi e le procedure attuati dal terzo per l'adeguata verifica della clientela ai fini dell'onboarding a distanza del cliente, nonché le informazioni e i dati raccolti in questo contesto, siano sufficienti e coerenti con i requisiti stabiliti nei presenti orientamenti;

b) assicurare la continuità dei rapporti d'affari tra l'acquirente e l'ente creditizio o istituto finanziario per proteggersi da eventi che potrebbero rivelare carenze nel processo di onboarding a distanza del cliente svolto dal terzo.

4.5.2 Esternalizzazione dell'adeguata verifica della clientela

48. Se gli enti creditizi e gli istituti finanziari esternalizzano in tutto o in parte il processo di onboarding a distanza del cliente a un prestatore di servizi esterno, come menzionato nell'articolo 29 della direttiva (UE) 2015/849, essi dovrebbero applicare, oltre ai paragrafi 2.20, 2.21 e dal 4.32 al 4.37 degli orientamenti dell'ABE in materia di fattori di rischio e, se del caso, oltre agli orientamenti dell'ABE in materia di esternalizzazione ([9]), prima e durante il rapporto d'affari con il prestatore di servizi esterno, le seguenti misure, la cui portata dovrebbe essere adattata in funzione del rischio:

a) assicurare che il prestatore di servizi esterno attui efficacemente e rispetti le politiche e le procedure di onboarding a distanza del cliente dell'ente creditizio o dell'istituto finanziario, in conformità dell'accordo di esternalizzazione. Tale risultato dovrebbe essere conseguito mediante segnalazioni periodiche, monitoraggio continuo, visite in loco o verifiche a campione;

b) effettuare valutazioni per assicurare che il prestatore di servizi esterno sia sufficientemente attrezzato e capace di eseguire il processo di onboarding a distanza

([8]) EBA/GL/2021/02.

([9]) Orientamenti dell'ABE in materia di esternalizzazione.docx (europa.eu).

del cliente. Le valutazioni possono riguardare, a titolo esemplificativo e non esaustivo, la formazione del personale, l'idoneità tecnologica e la governance dei dati presso il prestatore di servizi esterno;

c) assicurare che il prestatore di servizi esterno informi gli enti creditizi e gli istituti finanziari di qualsiasi proposta di modifica del processo di onboarding a distanza del cliente o di qualsiasi modifica apportata alla soluzione fornita dal prestatore di servizi esterno.

49. Qualora il prestatore di servizi esterno conservi i dati dei clienti, compresi, ma non solo, fotografie, video e documenti, durante il processo di onboarding a distanza, gli enti creditizi e gli istituti finanziari dovrebbero assicurare che:

a) siano raccolti e conservati solo i dati necessari del cliente, per un periodo di conservazione chiaramente definito;

b) l'accesso ai dati sia strettamente limitato e registrato;

c) siano attuate misure di sicurezza adeguate per assicurare la protezione dei dati conservati.

4.6 Gestione dei rischi delle ICT e di sicurezza

50. Gli enti creditizi e gli istituti finanziari dovrebbero individuare e gestire i rischi delle ICT e di sicurezza connessi all'utilizzo del processo di onboarding a distanza del cliente, anche quando ricorrono a terzi o il servizio è esternalizzato, anche a entità del gruppo.

51. Oltre a rispettare i requisiti di cui agli orientamenti dell'ABE sulla gestione dei rischi delle ICT e di sicurezza ([10]), ove applicabile, gli enti creditizi e gli istituti finanziari dovrebbero utilizzare canali di comunicazione sicuri per interagire con il cliente durante il processo di onboarding a distanza. La soluzione di onboarding a distanza del cliente dovrebbe utilizzare protocolli sicuri e algoritmi crittografici in linea con le migliori prassi del settore per salvaguardare la riservatezza, l'autenticità e l'integrità dei dati scambiati, ove applicabile.

52. Gli enti creditizi e gli istituti finanziari dovrebbero fornire un punto di accesso sicuro per l'avvio del processo di onboarding a distanza del cliente basato su certificati qualificati di sigillo elettronico di cui all'articolo 3, paragrafo 30, del regolamento (UE) n. 910/2014 o di autenticazione del sito web di cui all'articolo 3, paragrafo 39, del medesimo regolamento. Il cliente dovrebbe inoltre essere informato in merito alle misure di sicurezza applicabili da adottare per garantire un uso sicuro del sistema.

53. Qualora sia usato un dispositivo multifunzione per eseguire il processo di onboarding a distanza del cliente, dovrebbe essere utilizzato un ambiente sicuro per l'esecuzione del codice software da parte del cliente, ove applicabile. Dovrebbero essere attuate misure di sicurezza

([10]) EBA/GL/2019/04.

aggiuntive per garantire la sicurezza e l'affidabilità del codice software e dei dati raccolti, in base alla valutazione dei rischi di sicurezza di cui agli orientamenti dell'ABE sulla gestione dei rischi delle ICT e di sicurezza.

4.7 Conformità ai presenti orientamenti se gli enti creditizi e gli istituti finanziari utilizzano servizi fiduciari e processi di identificazione nazionale di cui all'articolo 13, paragrafo 1, lettera a), della direttiva (UE) 2015/849

54. Gli enti creditizi e gli istituti finanziari possono utilizzare servizi fiduciari e procedure di identificazione elettronica regolamentati, riconosciuti, approvati o accettati dalle autorità nazionali competenti, come previsto dall'articolo 13, paragrafo 1, lettera a), della direttiva (UE) 2015/849 per conformarsi ai presenti orientamenti. Se si avvalgono di tali soluzioni, gli enti creditizi e gli istituti finanziari dovrebbero valutare in che misura la soluzione è conforme alle disposizioni dei presenti orientamenti e applicare le misure necessarie per mitigare eventuali rischi rilevanti derivanti dall'uso di tali soluzioni. In particolare, dovrebbero considerare se sono affrontati i seguenti rischi:

    a) i rischi connessi all'autenticazione, definendo nelle proprie politiche e procedure specifiche misure di mitigazione, in particolare per quanto riguarda i rischi di sostituzione di persona;

    b) il rischio che l'identità del cliente non sia quella dichiarata;

    c) il rischio di smarrimento, furto, sospensione, revoca o scadenza dei documenti comprovanti l'identità, compresi, se del caso, strumenti per individuare e prevenire i furti d'identità.