EBA/GL/2022/15

22.11.2022

Orientations

sur l'utilisation de solutions d'entrée en relation d'affaires à distance conformément à l'article 13, paragraphe 1, de la directive (UE) 2015/849

1. Obligations en matière de conformité et de déclaration

Statut des présentes orientations

1. Le présent document contient des orientations émises en vertu de l'article 16 du règlement (UE) nº 1093/2010[1]. Conformément à l'article 16, paragraphe 3, du règlement (UE) nº 1093/2010, les autorités compétentes et les établissements financiers mettent tout en œuvre pour respecter les présentes orientations.

2. Les orientations exposent l'opinion de l'Autorité bancaire européenne (ABE) concernant les pratiques de surveillance appropriées au sein du Système européen de surveillance financière ou les modalités d'application de la législation de l'Union dans un domaine particulier. Les autorités compétentes, telles que définies à l'article 4, paragraphe 2, du règlement (UE) nº 1093/2010 qui sont soumises à ces orientations doivent les respecter en les intégrant dans leurs pratiques s'il y a lieu (par exemple en modifiant leur cadre juridique ou leurs procédures de surveillance), y compris lorsque les orientations s'adressent en priorité à des établissements.

Obligations de notification

3. Conformément à l'article 16, paragraphe 3, du règlement (UE) nº 1093/2010, les autorités compétentes doivent indiquer à l'ABE si elles respectent ou entendent respecter ces orientations ou communiquer, dans le cas contraire, les motifs de leur non-respect avant le 30.05.2023. En l'absence de notification avant cette date, l'ABE considérera que les autorités compétentes ne respectent pas les orientations. Les notifications doivent être transmises au moyen du formulaire disponible sur le site internet de l'ABE, sous la référence «EBA/GL/2022/15». Les notifications doivent être envoyées par des personnes dûment habilitées à rendre compte du respect de ces orientations au nom des autorités compétentes qu'elles représentent. Tout changement en matière de conformité avec les orientations doit également être signalé à l'ABE.

4. Conformément à l'article 16, paragraphe 3, du règlement (UE) nº 1093/2010, les notifications seront publiées sur le site internet de l'ABE.

[1] Règlement (UE) nº 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission (JO L 331 du 15.12.2010, p. 12).

2. Objet, champ d'application et définitions

Objet et champ d'application

5. Les présentes orientations décrivent les mesures que les établissements de crédit et les établissements financiers doivent mettre en œuvre pour s'acquitter de leurs obligations au titre de l'article 13, paragraphe 1, points a), b) et c), de la directive (UE) 2015/849[2] lorsqu'ils adoptent ou examinent des solutions d'entrée en relation d'affaires avec de nouveaux clients à distance. Elles précisent également les mesures que les établissements de crédit et les établissements financiers doivent prendre en cas d'exécution par des tiers conformément au chapitre II, section 4, de la directive (UE) 2015/849, et les politiques, contrôles et procédures que les établissements de crédit et les établissements financiers doivent mettre en place en matière de vigilance à l'égard de la clientèle telle que visée à l'article 8, paragraphes 3 et 4, point a), de la directive (UE) 2015/849 lorsque les mesures de vigilance à l'égard de la clientèle sont effectuées à distance.

6. Les autorités compétentes doivent tenir compte des présentes orientations lorsqu'elles déterminent si les mesures que les établissements de crédit et les établissements financiers doivent prendre pour s'acquitter de leurs obligations au titre de la directive (UE) 2015/849 dans le contexte de l'entrée en relation d'affaires à distance sont adéquates et efficaces.

Destinataires

7. Les présentes orientations s'adressent aux autorités compétentes telles que définies à l'article 4, paragraphe 2 du règlement (UE) nº 1093/2010, mais également aux opérateurs du secteur financier tels que définis à l'article 4, paragraphe 1*bis*, dudit règlement, qui sont des établissements de crédit et des établissements financiers au sens de l'article 3, paragraphes 1 et 2, de la directive (UE) 2015/849.

[2] Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme

Définitions

8. Sauf indication contraire, les termes employés et définis dans la directive (UE) 2015/849 revêtent la même signification dans les orientations. En outre, aux fins des présentes orientations, les définitions suivantes s'appliquent:

Données biométriques	Données personnelles relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment l'identification non équivoque de cette personne, telles que des images faciales ou des données dactyloscopiques, qui sont obtenues et traitées à l'aide de moyens techniques.

3. Mise en œuvre

Date d'application

Les présentes orientations s'appliquent à compter du 02.10.2023.

4. Orientations concernant l'utilisation de solutions d'entrée en relation d'affaires à distance conformément à l'article 13, paragraphe 1, de la directive (UE) 2015/849

4.1 Politiques et procédures internes

4.1.1 Politiques et procédures relatives à l'entrée en relation d'affaires à distance

9. Les établissements de crédit et les établissements financiers doivent mettre en place et tenir à jour des politiques et procédures visant à s'acquitter de leurs obligations au titre de l'article 13, paragraphe 1, points a) et c), de la directive (UE) 2015/849 en cas d'entrée en relation d'affaires avec le client à distance. Ces politiques et procédures doivent être adaptées au risque et comprendre au minimum:

   a) une description générale de la solution que les établissements de crédit et les établissements financiers ont mise en place pour recueillir, vérifier et enregistrer des informations tout au long du processus d'entrée en relation d'affaires à distance. Celle-ci doit comporter une explication des fonctionnalités et du fonctionnement de la solution;

   b) les situations dans lesquelles la solution d'entrée en relation d'affaires à distance peut être utilisée, en tenant compte des facteurs de risque identifiés et évalués conformément à l'article 8, paragraphe 1, de la directive (UE) 2015/849 et, dans l'évaluation du risque à l'échelle de l'entreprise, en incluant une description des catégories de clients, produits et services éligibles pour l'entrée en relation d'affaires à distance;

   c) les étapes qui sont entièrement automatisées et celles qui nécessitent une intervention humaine;

   d) les contrôles en place pour s'assurer que la première transaction avec un client avec lequel un établissement est récemment entré en relation d'affaires est exécutée seulement une fois que toutes les mesures initiales de vigilance à l'égard de la clientèle ont été appliquées;

   e) une description des programmes d'intégration et de formation régulière pour s'assurer que le personnel est sensibilisé et dispose de connaissances à jour quant

au fonctionnement de la solution d'entrée en relation d'affaires à distance, aux risques associés et aux politiques et procédures d'entrée en relation d'affaires à distance destinées à atténuer ces risques.

10. Lorsqu'elles sont mises en œuvre, ces politiques et procédures doivent permettre aux établissements de crédit et aux établissements financiers de garantir la conformité aux dispositions visées aux sections 4.2 à 4.7 des présentes orientations.

4.1.2 Gouvernance

11. En complément des dispositions énoncées à la section 4.2.4 des orientations de l'ABE[3] sur le responsable de la conformité, le responsable de la conformité en matière de LBC/FT[4] doit, dans le cadre de sa mission globale, élaborer des politiques et procédures afin de satisfaire aux exigences en matière de vigilance à l'égard de la clientèle, et veiller à ce que les politiques et procédures d'entrée en relation d'affaires à distance soient mises en œuvre efficacement, examinées régulièrement et modifiées si nécessaire.

12. L'organe de direction de l'établissement de crédit et de l'établissement financier doit approuver les politiques et procédures d'entrée en relation d'affaires à distance et veiller à leur bonne application.

4.1.3 Évaluation de la solution d'entrée en relation d'affaires à distance préalablement à sa mise en œuvre

13. Lorsqu'ils envisagent d'adopter une nouvelle solution d'entrée en relation d'affaires à distance, les établissements de crédit et les établissements financiers doivent réaliser une évaluation de la solution préalablement à sa mise en œuvre.

14. Les établissements de crédit et les établissements financiers doivent définir dans leurs politiques et procédures les exigences relatives au champ d'application, aux différentes étapes et à l'enregistrement de cette évaluation préalable, laquelle doit inclure au minimum:

    a) une évaluation du caractère adéquat de la solution du point de vue de l'exhaustivité et de l'exactitude des données et des documents à recueillir, ainsi que de la fiabilité et de l'indépendance des sources d'informations qu'ils utilisent;

    b) une évaluation de l'incidence du recours à la solution d'entrée en relation d'affaires à distance sur les risques à l'échelle de l'entreprise, notamment les risques en matière de LBC/FT, les risques opérationnels, les risques de réputation et les risques juridiques;

[3] Projet d'orientations concernant les politiques et procédures relatives à la gestion du respect des obligations et le rôle et les responsabilités du responsable du contrôle du respect des obligations en matière de LBC/FT au titre de l'article 8 et du chapitre VI de la directive

[4] Conformément aux critères de proportionnalité énoncés à la section 4.2.2 des orientations sur le responsable de la conformité

c) l'identification d'éventuelles mesures d'atténuation et actions correctrices pour chaque risque identifié par l'évaluation prévue au point b);

d) des tests permettant d'évaluer les risques de fraude, notamment les risques d'usurpation d'identité et autres risques liés aux technologies de l'information et de la communication («TIC») et à la sécurité, conformément au paragraphe 43 des orientations de l'ABE relatives à la gestion des risques liés aux TIC et à la sécurité[5];

e) des essais de bout en bout du fonctionnement de la solution ciblant le(s) client(s), produit(s) et service(s) identifiés dans les politiques et procédures d'entrée en relation d'affaires à distance.

15. Les établissements de crédit et les établissements financiers devraient veiller au respect des critères indiqués au paragraphe 14, points a), d) et e), si la solution utilise l'un des moyens suivants:

a) des schémas d'identification électronique notifiés conformément à l'article 9 du règlement (UE) n° 910/2014 et satisfaisant aux exigences en matière de niveaux de garantie «substantiel» ou «élevé» conformément à l'article 8 dudit règlement;

b) des services de confiance qualifiés au sens du règlement (UE) n° 910/2014, en particulier le chapitre III, section 3, et l'article 24, paragraphe 1, alinéa 2, point b), dudit règlement.

16. Les établissements de crédit et les établissements financiers doivent être en mesure de justifier auprès leur autorité compétente des évaluations qu'ils ont réalisées avant la mise en œuvre de la solution d'entrée en relation d'affaires à distance, du résultat de ces évaluations et du caractère approprié de l'utilisation de cette solution au regard des risques en matière de LBC/FT identifiés pour les différents types de clients, services, zones géographiques et produits concernés.

17. Les établissements de crédit et les établissements financiers doivent commencer à utiliser une solution d'entrée en relation d'affaires à distance seulement après s'être assurés que celle-ci pourra être intégrée au système de contrôle interne plus large de l'établissement, ce qui permettra ainsi à l'établissement de gérer de manière adéquate les risques en matière de LBC/FT pouvant résulter de l'utilisation de la solution d'entrée en relation d'affaires à distance.

[5] EBA/GL/2019/04

4.1.4 Suivi permanent de la solution d'entrée en relation d'affaires à distance

18. Les établissements de crédit et les établissements financiers doivent assurer un suivi permanent de la solution d'entrée en relation d'affaires à distance aux fins de vérifier qu'elle fonctionne conformément aux attentes des établissements de crédit et des établissements financiers. Ils doivent compléter leurs politiques et procédures énoncées au paragraphe 9, au moins par une description des éléments suivants:

    a) les mesures mises en œuvre pour assurer la qualité, l'exhaustivité, le caractère adéquat et l'exactitude des données recueillies pendant le processus d'entrée en relation d'affaires à distance, lesquelles doivent être adaptées aux risques en matière de LBC/FT auxquels l'établissement de crédit et l'établissement financier est exposé;

    b) l'étendue et la fréquence de ces examens réguliers; et

    c) les circonstances qui déclencheront des examens ponctuels, lesquels doivent inclure au minimum:

        a. des changements relatifs à l'exposition de l'établissement de crédit et de l'établissement financier au risque en matière de LBC/FT;

        b. des défaillances concernant le fonctionnement de la solution détectées au cours des activités de suivi, d'audit ou de surveillance;

        c. une augmentation perçue des tentatives de fraude;

        d. des modifications du cadre juridique ou réglementaire.

19. Les établissements de crédit et les établissements financiers doivent indiquer dans leurs procédures et processus les mesures correctrices à mettre en œuvre lors de l'apparition d'un risque ou l'identification d'erreurs ayant une incidence sur l'efficience et l'efficacité de la solution d'entrée en relation d'affaires à distance. Ces mesures devraient inclure au minimum:

    a) un examen de toutes les relations d'affaires concernées, pour déterminer si les établissements de crédit et les établissements financiers ont fait preuve d'une vigilance suffisante à l'égard de la clientèle lors de l'entrée en relation d'affaires, afin de se conformer à l'article 13, paragraphe 1), points a), b) et c), de la directive anti-blanchiment. Les établissements de crédit et les établissements financiers doivent accorder la priorité aux relations d'affaires présentant le risque le plus élevé en matière de LBC/FT;

b) en tenant compte des informations obtenues dans le cadre de l'examen susmentionné, une évaluation ayant pour but de déterminer si la relation d'affaires concernée devrait:

   a. faire l'objet de mesures de vigilance supplémentaires;

   b. lorsque la législation nationale le permet, faire l'objet de restrictions telles que des limites concernant le volume de transaction, jusqu'à ce qu'un réexamen ait lieu;

   c. être achevée;

   d. être signalée à la CRF;

   e. être classée dans une catégorie de risque différente.

20. Les établissements de crédit et les établissements financiers doivent déterminer le moyen le plus efficace de vérifier le caractère adéquat et la fiabilité des solutions d'entrée en relation d'affaires à distance. Ils doivent envisager notamment un ou plusieurs des moyens suivants:

    i. tests d'assurance qualité;

    ii. alertes et notifications automatisées de criticité;

    iii. rapports réguliers de qualité automatisés ;

    iv. analyse d'échantillons;

    v. examens manuels.

21. La présente section s'applique également lorsque sont utilisées des solutions d'entrée en relation d'affaires à distance entièrement automatisées, fortement dépendantes d'algorithmes automatisés, sans intervention humaine ou avec une intervention humaine limitée.

22. Les établissements de crédit et les établissements financiers doivent être en mesure de démontrer à leur autorité compétente que des examens ont été réalisés et qu'ils ont mis en œuvre des mesures correctrices pour remédier aux défaillances identifiées sur toute la durée de vie de la solution d'entrée en relation d'affaires à distance.

4.2 Obtention d'informations

4.2.1 Identification du client

23. En complément des points énoncés au paragraphe 9, les établissements de crédit et les établissements financiers doivent définir dans leurs politiques et procédures les informations nécessaires à l'identification du client, les types de documents, données ou informations que l'établissement utilisera pour vérifier l'identité du client et la manière dont ces informations seront vérifiées.

24. Les établissements de crédit et les établissements financiers doivent s'assurer que:

    a) les informations obtenues par le biais de la solution d'entrée en relation d'affaires à distance sont à jour et adaptées pour satisfaire aux normes légales et réglementaires applicables en matière de vigilance initiale à l'égard de la clientèle;

    b) les images, vidéos, sons et données sont enregistrés dans un format lisible et sont de qualité suffisante pour reconnaître clairement le client;

    c) le processus d'identification ne se poursuit pas si des défaillances techniques ou des interruptions inattendues de la connexion sont détectées.

25. Les établissements de crédit ou les établissements financiers doivent remplir les critères indiqués au paragraphe 24 si la solution utilise l'un des moyens suivants:

    a) des schémas d'identification électronique notifiés conformément à l'article 9 du règlement (UE) n° 910/2014 et satisfaisant aux exigences en matière de niveaux de garantie «substantiel» ou «élevé» conformément à l'article 8 dudit règlement;

    b) des services de confiance qualifiés au sens du règlement (UE) n° 910/2014, en particulier le chapitre III, section 3, et l'article 24, paragraphe 1, alinéa 2, point b), dudit règlement.

26. Les documents et informations recueillis pendant le processus d'identification à distance, qui doivent être conservés conformément à l'article 40, paragraphe 1, point a), de la directive (UE) 2015/849, doivent être horodatés et stockés de manière sécurisée par l'établissement de crédit et l'établissement financier. Le contenu des enregistrements stockés, y compris les images, vidéos, sons et données, doivent être disponibles dans un format lisible et permettre des vérifications ex post.

4.2.2 Identification de personnes physiques

27. Les établissements de crédit et les établissements financiers doivent définir dans leurs politiques, tel qu'indiqué à la section 4.1.1, paragraphe 9, les informations qu'ils doivent obtenir pour identifier les clients à distance, conformément à l'article 13, paragraphe 1,

points a) et c), de la directive (UE) 2015/849. Les établissements de crédit et les établissements financiers doivent également définir les informations qui:

a) sont saisies manuellement par le client;

b) sont obtenues automatiquement à partir des documents fournis par le client;

c) sont recueillies auprès d'autres sources internes ou externes.

28. Les établissements de crédit et les établissements financiers doivent mettre en place et tenir à jour des mécanismes appropriés pour s'assurer que les informations qu'ils obtiennent automatiquement conformément au paragraphe 27 sont fiables. Ils doivent appliquer des contrôles destinés à faire face aux risques associés, y compris les risques associés à l'obtention automatique de données tels que le brouillage de la localisation de l'appareil du client, l'usurpation de l'adresse IP ou de services comme le réseau privé virtuel (RPV ou VPN).

4.2.3 Identification de personnes morales

29. Lorsque les établissements de crédit et les établissements financiers entrent en relation d'affaires à distance avec des clients qui sont des personnes morales, ils doivent définir dans leurs politiques et procédures, conformément à la section 4.1.1. paragraphe 9, les catégories de personnes morales concernées, en tenant compte, pour chaque catégorie, du niveau de risque en matière de LCB-FT ainsi que du niveau d'intervention humaine requis pour la validation des informations d'identification.

30. Les établissements de crédit et les établissements financiers doivent s'assurer que la solution d'entrée en relation d'affaires à distance possède des fonctionnalités visant à recueillir:

a) l'ensemble des données et documents pertinents permettant d'identifier et de vérifier la personne morale;

b) l'ensemble des données et documents pertinents permettant de vérifier que la personne physique agissant au nom de la personne morale est légalement habilitée à le faire;

c) les informations concernant les bénéficiaires effectifs, conformément au point 4.12 des orientations de l'ABE relatives aux facteurs de risque[6].

31. Pour la personne physique agissant au nom d'une personne morale, les établissements de crédit et les établissements financiers doivent appliquer le processus d'identification décrit à la section 4.2.2.

[6] EBA/GL/2021/02

4.2.4 Nature et objet de la relation d'affaires

32. Lorsque les établissements de crédit et les établissements financiers évaluent et, le cas échéant, obtiennent des informations concernant l'objet et la nature envisagée de la relation d'affaires, conformément à l'article 13, paragraphe 1, point c), de la directive (UE) 2015/849, tel que spécifié, en outre, à la section 4.38 des orientations de l'ABE relatives aux facteurs de risque, ils doivent, aux fins des présentes orientations, avoir exécuté les actions pertinentes avant la fin du processus d'entrée en relation d'affaires à distance.

4.3 Authenticité et intégrité des documents

33. Lorsque les établissements de crédit et les établissements financiers acceptent la copie d'un document original sans procéder à la vérification du document original, ils doivent mettre en œuvre des mesures permettant de vérifier que la reproduction est fiable. Les établissements de crédit et les établissements financiers doivent établir au minimum ce qui suit:

    a) que la reproduction comporte des caractéristiques de sécurité intégrées au document original et que les spécifications du document original en cours de reproduction sont valables et acceptables, en particulier, le type, la taille des caractères et la structure du document, en les comparant avec des bases de données officielles, telles que PRADO[7];

    b) que si des données personnelles ont été modifiées ou falsifiées, la photographie du client intégrée au document n'a pas été remplacée;

    c) en cas de délivrance du document officiel avec une zone de lecture automatique (ZLA), que l'intégrité de l'algorithme utilisé pour générer le numéro d'identification unique du document original a été préservée;

    d) que la reproduction fournie présente une qualité et une définition suffisantes pour garantir que les informations pertinentes sont sans ambiguïté;

    e) que la reproduction fournie n'a pas été affichée sur un écran sur la base d'une photographie ou d'une numérisation de la pièce d'identité originale.

34. Lorsque les établissements de crédit et les établissements financiers utilisent des fonctionnalités, telles que des algorithmes de reconnaissance optique de caractères (ROC) ou des vérifications par zone de lecture automatique (ZLA), permettant de lire automatiquement les informations figurant dans des documents, ils doivent prendre les mesures nécessaires pour s'assurer que ces outils saisissent les informations de manière précise et cohérente.

35. Dans les cas où l'appareil utilisé par les clients pour prouver leur identité permet de recueillir les données pertinentes, par exemple lorsque les données sont contenues dans la puce d'une carte nationale d'identité, et qu'il est techniquement faisable pour les établissements de

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

crédit et les établissements financiers d'accéder à ces données, lesdits établissements doivent considérer l'utilisation de ces informations pour vérifier leur cohérence avec celles obtenues par le biais d'autres sources, telles que les données transmises ou d'autres documents transmis par le client.

36. Le cas échéant, pendant le processus de vérification, les établissements de crédit et les établissements financiers doivent vérifier les éventuelles fonctionnalités de sécurité intégrées au document officiel, telles que des hologrammes, en guise de preuve de leur authenticité.

37. Les établissements de crédit et les établissements financiers doivent indiquer dans leurs politiques et procédures la manière dont ils adapteront leurs demandes de documents aux fins d'inclusion financière. Lorsque des formes de documents non traditionnelles ou moins sûres sont acceptées, les établissements de crédit et les établissements financiers doivent exercer, en plus des mesures énoncées au paragraphe 4.10 des orientations de l'ABE relatives aux facteurs de risque, des contrôles ou une intervention humaine renforcée pour s'assurer qu'ils comprennent le risque en matière de LBC/FT associé à la relation d'affaires.

4.4 Mise en correspondance de l'identité du client dans le cadre du processus de vérification

38. Les solutions d'entrée en relation d'affaires à distance mises en œuvre par les établissements de crédit et les établissements financiers doivent intégrer, dans le cadre du processus de vérification de l'identité du client, au minimum les éléments suivants :

    a) une correspondance entre les informations visibles de la personne physique et les documents fournis;

    b) lorsque le client est une personne morale, le fait qu'il figure, le cas échéant, dans un registre public,;

    c) lorsque le client est une personne morale, le fait que la personne physique qui la représente soit habilitée à agir en son nom.

39. Lorsque la solution d'entrée en relation d'affaires à distance implique l'utilisation de données biométriques pour vérifier l'identité du client, les établissements de crédit et les établissements financiers doivent s'assurer que les données biométriques sont suffisamment uniques pour être associées sans équivoque à une seule personne physique. Les établissements de crédit et les établissements financiers doivent avoir recours à des algorithmes performants et fiables pour vérifier la correspondance entre les données biométriques figurant sur la pièce d'identité transmise et le client objet de l'entrée en relation d'affaires. Dans les cas où la solution ne garantit pas le niveau de fiabilité requis, des contrôles supplémentaires doivent être appliqués.

40. Dans les cas où le justificatif présenté est de qualité insuffisante, entraînant une ambiguïté ou une incertitude de sorte que les performances des contrôles à distance s'en trouvent affectées, le processus d'entrée en relation d'affaires à distance concerné doit être interrompu et redémarré ou réorienté vers une vérification en face à face.

41. Lorsque les établissements de crédit et les établissements financiers ont recours à des solutions d'entrée en relation d'affaires à distance automatisées, dans le cadre desquelles le client n'interagit pas avec un employé pour effectuer le processus de vérification, ils doivent:

    a) s'assurer que toute photographie ou vidéo est prise dans des conditions d'éclairage satisfaisantes et que les propriétés requises sont capturées avec une netteté suffisante pour permettre la vérification appropriée de l'identité du client;

    b) s'assurer que toute photographie ou vidéo est prise au moment où le client effectue le processus de vérification;

    c) réaliser des tests de vérification du vivant (« liveness detection verifications »), qui peuvent inclure des procédures dans lesquelles une action spécifique du client est requise pour s'assurer qu'il ou elle est présent(e) lors de la session de communication ou qui peut être fondée sur l'analyse des données reçues et ne nécessite pas d'action spécifique de la part du client;

    d) utiliser des algorithmes performants et fiables pour vérifier si la ou les photographies ou vidéos prises correspondent à l'image ou aux images récupérées à partir du ou des documents officiels appartenant au client.

42. Lorsque les établissements de crédit et les établissements financiers ont recours à des solutions d'entrée en relation d'affaires à distance non automatisées, dans le cadre desquelles le client interagit avec un employé pour effectuer le processus de vérification, ils doivent:

    a) s'assurer que la qualité de l'image et de l'audio est suffisante pour permettre la vérification appropriée de l'identité du client, et que des systèmes technologiques fiables sont utilisés;

    b) prévoir la participation d'un employé qui possède des connaissances suffisantes concernant le règlement applicable en matière de LBC/FT et les questions de sécurité liées à la vérification à distance et qui est suffisamment formé pour anticiper et prévenir l'utilisation intentionnelle ou délibérée de techniques trompeuses relatives à la vérification à distance et pour les détecter et réagir le cas échéant;

    c) élaborer un guide d'entrevue définissant les étapes ultérieures du processus de vérification à distance ainsi que les actions requises de la part d'un employé. Le guide d'entrevue doit comprendre des orientations concernant l'observation et l'identification de facteurs psychologiques ou autres caractéristiques pouvant établir un comportement suspect lors de la vérification à distance.

43. Les établissements de crédit et les établissements financiers doivent, dans la mesure du possible, avoir recours à des solutions d'entrée en relation d'affaires à distance dont l'ordre des actions devant être exécutées par le client aux fins de vérification est fixé de manière aléatoire, afin de se prémunir contre les risques tels que l'utilisation d'identités synthétiques ou la coercition. Les établissements de crédit et les établissements financiers doivent également, dans la mesure du possible, assigner des tâches aléatoires à l'employé responsable du processus de vérification à distance pour éviter toute collusion entre le client et l'employé responsable.

44. En plus de ce qui précède, et lorsque cela est adapté au risque en matière de LBC/FT associé à la relation d'affaires, les établissements de crédit et les établissements financiers doivent utiliser un ou plusieurs des contrôles suivants ou une mesure similaire pour augmenter la fiabilité du processus de vérification. Ces contrôles ou mesures peuvent englober, à titre indicatif:

    a) le fait que le premier paiement provienne d'un compte détenu au nom du client, à titre individuel ou joint, auprès d'un établissement de crédit ou d'un établissement financier réglementé de l'EEE ou d'un pays tiers dont les exigences en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme ne sont pas moins strictes que celles prévues par la directive (UE) 2015/849;

    b) l'envoi au client d'un code généré de manière aléatoire pour confirmer la présence pendant le processus de vérification à distance. Le code doit être un code à usage unique et limité dans le temps;

    c) la capture de données biométriques pour les comparer aux données recueillies par le biais d'autres sources indépendantes et fiables;

    d) les contacts téléphoniques avec le client;

    e) l'envoi direct de courriers (qu'ils soient électroniques ou postaux) au client.

45. Les établissements de crédit et les établissements financiers doivent remplir les critères indiqués au paragraphe 38 à 43 si la solution utilise l'un des moyens suivants:

    a) des schémas d'identification électronique notifiés conformément à l'article 9 du règlement (UE) n° 910/2014 et satisfaisant aux exigences en matière de niveaux de garantie «substantiel» ou «élevé» conformément à l'article 8 dudit règlement;

    b) des services de confiance qualifiés au sens du règlement (UE) n° 910/2014, en particulier le chapitre III, section 3, et l'article 24, paragraphe 1, alinéa 2, point b), dudit règlement.

4.5 Recours à des tiers et externalisation

46. En complément des points énoncés au paragraphe 9, les établissements de crédit et les établissements financiers doivent inclure dans leurs politiques et procédures des spécifications précisant les fonctions et activités d'entrée en relation d'affaires à distance qui seront exécutées ou réalisées par l'établissement de crédit et l'établissement financier, par des tiers ou par un autre prestataire de services externe.

4.5.1 Recours à des tiers conformément au chapitre II, section 4, de la directive (UE) 2015/849

47. En complément des orientations de l'ABE relatives aux facteurs de risque[8], en particulier les paragraphes 2.20 à 2.21 et 4.32 à 4.37 de ces orientations, ils doivent appliquer les critères suivants:

    a) prendre les mesures nécessaires pour s'assurer que les processus et procédures d'entrée en relation d'affaires à distance mis en œuvre par le tiers dans le cadre des obligations de vigilance à l'égard de la clientèle et que les informations et données qu'ils permettent de recueillir dans ce contexte sont suffisantes et conformes aux exigences énoncées dans les présentes orientations;

    b) garantir la continuité des relations d'affaires établies entre le client et l'établissement de crédit et l'établissement financier pour se prémunir contre des événements pouvant mettre en lumière des défaillances concernant le processus d'entrée en relation d'affaires à distance entrepris par le tiers.

4.5.2 Externalisation des mesures de vigilance à l'égard de la clientèle

48. Lorsque les établissements de crédit et les établissements financiers externalisent tout ou partie du processus d'entrée en relation d'affaires à distance à un prestataire de services externe, tel que visé à l'article 29 de la directive (UE) 2015/849, les établissements de crédit et les établissements financiers doivent appliquer, en plus des paragraphes 2.20 à 2.21 et 4.32 à 4.37 des orientations de l'ABE relatives à l'externalisation[9] , avant et pendant la relation avec le prestataire de services externe, les mesures suivantes, dont l'étendue doit être adaptée selon une approche par les risques:

    a) s'assurer que le prestataire de services externe met en œuvre et respecte de manière effective les politiques et procédures d'entrée en relation d'affaires à distance de l'établissement de crédit et de l'établissement financier, conformément au contrat d'externalisation. Cet objectif devrait être atteint au moyen de rapports réguliers, d'un suivi continu, de visites sur place ou d'analyse d'échantillons;

[8] EBA/GL/2021/02

[9] EBA Guidelines on outsourcing arrangements.docx (europa.eu)

b) réaliser des évaluations pour s'assurer que le prestataire de services externe est suffisamment équipé et capable d'effectuer le processus d'entrée en relation d'affaires à distance. Les évaluations peuvent comprendre, entre autres, l'évaluation de la formation du personnel, du caractère approprié de la technologie et de la gouvernance des données au niveau du prestataire de services externe;

c) s'assurer que le prestataire de services externe informe les établissements de crédit et les établissements financiers de toutes les propositions de changements du processus d'entrée en relation d'affaires à distance ou de toute modification apportée à la solution fournie par le prestataire de services externe.

49. Lorsque le prestataire de services externe stocke des données relatives au client, notamment des photographies, vidéos et documents, pendant le processus d'entrée en relation d'affaires à distance, les établissements de crédit et les établissements financiers doivent s'assurer que:

a) seules les données nécessaires sur le client sont recueillies et stockées, dans le respect d'une période de conservation clairement définie;

b) l'accès aux données est strictement limité et enregistré;

c) des mesures de sécurité appropriées sont mises en œuvre pour garantir que les données stockées sont protégées.

4.6 Gestion des risques liés aux TIC et à la sécurité

50. Les établissements de crédit et les établissements financiers doivent identifier et gérer leurs risques liés aux TIC et à la sécurité relatifs à l'utilisation du processus d'entrée en relation d'affaires à distance, y compris lorsque les établissements de crédit et les établissements financiers s'appuient sur des tiers ou lorsque le service est externalisé, y compris à des entités du groupe.

51. En plus de satisfaire aux exigences énoncées dans les orientations de l'ABE sur la gestion des risques liés aux TIC et à la sécurité lorsqu'elles sont applicables[10], les établissements de crédit et les établissements financiers doivent utiliser des canaux de communication sécurisés pour interagir avec le client pendant le processus d'entrée en relation d'affaires à distance. La solution d'entrée en relation d'affaires à distance doit utiliser des protocoles et des algorithmes cryptographiques sécurisés conformes aux bonnes pratiques du secteur, afin de préserver, dans la mesure du possible, la confidentialité, l'authenticité et l'intégrité des données échangées.

52. Les établissements de crédit et les établissements financiers doivent offrir un point d'accès sécurisé pour le démarrage du processus d'entrée en relation d'affaires à distance fondé sur des certificats qualifiés de cachets électroniques tels que visés à l'article 3, paragraphe 30, du

[10] EBA/GL/2019/04

règlement (UE) nº 910/2014 ou des certificats qualifiés d'authentification de sites internet tels que visés à l'article 3, paragraphe 39, dudit règlement. Le client doit également être informé des mesures de sécurité applicables qui doivent être prises pour garantir une utilisation sécurisée du système.

53. Lorsqu'un appareil multifonctionnel est utilisé pour exécuter le processus d'entrée en relation d'affaires à distance, un environnement sécurisé doit être utilisé pour l'exécution du code logiciel côté client, le cas échéant. Des mesures de sécurité supplémentaires doivent être mises en œuvre pour garantir la sécurité et la fiabilité du code logiciel et des données recueillies, conformément à l'évaluation des risques de sécurité telle qu'énoncée dans les orientations de l'ABE sur la gestion des risques liés aux TIC et à la sécurité.

4.7 Respect des présentes orientations lorsque les établissements de crédit et les établissements financiers utilisent des services de confiance et des processus d'identification nationaux tels que visés à l'article 13, paragraphe 1, point a), de la directive (UE) 2015/849

54. Les établissements de crédit et les établissements financiers peuvent avoir recours à des services de confiance pertinents et à des processus d'identification électronique réglementés, reconnus, approuvés ou acceptés par les autorités nationales compétentes telles que visées à l'article 13, paragraphe 1, point a), de la directive (UE) 2015/849 pour se conformer aux présentes orientations. Lorsqu'ils ont recours à ces solutions, les établissements de crédit et les établissements financiers doivent évaluer dans quelle mesure la solution respecte les dispositions contenues dans les présentes orientations et appliquer les mesures nécessaires pour atténuer tout risque pertinent découlant du recours à ces solutions. Ils doivent notamment déterminer si les risques suivants sont pris en compte:

    a) les risques liés à l'authentification et énoncés dans les mesures d'atténuation de leurs politiques et procédures, en particulier les risques de fraude à l'identité;

    b) le risque que l'identité du client ne corresponde pas à l'identité déclarée;

    c) le risque de perte, vol, suspension, nullité ou expiration d'un justificatif d'identité, comprenant, le cas échéant, les outils permettant de détecter et de prévenir l'utilisation de fraudes à l'identité.