EBA/GL/2022/15

22/11/2022

Κατευθυντήριες γραμμές

σχετικά με τη χρήση λύσεων εξ αποστάσεως ταυτοποίησης πελατών σύμφωνα με το άρθρο 13 παράγραφος 1 της οδηγίας (ΕΕ) 2015/849

1. Συμμόρφωση και υποχρεώσεις υποβολής στοιχείων και αναφορών

Καθεστώς των κατευθυντήριων γραμμών

1. Το παρόν έγγραφο περιέχει κατευθυντήριες γραμμές οι οποίες εκδίδονται βάσει του άρθρου 16 του κανονισμού (ΕΕ) αριθ. 1093/2010 [1] . Σύμφωνα με το άρθρο 16 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 1093/2010, οι αρμόδιες αρχές και τα χρηματοοικονομικά ιδρύματα καταβάλλουν κάθε δυνατή προσπάθεια για να συμμορφωθούν προς τις κατευθυντήριες γραμμές.

2. Οι κατευθυντήριες γραμμές παρουσιάζουν την άποψη της ΕΑΤ σχετικά με τις ενδεδειγμένες εποπτικές πρακτικές στο πλαίσιο του Ευρωπαϊκού Συστήματος Χρηματοοικονομικής Εποπτείας ή σχετικά με τον τρόπο ορθής εφαρμογής της ενωσιακής νομοθεσίας στον συγκεκριμένο τομέα. Οι αρμόδιες αρχές, όπως ορίζονται στο άρθρο 4 παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 1093/2010, προς τις οποίες απευθύνονται οι κατευθυντήριες γραμμές, πρέπει να συμμορφωθούν ενσωματώνοντάς τες δεόντως στις πρακτικές τους (π.χ. τροποποιώντας το νομικό τους πλαίσιο ή τις εποπτικές διαδικασίες τους), συμπεριλαμβανομένων των σημείων στα οποία οι κατευθυντήριες γραμμές απευθύνονται κυρίως στα ιδρύματα.

Απαιτήσεις υποβολής αναφορών

3. Σύμφωνα με το άρθρο 16 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 1093/2010, οι αρμόδιες αρχές πρέπει να γνωστοποιήσουν στην ΕΑΤ εάν συμμορφώνονται ή προτίθενται να συμμορφωθούν προς τις παρούσες κατευθυντήριες γραμμές, ή άλλως να εκθέσουν τους λόγους μη συμμόρφωσης, έως τις 30.05.2023. Εάν η προθεσμία γνωστοποίησης παρέλθει άπρακτη, η ΕΑΤ θεωρεί ότι οι αρμόδιες αρχές δεν συμμορφώνονται. Οι γνωστοποιήσεις πρέπει να αποστέλλονται, με την υποβολή του εντύπου που παρέχεται στον διαδικτυακό τόπο της ΕΑΤ, με την επισήμανση «EBA/GL/2022/15». Οι γνωστοποιήσεις πρέπει να υποβάλλονται από πρόσωπα δεόντως εξουσιοδοτημένα να γνωστοποιούν τη συμμόρφωση εκ μέρους των αρμόδιων αρχών τους. Οποιαδήποτε μεταβολή στην κατάσταση συμμόρφωσης πρέπει επίσης να αναφέρεται στην ΕΑΤ.

4. Οι γνωστοποιήσεις δημοσιεύονται στον διαδικτυακό τόπο της ΕΑΤ, σύμφωνα με το άρθρο 16 παράγραφος 3.

[1] Κανονισμός (ΕΕ) αριθ. 1093/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Νοεμβρίου 2010, σχετικά με τη σύσταση Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Τραπεζών), την τροποποίηση της απόφασης αριθ. 716/2009/ΕΚ και την κατάργηση της απόφασης 2009/78/ΕΚ της Επιτροπής (ΕΕ L 331, της 15.12.2010, σ. 12).

2. Αντικείμενο, πεδίο εφαρμογής και ορισμοί

Αντικείμενο και πεδίο εφαρμογής

5. Οι παρούσες κατευθυντήριες γραμμές καθορίζουν τα μέτρα που θα πρέπει να λαμβάνουν τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί κατά τη θέσπιση ή την επανεξέταση των λύσεων με σκοπό τη συμμόρφωση προς τις υποχρεώσεις τους βάσει του άρθρου 13 παράγραφος 1 στοιχεία α), β) και γ) της οδηγίας (ΕΕ) 2015/849 [2] για την εξ αποστάσεως ταυτοποίηση νέων πελατών. Καθορίζει επίσης τα μέτρα που θα πρέπει να λαμβάνουν τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί όταν βασίζονται σε τρίτα μέρη σύμφωνα με το κεφάλαιο ΙΙ, τμήμα 4 της οδηγίας (ΕΕ) 2015/849, καθώς και τις πολιτικές, τους ελέγχους και τις διαδικασίες που θα πρέπει να εφαρμόζουν τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί σε σχέση με τη δέουσα επιμέλεια ως προς τον πελάτη (ΔΕΠ) σύμφωνα με το άρθρο 8 παράγραφοι 3 και παράγραφος 4 στοιχείο α) της οδηγίας (ΕΕ) 2015/849 όταν τα μέτρα ΔΕΠ εφαρμόζονται εξ αποστάσεως.

6. Οι αρμόδιες αρχές θα πρέπει να λαμβάνουν υπόψη τις παρούσες κατευθυντήριες γραμμές κατά την εκτίμηση της επάρκειας και της αποτελεσματικότητας των μέτρων που λαμβάνουν τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί για να συμμορφωθούν προς τις υποχρεώσεις που υπέχουν σύμφωνα με την οδηγία (ΕΕ) 2015/849 στο πλαίσιο της εξ αποστάσεως ταυτοποίησης πελατών.

Αποδέκτες

7. Οι παρούσες κατευθυντήριες γραμμές απευθύνονται στις αρμόδιες αρχές, όπως ορίζονται στο άρθρο 4 παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 1093/2010. Οι παρούσες κατευθυντήριες γραμμές απευθύνονται επίσης στους φορείς του χρηματοοικονομικού τομέα όπως ορίζονται στο άρθρο 4 παράγραφος 1 του κανονισμού αυτού, ήτοι στα πιστωτικά ιδρύματα και τους χρηματοπιστωτικούς οργανισμούς όπως ορίζονται στο άρθρο 3 παράγραφοι 1 και 2 της οδηγίας (ΕΕ) 2015/849.

[2] Οδηγία (ΕΕ) 2015/849 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Μαΐου 2015, σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας

Ορισμοί

8. Εκτός εάν προβλέπεται διαφορετικά, οι όροι που χρησιμοποιούνται και ορίζονται στην οδηγία (ΕΕ) 2015/849 έχουν την ίδια έννοια και στις κατευθυντήριες γραμμές. Επιπλέον, για τους σκοπούς του παρόντος εγγράφου ισχύουν οι ακόλουθοι ορισμοί:

Βιομετρικά δεδομένα	Δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με φυσικά, φυσιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου, τα οποία επιτρέπουν την αδιαμφισβήτητη ταυτοποίησή του, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα που αποκτώνται και υποβάλλονται σε επεξεργασία με χρήση τεχνικών μέσων.

3. Εφαρμογή

Ημερομηνία εφαρμογής

Οι παρούσες κατευθυντήριες γραμμές τίθενται σε ισχύ από 02.10.2023.

4. Κατευθυντήριες γραμμές σχετικά με τη χρήση λύσεων εξ αποστάσεως ταυτοποίησης πελατών σύμφωνα με το άρθρο 13 παράγραφος 1 της οδηγίας (ΕΕ) 2015/849

4.1 Εσωτερικές πολιτικές και διαδικασίες

4.1.1 Πολιτικές και διαδικασίες σχετικά με την εξ αποστάσεως ταυτοποίηση πελατών

9. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να εφαρμόζουν και να τηρούν πολιτικές και διαδικασίες για τη συμμόρφωσή τους προς τις υποχρεώσεις που υπέχουν σύμφωνα με το άρθρο 13 παράγραφος 1 στοιχεία α), β) και γ) της οδηγίας (ΕΕ) 2015/849 σε περιπτώσεις εξ αποστάσεως ταυτοποίησης πελατών. Οι εν λόγω πολιτικές και διαδικασίες θα πρέπει να προβλέπουν μέτρα ανάλογα με τον βαθμό κινδύνου και να καθορίζουν τουλάχιστον:

    α) γενική περιγραφή της λύσης που εφαρμόζουν τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί για τη συλλογή, την επαλήθευση και την αρχειοθέτηση πληροφοριών που αφορούν το σύνολο της διαδικασίας εξ αποστάσεως ταυτοποίησης πελατών. Η περιγραφή αυτή θα πρέπει να περιλαμβάνει επεξήγηση των χαρακτηριστικών και της λειτουργίας της λύσης·

    β) τις περιπτώσεις στις οποίες μπορεί να χρησιμοποιηθεί η λύση της εξ αποστάσεως ταυτοποίησης πελατών, λαμβανομένων υπόψη των παραγόντων κινδύνου που προσδιορίζονται και αξιολογούνται σύμφωνα με το άρθρο 8 παράγραφος 1 της οδηγίας (ΕΕ) 2015/849 και της συνολικής εκτίμησης κινδύνου για ολόκληρη την επιχείρηση, συμπεριλαμβανομένης της περιγραφής της κατηγορίας πελατών, προϊόντων και υπηρεσιών που είναι επιλέξιμη για εξ αποστάσεως ταυτοποίηση·

    γ) ποια στάδια είναι πλήρως αυτόνομα και ποια απαιτούν ανθρώπινη παρέμβαση·

    δ) τους ελέγχους που εφαρμόζονται για να διασφαλίζεται ότι η πρώτη συναλλαγή με εξ αποστάσεως ενταγμένο νέο πελάτη εκτελείται μόνον αφού θα έχουν εφαρμοστεί όλα τα αρχικά μέτρα δέουσας επιμέλειας ως προς τον πελάτη (ΔΕΠ)·

    ε) περιγραφή της εισαγωγικής εκπαίδευσης και των προγραμμάτων τακτικής κατάρτισης που διασφαλίζουν την ευαισθητοποίηση του προσωπικού και την επικαιροποίηση των γνώσεών του όσον αφορά τη λειτουργία της λύσης εξ

αποστάσεως ταυτοποίησης πελατών, τους συναφείς κινδύνους, καθώς και τις πολιτικές και τις διαδικασίες που αποσκοπούν στον μετριασμό αυτών των κινδύνων κατά την εξ αποστάσεως ταυτοποίηση πελατών.

10. Η εφαρμογή αυτών των πολιτικών και διαδικασιών θα πρέπει να διασφαλίζει τη συμμόρφωση των πιστωτικών ιδρυμάτων και των χρηματοπιστωτικών οργανισμών προς τις διατάξεις της ενότητας 4.2 έως 4.7 των παρουσών κατευθυντηρίων γραμμών.

4.1.2 Διακυβέρνηση

11. Επιπλέον των διατάξεων που θεσπίζονται στην ενότητα 4.2.4 των κατευθυντήριων γραμμών της ΕΑΤ σχετικά με τον υπεύθυνο συμμόρφωσης[3], ο υπεύθυνος συμμόρφωσης σε θέματα ΚΞΧ/ΧΤ[4] θα πρέπει, στο πλαίσιο του γενικού καθήκοντός του να προετοιμάζει πολιτικές και διαδικασίες που θα συμμορφώνονται προς τις απαιτήσεις ΔΕΠ, να διασφαλίζει την αποτελεσματική εφαρμογή, την τακτική επανεξέταση και την κατά περίπτωση τροποποίηση των πολιτικών και των διαδικασιών για την εξ αποστάσεως ταυτοποίηση πελατών.

12. Το διοικητικό όργανο του πιστωτικού ιδρύματος ή και του χρηματοπιστωτικού οργανισμού θα πρέπει να εγκρίνει τις πολιτικές και τις διαδικασίες για την εξ αποστάσεως ταυτοποίηση πελατών και να εποπτεύει την ορθή εφαρμογή τους.

4.1.3 Η προ της εφαρμογής αξιολόγηση της λύσης εξ αποστάσεως ταυτοποίησης πελατών

13. Κατά την εξέταση σκοπιμότητας της υιοθέτησης νέας λύσης εξ αποστάσεως ταυτοποίησης πελατών, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να διενεργούν αξιολόγηση της λύσης εξ αποστάσεως ταυτοποίησης πελατών πριν από την υλοποίηση της.

14. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να καθορίζουν το πεδίο εφαρμογής, τα στάδια και τις απαιτήσεις τήρησης αρχείων της προ της εφαρμογής αξιολόγησης στις πολιτικές και τις διαδικασίες τους, οι οποίες θα πρέπει να περιλαμβάνουν τουλάχιστον:

    α) αξιολόγηση της επάρκειας της λύσης όσον αφορά την πληρότητα και την ακρίβεια των στοιχείων και των εγγράφων που πρόκειται να συλλεχθούν, καθώς και την αξιοπιστία και την ανεξαρτησία των χρησιμοποιούμενων πηγών πληροφοριών·

    β) αξιολόγηση της επίπτωσης της χρήσης της λύσης εξ αποστάσεως ταυτοποίησης πελατών στους κινδύνους για ολόκληρη την επιχείρηση, συμπεριλαμβανομένων

[3] Σχέδιο κατευθυντήριων γραμμών για τις πολιτικές και τις διαδικασίες σε σχέση με τη διαχείριση της συμμόρφωσης και τον ρόλο και τις αρμοδιότητες του υπευθύνου συμμόρφωσης με τις απαιτήσεις σε θέματα ΚΞΧ/ΧΤ σύμφωνα με το άρθρο 8 και το κεφάλαιο VI της οδηγίας (ΕΕ) 2015/849.

[4] Σύμφωνα με τα κριτήρια αναλογικότητας που καθορίζονται στην ενότητα 4.2.2 των κατευθυντηρίων γραμμών σχετικά με τον υπεύθυνο συμμόρφωσης.

των κινδύνων ΞΧ/ΧΤ, των επιχειρησιακών κινδύνων, των κινδύνων φήμης και των νομικών κινδύνων·

γ) προσδιορισμό των πιθανών μέτρων μετριασμού και διορθωτικών ενεργειών για κάθε κίνδυνο που εντοπίζεται στο πλαίσιο της αξιολόγησης βάσει του στοιχείου β)·

δ) ελέγχους εκτίμησης κινδύνων απάτης, συμπεριλαμβανομένων των κινδύνων πλαστοπροσωπίας και άλλων κινδύνων των τεχνολογιών πληροφοριών και επικοινωνιών («ΤΠΕ») και κινδύνων ασφάλειας, σύμφωνα με τη διάταξη 43 των κατευθυντηρίων γραμμών της ΕΑΤ σχετικά με τη διαχείριση κινδύνων ΤΠΕ και ασφάλειας[5].

ε) ελέγχους από άκρο σε άκρο σχετικά με τη λειτουργία της λύσης που εστιάζει σε πελάτη/-ες, προϊόν/-τα και υπηρεσία/-ες που προσδιορίζεται/-ονται στις πολιτικές και τις διαδικασίες για την εξ αποστάσεως ταυτοποίηση πελατών.

15. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να μεριμνούν ώστε να πληρούνται τα κριτήρια της παραγράφου 14 στοιχεία α), δ) και ε) όταν η λύση χρησιμοποιεί κάποιο από τα ακόλουθα μέσα:

α) συστήματα ηλεκτρονικής ταυτοποίησης που κοινοποιούνται σύμφωνα με το άρθρο 9 του κανονισμού (ΕΕ) αριθ. 910/2014 και πληρούν τις απαιτήσεις επιπέδου διασφάλισης «βασικό» ή «υψηλό» σύμφωνα με το άρθρο 8 του κανονισμού αυτού·

β) εγκεκριμένες υπηρεσίες εμπιστοσύνης που πληρούν τις απαιτήσεις του κανονισμού (ΕΕ) αριθ. 910/2014, ειδικότερα τις απαιτήσεις του κεφαλαίου III, τμήμα 3 και του άρθρου 24 παράγραφος 1, εδάφιο 2, στοιχείο β) του εν λόγω κανονισμού.

16. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να είναι σε θέση να αποδείξουν στην οικεία αρμόδια αρχή ποιες αξιολογήσεις διενήργησαν πριν από την εφαρμογή της λύσης εξ αποστάσεως ταυτοποίησης πελατών, το αποτέλεσμα της αξιολόγησής τους και την καταλληλότητα της χρήσης της υπό το πρίσμα των κινδύνων ΞΧ/ΧΤ που προσδιορίστηκαν για τους τύπους πελάτη/-ών, υπηρεσίας/-ών, γεωγραφικών περιοχών και προϊόντος/-ων που εμπίπτουν στο πεδίο εφαρμογής της.

17. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να θέσουν σε εφαρμογή τη λύση εξ αποστάσεως ταυτοποίησης πελατών μόνον αφού θα έχουν βεβαιωθεί ότι μπορεί να ενσωματωθεί στο ευρύτερο σύστημα εσωτερικού ελέγχου του πιστωτικού ιδρύματος και του χρηματοπιστωτικού οργανισμού, ώστε το πιστωτικό ίδρυμα και ο χρηματοπιστωτικός οργανισμός να δύναται να διαχειριστεί επαρκώς τους κινδύνους ΞΧ/ΧΤ που ενδέχεται να προκύψουν από τη χρήση της λύσης εξ αποστάσεως ταυτοποίησης πελατών.

[5] EBA/GL/2019/04

4.1.4 Συνεχής παρακολούθηση της λύσης εξ αποστάσεως ταυτοποίησης πελατών

18. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να παρακολουθούν τη λύση εξ αποστάσεως ταυτοποίησης πελατών σε συνεχή βάση για να διασφαλίζουν ότι η εφαρμογή της συνάδει με τις προσδοκίες των πιστωτικών ιδρυμάτων και των χρηματοπιστωτικών οργανισμών. Θα πρέπει να συμπληρώνουν τις πολιτικές και τις διαδικασίες τους που περιγράφονται στην παράγραφο 9 με περιγραφή που θα αφορά τουλάχιστον τα ακόλουθα σημεία:

    α) τα μέτρα που θα λάβουν για να διασφαλίσουν τη συνεχιζόμενη ποιότητα, την πληρότητα, την ακρίβεια και την επάρκεια των στοιχείων που συλλέγονται στο πλαίσιο της διαδικασίας εξ αποστάσεως ταυτοποίησης πελατών, τα οποία θα πρέπει να είναι ανάλογα των κινδύνων ΞΧ/ΧΤ στους οποίους εκτίθεται το πιστωτικό ίδρυμα και ο χρηματοπιστωτικός οργανισμός·

    β) το πεδίο εφαρμογής και τη συχνότητα αυτών των τακτικών ελέγχων· και

    γ) τις περιστάσεις που οδηγούν σε ad hoc επανεξέταση, μεταξύ των οποίων θα πρέπει να περιλαμβάνονται τουλάχιστον οι εξής:

        α. αλλαγές όσον αφορά την έκθεση του πιστωτικού ιδρύματος και του χρηματοπιστωτικού οργανισμού στον κίνδυνο ΞΧ/ΧΤ·

        β. ελλείψεις που εντοπίστηκαν κατά τη λειτουργία της λύσης στο πλαίσιο της παρακολούθησης, του ελέγχου ή των εποπτικών δραστηριοτήτων·

        γ. εικαζόμενη αύξηση των αποπειρών απάτης·

        δ. μεταβολές στο νομικό ή το κανονιστικό πλαίσιο.

19. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να καθορίζουν στις οικείες διαδικασίες και διεργασίες διορθωτικά μέτρα που λαμβάνονται σε περίπτωση επέλευσης του κινδύνου ή σε περιπτώσεις εντοπισμού σφαλμάτων με αντίκτυπο στην αποδοτικότητα και την αποτελεσματικότητα της γενικής λύσης εξ αποστάσεως ταυτοποίησης πελατών. Μεταξύ των μέτρων αυτών θα πρέπει να περιλαμβάνονται τουλάχιστον:

    α) επανεξέταση όλων των επιχειρηματικών σχέσεων που επηρεάζονται, προκειμένου να αξιολογηθεί κατά πόσον η αρχική ΔΕΠ που εφαρμόστηκε από τα πιστωτικά ιδρύματα και τους χρηματοπιστωτικούς οργανισμούς ήταν επαρκής στο πλαίσιο της συμμόρφωσής τους προς το άρθρο 13 παράγραφος 1 στοιχεία α), β) και γ) της οδηγίας (ΕΕ) 2015/849. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να εξετάζουν κατά προτεραιότητα τις επιχειρηματικές σχέσεις που ενέχουν τον υψηλότερο κίνδυνο ΞΧ/ΧΤ·

β) λαμβανομένων υπόψη των πληροφοριών που συλλέγονται στο πλαίσιο της προαναφερθείσας επανεξέτασης, αξιολόγηση του κατά πόσον οι επιχειρηματικές σχέσεις που επηρεάζονται θα πρέπει:

α. να υπόκεινται σε πρόσθετα μέτρα δέουσας επιμέλειας·

β. να υπόκεινται σε περιορισμούς, π.χ. σε όρια ως προς τον όγκο της συναλλαγής, εφόσον επιτρέπονται από το εθνικό δίκαιο, έως ότου διενεργηθεί ή εν λόγω επανεξέταση·

γ. να τερματίζονται·

δ. να αναφέρονται στη μονάδα χρηματοοικονομικών πληροφοριών (ΜΧΠ)·

ε. να αναταξινομούνται σε διαφορετική κατηγορία κινδύνου.

20. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να αναζητούν τον πλέον αποτελεσματικό τρόπο διαρκούς παρακολούθησης της επάρκειας και αξιοπιστίας των λύσεων εξ αποστάσεως ταυτοποίησης πελατών. Θα πρέπει να εξετάζουν ένα ή περισσότερα από τα, ενδεικτικώς αναφερόμενα, παρακάτω μέσα:

i. δοκιμές διασφάλισης ποιότητας·

ii. αυτόματες κρίσιμες προειδοποιήσεις και κοινοποιήσεις

iii. τακτικές αυτόματες εκθέσεις για θέματα ποιότητας·

iv. δειγματοληπτικές δοκιμές·

v. μη αυτόματες επανεξετάσεις.

21. Η ενότητα αυτή εφαρμόζεται επίσης όταν χρησιμοποιούνται πλήρως αυτόματες λύσεις εξ αποστάσεως ταυτοποίησης πελατών οι οποίες εξαρτώνται σε πολύ σημαντικό βαθμό από αυτόματους αλγόριθμους, χωρίς ή με ελάχιστη ανθρώπινη παρέμβαση.

22. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να είναι σε θέση να αποδείξουν στην οικεία αρμόδια αρχή ποιες επανεξετάσεις διενήργησαν και ποια διορθωτικά μέτρα εφάρμοσαν για να θεραπεύσουν τυχόν ελλείψεις που εντοπίστηκαν καθ’ όλη τη διάρκεια ζωής της λύσης της εξ αποστάσεως ταυτοποίησης πελατών.

4.2 Απόκτηση πληροφοριών

4.2.1 Ταυτοποίηση του πελάτη

23. Επιπλέον των σημείων που αναφέρονται στην παράγραφο 9, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να καθορίζουν στις πολιτικές και τις διαδικασίες τους τις πληροφορίες που απαιτούνται για την ταυτοποίηση του πελάτη, τους τύπους των εγγράφων, τα στοιχεία ή τις πληροφορίες που θα χρησιμοποιεί το πιστωτικό ίδρυμα και ο χρηματοπιστωτικός οργανισμός για την επαλήθευση της ταυτότητας του πελάτη και τον τρόπο επαλήθευσης αυτών των πληροφοριών.

24. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να διασφαλίζουν ότι:

    α) οι πληροφορίες που λαμβάνονται μέσω της λύσης εξ αποστάσεως ταυτοποίησης πελατών είναι επικαιροποιημένες και πληρούν τα ισχύοντα νομικά και κανονιστικά πρότυπα για την αρχική δέουσα επιμέλεια ως προς τον πελάτη·

    β) τυχόν εικόνες, βίντεο, ηχογραφήσεις και στοιχεία καταγράφονται σε αναγνώσιμη μορφή και με επαρκή ποιότητα ώστε ο πελάτης να είναι αναγνωρίσιμος πέραν πάσης αμφιβολίας·

    γ) η διαδικασία ταυτοποίησης δεν συνεχίζεται εάν διαπιστωθούν τεχνικά προβλήματα ή απροσδόκητες διακοπές της σύνδεσης.

25. Τα πιστωτικά ιδρύματα ή οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να μεριμνούν ώστε να πληρούνται τα κριτήρια της παραγράφου 24 όταν η λύση χρησιμοποιεί κάποιο από τα ακόλουθα μέσα:

    α) συστήματα ηλεκτρονικής ταυτοποίησης που κοινοποιούνται σύμφωνα με το άρθρο 9 του κανονισμού (ΕΕ) αριθ. 910/2014 και πληρούν τις απαιτήσεις επιπέδου διασφάλισης «βασικό» ή «υψηλό» σύμφωνα με το άρθρο 8 του κανονισμού αυτού·

    β) εγκεκριμένες υπηρεσίες εμπιστοσύνης που πληρούν τις απαιτήσεις του κανονισμού (ΕΕ) αριθ. 910/2014, ειδικότερα στο κεφάλαιο III, τμήμα 3 και στο άρθρο 24 παράγραφος 1, εδάφιο 2, στοιχείο β) του κανονισμού αυτού.

26. Έγγραφα και πληροφορίες που συλλέγονται κατά τη διάρκεια της διαδικασίας εξ αποστάσεως ταυτοποίησης, τα οποία απαιτείται να διατηρούνται σύμφωνα με το άρθρο 40 παράγραφος 1 στοιχείο α) της οδηγίας (ΕΕ) 2015/849, θα πρέπει να είναι χρονοσφραγισμένα και να διατηρούνται ασφαλή από το πιστωτικό ίδρυμα και τον χρηματοπιστωτικό οργανισμό. Το περιεχόμενο των αποθηκευμένων αρχείων, συμπεριλαμβανομένων των εικόνων, των βίντεο, των ηχογραφήσεων και των δεδομένων, θα πρέπει να είναι διαθέσιμο σε αναγνώσιμη μορφή και να επιδέχεται εκ των υστέρων επαληθεύσεις.

4.2.2 Ταυτοποίηση φυσικών προσώπων

27. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να προσδιορίζουν στις πολιτικές τους, όπως καθορίζονται στην ενότητα 4.1.1 παράγραφος 9, τις πληροφορίες που απαιτείται να προσκομίζονται για την εξ αποστάσεως ταυτοποίηση των πελατών σύμφωνα με το άρθρο 13 παράγραφος 1 στοιχεία α) και γ) της οδηγίας (ΕΕ) 2015/849. Επιπλέον, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να καθορίζουν ποιες πληροφορίες:

    α) υποβάλλονται με μη αυτόματο τρόπο από τον πελάτη·

    β) προκύπτουν αυτόματα από τα έγγραφα που υποβάλλονται από τον πελάτη·

    γ) συγκεντρώνονται με τη χρήση εσωτερικών και εξωτερικών πηγών.

28. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να εφαρμόζουν και να διατηρούν κατάλληλους μηχανισμούς που θα διασφαλίζουν ότι οι πληροφορίες που προκύπτουν αυτόματα σύμφωνα με την παράγραφο 27 είναι αξιόπιστες. Θα πρέπει να εφαρμόζουν ελέγχους για την αντιμετώπιση των σχετικών κινδύνων, συμπεριλαμβανομένων των κινδύνων που σχετίζονται με αυτόματη συλλογή των δεδομένων, όπως είναι η απόκρυψη της τοποθεσίας της συσκευής του πελάτη ή η χρήση πλαστών διευθύνσεων πρωτοκόλλου Ίντερνετ (IP) ή υπηρεσιών εικονικών ιδιωτικών δικτύων (VPN).

4.2.3 Ταυτοποίηση νομικών οντοτήτων

29. Εφόσον τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί εντάσσουν εξ αποστάσεως πελάτες που είναι νομικές οντότητες, θα πρέπει να καθορίζουν στις πολιτικές και τις διαδικασίες τους, όπως προβλέπεται στην ενότητα 4.1.1 παράγραφος 9, ποια κατηγορία νομικών οντοτήτων θα εντάσσουν εξ αποστάσεως, λαμβάνοντας υπόψη το επίπεδο του κινδύνου ΞΧ/ΧΤ που συνδέεται με κάθε κατηγορία, καθώς και το επίπεδο ανθρώπινης παρέμβασης που χρειάζεται για την επικύρωση των πληροφοριών ταυτοποίησης.

30. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να διασφαλίζουν ότι η λύση εξ αποστάσεως ταυτοποίησης πελατών διαθέτει χαρακτηριστικά για τη συλλογή:

    α) όλων των σχετικών δεδομένων και εγγράφων για την εξακρίβωση και την επαλήθευση της ταυτότητας του νομικού προσώπου·

    β) όλων των σχετικών δεδομένων και εγγράφων βάσει των οποίων επαληθεύεται ότι το φυσικό πρόσωπο που ενεργεί εκ μέρους του νομικού προσώπου έχει την εξουσιοδότηση να ενεργεί υπό την ιδιότητα αυτή·

γ) των πληροφοριών σχετικά με τους πραγματικούς δικαιούχους σύμφωνα με τη διάταξη 4.12 των κατευθυντηρίων γραμμών της ΕΑΤ σχετικά με τους παράγοντες κινδύνου[6].

31. Όσον αφορά το φυσικό πρόσωπο που ενεργεί εκ μέρους νομικού προσώπου, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να εφαρμόζουν τη διαδικασία ταυτοποίησης που προβλέπεται στην ενότητα 4.2.2.

4.2.4 Φύση και σκοπός της επιχειρηματικής σχέσης

32. Όταν τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί αξιολογούν και, κατά περίπτωση, αποκτούν πληροφορίες σχετικά με τον σκοπό και τη σκοπούμενη φύση της επιχειρηματικής σχέσης σύμφωνα με το άρθρο 13 παράγραφος 1 στοιχείο γ) της οδηγίας (ΕΕ) 2015/849, όπως προσδιορίζονται περαιτέρω στην ενότητα 4.38 των κατευθυντηρίων γραμμών της ΕΑΤ σχετικά με τους παράγοντες κινδύνου, θα πρέπει, για τους σκοπούς των παρουσών κατευθυντηρίων γραμμών, να έχουν περατώσει τις σχετικές ενέργειες πριν από το πέρας της διαδικασίας εξ αποστάσεως ταυτοποίησης πελατών.

4.3 Αυθεντικότητα και ακεραιότητα εγγράφων

33. Όταν τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί κάνουν δεκτές αναπαραγωγές αυθεντικού εγγράφου και δεν εξετάζουν το αυθεντικό έγγραφο, θα πρέπει να λαμβάνουν μέτρα για να επιβεβαιώσουν ότι η αναπαραγωγή είναι αξιόπιστη. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να εξακριβώνουν τουλάχιστον τα εξής:

α) το κατά πόσον η αναπαραγωγή περιλαμβάνει χαρακτηριστικά ασφαλείας ενσωματωμένα στο πρωτότυπο έγγραφο και κατά πόσον οι προδιαγραφές του πρωτότυπου εγγράφου που αναπαράγονται, ειδικότερα ο τύπος, το μέγεθος των χαρακτήρων και η δομή του εγγράφου, είναι έγκυρες και αποδεκτές, μέσω σύγκρισης με επίσημες βάσεις δεδομένων, όπως η PRADO[7]·

β) το ότι τα δεδομένα προσωπικού χαρακτήρα δεν έχουν τροποποιηθεί ή άλλως παραποιηθεί ή, κατά περίπτωση, ότι δεν αντικαταστάθηκε η ενσωματωμένη στο έγγραφο φωτογραφία του πελάτη·

γ) την ακεραιότητα του αλγόριθμου που χρησιμοποιήθηκε για τη δημιουργία του μοναδικού αναγνωριστικού αριθμού του πρωτότυπου εγγράφου, σε περίπτωση επίσημου εγγράφου που εκδόθηκε με μηχανικώς αναγνώσιμη ζώνη (MRZ)·

[6] EBA/GL/2021/02

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

δ) το εάν η παρασχεθείσα αναπαραγωγή είναι επαρκούς ποιότητας και ευκρίνειας ώστε να διασφαλίζεται η σαφήνεια της σχετικής πληροφορίας πέραν πάσης αμφιβολίας·

ε) το ότι η υποβληθείσα αναπαραγωγή δεν προβλήθηκε σε οθόνη ως φωτογραφία ή προϊόν σάρωσης του πρωτότυπου εγγράφου ταυτότητας.

34. Όταν τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί χρησιμοποιούν χαρακτηριστικά για την αυτόματη ανάγνωση πληροφοριών από έγγραφα, όπως αλγόριθμους οπτικής αναγνώρισης χαρακτήρων (OCR) ή επαληθεύσεις μηχανικώς αναγνώσιμης ζώνης (MRZ), θα πρέπει να λαμβάνουν τα αναγκαία μέτρα που θα διασφαλίζουν ότι τα εργαλεία αυτά συλλέγουν τις πληροφορίες με ακρίβεια και συνέπεια.

35. Οσάκις η συσκευή που χρησιμοποιεί ο πελάτης προς απόδειξη της ταυτότητάς του παρέχει τη δυνατότητα συλλογής των σχετικών δεδομένων, για παράδειγμα επειδή τα δεδομένα περιέχονται στο μικροκύκλωμα του εθνικού δελτίου ταυτότητας, και, ως εκ τούτου, είναι από τεχνική άποψη εφικτή η πρόσβαση των πιστωτικών ιδρυμάτων και των χρηματοπιστωτικών οργανισμών στα δεδομένα αυτά, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να εξετάζουν το ενδεχόμενο να χρησιμοποιήσουν αυτές τις πληροφορίες προκειμένου να επαληθεύσουν τη συνέπειά τους με πληροφορίες που απέκτησαν από άλλες πηγές, όπως τα υποβληθέντα στοιχεία ή άλλα έγγραφα που υπέβαλε ο πελάτης.

36. Κατά περίπτωση, κατά τη διάρκεια της διαδικασίας επαλήθευσης, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να επαληθεύουν τα χαρακτηριστικά ασφάλειας, εφόσον υπάρχουν, τα οποία έχουν ενσωματωθεί στο επίσημο έγγραφο, π.χ. ολογραφήματα, ως απόδειξη της αυθεντικότητας του εγγράφου.

37. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να καθορίζουν στις πολιτικές και τις διαδικασίες τους τον τρόπο προσαρμογής των οικείων απαιτήσεων τεκμηρίωσης για τους σκοπούς της χρηματοοικονομικής ένταξης. Όταν, συνεπεία αυτής της προσαρμογής, γίνονται δεκτά έγγραφα μειωμένης αξιοπιστίας ή μη παραδοσιακά έγγραφα ταυτοποίησης, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει, επιπροσθέτως των μέτρων που προβλέπονται στην παράγραφο 4.10 των κατευθυντηρίων γραμμών της ΕΑΤ σχετικά με τους παράγοντες κινδύνου, να διενεργούν ελέγχους ή να αυξάνουν την ανθρώπινη παρέμβαση προκειμένου να βεβαιωθούν ότι κατανοούν τον κίνδυνο ΞΧ/ΧΤ που σχετίζεται με την επιχειρηματική σχέση.

4.4 Η αντιστοίχιση της ταυτότητας του πελάτη ως μέρος της διαδικασίας επαλήθευσης

38. Οι λύσεις εξ αποστάσεως ταυτοποίησης των πελατών που εφαρμόζονται από τα πιστωτικά ιδρύματα και τους χρηματοπιστωτικούς οργανισμούς θα πρέπει, τουλάχιστον, να παρέχουν τις ακόλουθες δυνατότητες στο πλαίσιο της οικείας διαδικασίας επαλήθευσης:

    α) αντιστοίχιση μεταξύ των οπτικών στοιχείων του φυσικού προσώπου και των υποβληθέντων εγγράφων·

    β) εφόσον ο πελάτης είναι νομική οντότητα, να είναι καταχωρισμένη σε δημόσιο μητρώο, κατά περίπτωση·

    γ) εφόσον ο πελάτης είναι νομική οντότητα, το φυσικό πρόσωπο που τον εκπροσωπεί να έχει το δικαίωμα να ενεργεί εκ μέρους του.

39. Όταν η λύση εξ αποστάσεως ταυτοποίησης πελατών περιλαμβάνει τη χρήση βιομετρικών στοιχείων για την επαλήθευση της ταυτότητας του πελάτη, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να διασφαλίζουν ότι τα βιομετρικά στοιχεία είναι επαρκώς μοναδικά ώστε να συνδέονται ανεπιφύλακτα με ένα και μόνο φυσικό πρόσωπο. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να χρησιμοποιούν ισχυρούς και αξιόπιστους αλγόριθμους για την επαλήθευση της αντιστοίχισης μεταξύ των παρεχόμενων με το υποβληθέν έγγραφο ταυτότητας βιομετρικών στοιχείων και του υπό ταυτοποίηση πελάτη. Σε περίπτωση που η λύση δεν παρέχει το απαιτούμενο επίπεδο βεβαιότητας, θα πρέπει να διενεργούνται πρόσθετοι έλεγχοι.

40. Όταν η ποιότητα των αποδεικτικών στοιχείων που υποβάλλονται κρίνεται ανεπαρκής με αποτέλεσμα να προκύπτει ασάφεια η αβεβαιότητα που επηρεάζει την εκτέλεση των εξ αποστάσεως ελέγχων, η διαδικασία εξ αποστάσεως ταυτοποίησης του συγκεκριμένου πελάτη θα πρέπει να διακόπτεται και να ξεκινά εκ νέου ή να ανακατευθύνεται προς τη διά ζώσης επαλήθευση.

41. Όταν τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί χρησιμοποιούν αυτόματες λύσεις εξ αποστάσεως ταυτοποίησης, στο πλαίσιο των οποίων ο πελάτης δεν αλληλεπιδρά με κάποιον υπάλληλο που διενεργεί τη διαδικασία επαλήθευσης, θα πρέπει:

    α) να διασφαλίζουν ότι η φωτογραφία/οι φωτογραφίες ή οι μαγνητοσκοπήσεις λαμβάνονται υπό συνθήκες επαρκούς φωτισμού και ότι τα απαιτούμενα χαρακτηριστικά αποτυπώνονται με την αναγκαία ευκρίνεια, η οποία θα επιτρέψει τη δέουσα επαλήθευση της ταυτότητας του πελάτη·

    β) να διασφαλίζουν ότι η φωτογραφία/οι φωτογραφίες ή οι μαγνητοσκοπήσεις λαμβάνονται κατά τη διάρκεια της διαδικασίας επαλήθευσης της ταυτότητας του πελάτη·

γ) να επαληθεύουν την ενεργό συμμετοχή του πελάτη, ήτοι με την ενδεχόμενη εφαρμογή διαδικασιών στο πλαίσιο των οποίων ο πελάτης καλείται να προβεί σε συγκεκριμένες ενέργειες που θα επαληθεύουν την παρουσία του κατά τη διάρκεια της επικοινωνίας μαζί του ή διαδικασιών που μπορεί να βασίζονται στην ανάλυση των ληφθέντων στοιχείων και δεν απαιτούν κάποια συγκεκριμένη ενέργεια εκ μέρους του πελάτη·

δ) να χρησιμοποιούν ισχυρούς και αξιόπιστους αλγόριθμους για να επαληθεύουν εάν η/οι φωτογραφία/-ες ή τα βίντεο που ελήφθησαν αντιστοιχίζονται με την/τις εικόνα/-ες που ανακτήθηκαν από επίσημο/-α έγγραφο/-α του πελάτη.

42. Όταν τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί χρησιμοποιούν λύσεις εξ αποστάσεως ταυτοποίησης πελατών, στο πλαίσιο των οποίων ο πελάτης αλληλεπιδρά με υπάλληλο που εφαρμόζει τη διαδικασία επαλήθευσης, θα πρέπει:

α) να διασφαλίζουν ότι η ποιότητα της εικόνας και του βίντεο είναι επαρκής και επιτρέπει τη δέουσα επαλήθευση της ταυτότητας του πελάτη, καθώς και ότι χρησιμοποιούνται αξιόπιστα τεχνολογικά συστήματα για τον σκοπό αυτό·

β) να προβλέπουν τη συμμετοχή ενός υπαλλήλου με επαρκή γνώση των διατάξεων ΚΞΧ/ΧΤ και των πτυχών ασφαλείας της εξ αποστάσεως επαλήθευσης και ο οποίος είναι επαρκώς εκπαιδευμένος για να προβλέπει και να προλαμβάνει την εσκεμμένη ή δόλια χρήση τεχνικών εξαπάτησης που σχετίζονται με την εξ αποστάσεως επαλήθευση, καθώς και για να εντοπίζει και να αντιμετωπίζει τα σχετικά συμβάντα·

γ) να καταρτίζουν οδηγό συνεντεύξεων που θα καθορίζει τα επόμενα στάδια της διαδικασίας εξ αποστάσεως επαλήθευσης, καθώς και τις ενέργειες που απαιτούνται από τον υπάλληλο. Ο οδηγός συνέντευξης θα πρέπει να περιλαμβάνει καθοδήγηση σχετικά με την παρατήρηση και τον εντοπισμό ψυχολογικών παραγόντων ή άλλων χαρακτηριστικών τα οποία ενδέχεται να χαρακτηρίζουν κάποια ύποπτη συμπεριφορά κατά τη διάρκεια της εξ αποστάσεως επαλήθευσης.

43. Στο μέτρο του δυνατού, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να χρησιμοποιούν λύσεις εξ αποστάσεως ταυτοποίησης πελατών που περιλαμβάνουν τυχαία ακολουθία ενεργειών τις οποίες θα πρέπει να εκτελεί ο πελάτης για σκοπούς επαλήθευσης της ταυτότητάς του και προκειμένου τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί να προστατεύονται από τη χρήση συνθετικών ταυτοτήτων ή ενεργειών εξαναγκασμού. Στο μέτρο του δυνατού, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει επίσης να προβλέπουν την τυχαία ανάθεση πελατών στον υπάλληλο που είναι αρμόδιος για την εφαρμογή της διαδικασίας εξ αποστάσεως επαλήθευσης ώστε να αποτρέπεται το ενδεχόμενο αθέμιτης σύμπραξης μεταξύ πελάτη και αρμόδιου υπαλλήλου.

44. Επιπλέον των ανωτέρω, και αναλογικά με τον κίνδυνο ΞΧ/ΧΤ που σχετίζεται με την επιχειρηματική σχέση, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα

πρέπει να εφαρμόζουν έναν ή περισσότερους από τους παρακάτω ελέγχους ή κάποιο παρόμοιο μέτρο με στόχο την ενίσχυση της αξιοπιστίας της διαδικασίας επαλήθευσης. Μεταξύ των εν λόγω ελέγχων ή μέτρων περιλαμβάνονται, ενδεικτικά, οι ακόλουθες ενέργειες:

α) η αρχική πληρωμή γίνεται μέσω λογαριασμού, με μοναδικό δικαιούχο ή συνδικαιούχο τον πελάτη, ο οποίος τηρείται σε ρυθμιζόμενο πιστωτικό ίδρυμα ή ρυθμιζόμενο χρηματοπιστωτικό οργανισμό εντός του ΕΟΧ ή σε τρίτη χώρα που προβλέπει απαιτήσεις ΚΞΧ/ΧΤ οι οποίες δεν είναι λιγότερο αυστηρές από τις αντίστοιχες απαιτήσεις της οδηγίας (ΕΕ) 2015/849·

β) Αποστολή τυχαία παραγόμενου κωδικού πρόσβασης στον πελάτη για να επιβεβαιώσει την παρουσία του κατά τη διάρκεια της διαδικασίας εξ αποστάσεως επαλήθευσης. Ο κωδικός πρόσβασης πρέπει να είναι μίας χρήσης και περιορισμένης χρονικής διάρκειας ισχύος·

γ) συλλογή βιομετρικών στοιχείων προς σύγκριση με στοιχεία τα οποία συλλέγονται μέσω άλλων ανεξάρτητων και αξιόπιστων πηγών·

δ) τηλεφωνική επικοινωνία με τον πελάτη·

ε) άμεσο ταχυδρομείο (ηλεκτρονικό και μέσω ταχυδρομικής υπηρεσίας) με τον πελάτη.

45. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να θεωρούν ότι πληρούνται τα κριτήρια των παραγράφων 38 έως 43 όταν η λύση χρησιμοποιεί κάποιο από τα ακόλουθα μέσα:

α) συστήματα ηλεκτρονικής ταυτοποίησης που κοινοποιούνται σύμφωνα με το άρθρο 9 του κανονισμού (ΕΕ) αριθ. 910/2014 και πληρούν τις απαιτήσεις επιπέδου διασφάλισης «βασικό» ή «υψηλό» σύμφωνα με το άρθρο 8 του κανονισμού αυτού·

β) εγκεκριμένες υπηρεσίες εμπιστοσύνης που πληρούν τις απαιτήσεις του κανονισμού (ΕΕ) αριθ. 910/2014, ειδικότερα του κεφαλαίου ΙΙΙ, τμήμα 3 και του άρθρου 24 παράγραφος 1, εδάφιο 2, στοιχείο β) του εν λόγω κανονισμού.

4.5 Στήριξη σε τρίτα μέρη και εξωτερική ανάθεση

46. Επιπλέον των σημείων που αναφέρονται στην παράγραφο 9, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να περιλαμβάνουν στις πολιτικές και τις διαδικασίες τους τις προδιαγραφές βάσει των οποίων καθορίζονται οι λειτουργίες της εξ αποστάσεως ταυτοποίησης πελατών που εφαρμόζονται ή εκτελούνται από το πιστωτικό ίδρυμα και τον χρηματοπιστωτικό οργανισμό, από τρίτους ή από άλλον εξωτερικό πάροχο υπηρεσιών.

4.5.1 Στήριξη σε τρίτα μέρη σύμφωνα με το κεφάλαιο II τμήμα 4 της οδηγίας (ΕΕ) 2015/849

47. Επιπλέον των κατευθυντηρίων γραμμών της ΕΑΤ σχετικά με τους παράγοντες κινδύνου[8], ειδικότερα των κατευθυντηρίων γραμμών 2.20 έως 2.21, 4.32 έως 4.37 των εν λόγω κατευθυντηρίων γραμμών, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να εφαρμόζουν τα ακόλουθα κριτήρια:

α) λαμβάνουν τα αναγκαία μέτρα για να βεβαιωθούν ότι οι διαδικασίες για την εξ αποστάσεως διενέργεια ΜΔΕ που εφαρμόζει το τρίτο μέρος, καθώς και οι πληροφορίες που το τρίτο μέρος συλλέγει στο πλαίσιο αυτό, είναι επαρκείς και συνεπείς με τις απαιτήσεις που θεσπίζονται στις παρούσες κατευθυντήριες γραμμές·

β) διασφαλίζουν τη συνέχεια των επιχειρηματικών σχέσεων που δημιουργούνται μεταξύ του πελάτη και του πιστωτικού ιδρύματος ή του χρηματοπιστωτικού οργανισμού ώστε να προστατεύονται από συμβάντα τα οποία ενδέχεται να αποκαλύψουν ελλείψεις της διαδικασίας εξ αποστάσεως ταυτοποίησης πελατών που εφαρμόζει το τρίτο μέρος.

4.5.2 Εξωτερική ανάθεση της ΔΕΠ

48. Όταν τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί αναθέτουν εν όλω ή εν μέρει τη διαδικασία εξ αποστάσεως ταυτοποίησης πελατών σε εξωτερικό πάροχο υπηρεσιών, όπως ορίζεται στο άρθρο 29 της οδηγίας (ΕΕ) 2015/849, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να εφαρμόζουν, επιπλέον των κατευθυντηρίων γραμμών 2.20 έως 2.21, 4.32 έως 4.37 των κατευθυντηρίων γραμμών της ΕΑΤ σχετικά με τους παράγοντες κινδύνου και των κατευθυντηρίων γραμμών της ΕΑΤ σχετικά με την εξωτερική ανάθεση[9] κατά περίπτωση, πριν και κατά τη διάρκεια της επιχειρηματικής σχέσης με τον εξωτερικό πάροχο υπηρεσιών, τα ακόλουθα μέτρα, η έκταση των οποίων θα πρέπει να προσαρμόζεται ανάλογα με τον βαθμό του κινδύνου:

α) να διασφαλίζουν ότι ο πάροχος υπηρεσιών στον οποίο έχει γίνει η εξωτερική ανάθεση εφαρμόζει αποτελεσματικά και συμμορφώνεται προς τις πολιτικές και τις διαδικασίες εξ αποστάσεως ταυτοποίησης πελατών του πιστωτικού ιδρύματος και του χρηματοπιστωτικού οργανισμού σύμφωνα με τη συμφωνία εξωτερικής ανάθεσης. Η συμμόρφωση αυτή θα πρέπει να επιτυγχάνεται μέσω τακτικής υποβολής εκθέσεων, συνεχιζόμενης παρακολούθησης, πραγματοποίησης επιτόπιων επισκέψεων ή διεξαγωγής δειγματοληπτικών δοκιμών·

β) να διενεργούν αξιολογήσεις για να διασφαλίζουν ότι ο πάροχος υπηρεσιών στον οποίο έχει γίνει η εξωτερική ανάθεση διαθέτει επαρκή εξοπλισμό και είναι ικανός

[8] EBA/GL/2016/02.

[9] Κατευθυντήριες γραμμές της ΕΑΤ σχετικά με την εξωτερική ανάθεση δραστηριοτήτων.docx (europa.eu)

να εφαρμόζει τη διαδικασία εξ αποστάσεως ταυτοποίησης πελατών. Μεταξύ των αξιολογήσεων περιλαμβάνονται, ενδεικτικά, η αξιολόγηση της κατάρτισης του προσωπικού, της καταλληλότητας της τεχνολογίας και της διακυβέρνησης των δεδομένων του παρόχου υπηρεσιών στον οποίο έχει γίνει η εξωτερική ανάθεση·

γ) να διασφαλίζουν ότι ο πάροχος υπηρεσιών στον οποίο έχει γίνει η εξωτερική ανάθεση ενημερώνει τα πιστωτικά ιδρύματα και τους χρηματοπιστωτικούς οργανισμούς για οποιεσδήποτε προτεινόμενες αλλαγές της διαδικασίας εξ αποστάσεως ταυτοποίησης πελατών ή οποιαδήποτε τροποποίηση της λύσης που παρέχεται από τον εξωτερικό πάροχο υπηρεσιών.

49. Όταν ο εξωτερικός πάροχος υπηρεσιών αποθηκεύει δεδομένα πελατών, μεταξύ των οποίων, ενδεικτικά, φωτογραφίες, βίντεο και έγγραφα, κατά τη διάρκεια της διαδικασίας εξ αποστάσεως ταυτοποίησης πελατών, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να διασφαλίζουν ότι:

α) συλλέγονται και αποθηκεύονται μόνο τα αναγκαία δεδομένα του πελάτη για σαφώς καθορισμένη περίοδο διατήρησης·

β) η πρόσβαση στα δεδομένα είναι αυστηρά περιορισμένη και καταγράφεται·

γ) εφαρμόζονται μέτρα ασφαλείας για τη διασφάλιση της προστασίας των αποθηκευμένων δεδομένων.

4.6 Διαχείριση κινδύνων ΤΠΕ και ασφάλειας

50. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να προσδιορίζουν και να διαχειρίζονται τους οικείους κινδύνους ΤΠΕ και ασφάλειας που σχετίζονται με την εφαρμογή της διαδικασίας εξ αποστάσεως ταυτοποίησης πελατών, συμπεριλαμβανομένων των περιπτώσεων όπου πιστωτικά ιδρύματα και χρηματοπιστωτικοί οργανισμοί στηρίζονται σε τρίτα μέρη ή στην περίπτωση της εξωτερικής ανάθεσης των υπηρεσιών, μεταξύ άλλων, σε οντότητες του ομίλου.

51. Επιπλέον της συμμόρφωσης προς τις απαιτήσεις που καθορίζονται στις κατευθυντήριες γραμμές της ΕΑΤ σχετικά με τη διαχείριση κινδύνων ΤΠΕ και ασφάλειας[10] κατά περίπτωση, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να χρησιμοποιούν ασφαλείς διαύλους επικοινωνίας για την αλληλεπίδραση με τον πελάτη κατά τη διάρκεια της διαδικασίας εξ αποστάσεως ταυτοποίησης πελατών. Η λύση εξ αποστάσεως ταυτοποίησης πελατών θα πρέπει να χρησιμοποιεί ασφαλή πρωτόκολλα και κρυπτογραφικούς αλγόριθμους σύμφωνα με τις βέλτιστες πρακτικές του κλάδου για τη διασφάλιση της εμπιστευτικότητας, της αυθεντικότητας και της ακεραιότητας των ανταλλασσόμενων δεδομένων, κατά περίπτωση.

[10] EBA/GL/2019/04

52. Τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να παρέχουν ασφαλές σημείο πρόσβασης για την εκκίνηση της διαδικασίας εξ αποστάσεως ταυτοποίησης πελατών βάσει εγκεκριμένων πιστοποιητικών ηλεκτρονικών σφραγίδων, όπως ορίζεται στο άρθρο 3 σημείο 30 του κανονισμού (ΕΕ) αριθ. 910/2014, ή πιστοποιητικό για την επαλήθευση της γνησιότητας του ιστοτόπου, όπως ορίζεται στο άρθρο 3 σημείο 39 του εν λόγω κανονισμού. Ο πελάτης θα πρέπει επίσης να ενημερώνεται σχετικά με τα ισχύοντα μέτρα ασφαλείας που θα πρέπει να λαμβάνονται για τη διασφάλιση της ασφαλούς χρήσης του συστήματος.

53. Όταν χρησιμοποιείται συσκευή πολλαπλών χρήσεων για την εφαρμογή της διαδικασίας εξ αποστάσεως ταυτοποίησης πελατών, θα πρέπει να χρησιμοποιείται ασφαλές περιβάλλον για την κατά περίπτωση εκτέλεση του κώδικα λογισμικού από τον πελάτη. Θα πρέπει να εφαρμόζονται πρόσθετα μέτρα ασφαλείας προκειμένου να διασφαλίζεται η ασφάλεια και η αξιοπιστία του κώδικα λογισμικού και των συλλεχθέντων δεδομένων, σύμφωνα με την αξιολόγηση των κινδύνων για την ασφάλεια που προβλέπεται στις κατευθυντήριες γραμμές της ΕΑΤ σχετικά με τη διαχείριση κινδύνων ΤΠΕ και ασφάλειας.

4.7 Συμμόρφωση προς τις εν λόγω κατευθυντήριες γραμμές όταν τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί χρησιμοποιούν υπηρεσίες εμπιστοσύνης και εθνικές διαδικασίες ταυτοποίησης σύμφωνα με το άρθρο 13 παράγραφος 1 στοιχείο α) της οδηγίας (ΕΕ) 2015/849.

54. Για τη συμμόρφωσή τους προς τις παρούσες κατευθυντήριες γραμμές, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί μπορούν να χρησιμοποιούν κατάλληλες υπηρεσίες εμπιστοσύνης και διαδικασίες ηλεκτρονικής ταυτοποίησης οι οποίες ρυθμίζονται, αναγνωρίζονται, εγκρίνονται ή γίνονται δεκτές από τις αρμόδιες εθνικές αρχές σύμφωνα με το άρθρο 13 παράγραφος 1 στοιχείο α) της οδηγίας (ΕΕ) 2015/849. Όταν χρησιμοποιούν τέτοιες λύσεις, τα πιστωτικά ιδρύματα και οι χρηματοπιστωτικοί οργανισμοί θα πρέπει να αξιολογούν τον βαθμό συμμόρφωσης της εκάστοτε λύσης προς τις διατάξεις των παρουσών κατευθυντηρίων γραμμών και να εφαρμόζουν τα αναγκαία μέτρα για τον μετριασμό τυχόν κινδύνων που προκύπτουν από τη χρήση της. Ειδικότερα, θα πρέπει να λαμβάνουν υπόψη κατά πόσον αντιμετωπίζονται οι ακόλουθοι κίνδυνοι:

α) οι κίνδυνοι που άπτονται της επαλήθευσης της γνησιότητας, τους οποίους πρέπει να αντιμετωπίζουν καθορίζοντας στις πολιτικές και τις διαδικασίες τους ειδικά μέτρα μετριασμού, ιδίως για την αντιμετώπιση των κινδύνων απάτης μέσω πλαστοπροσωπίας·

β) ο κίνδυνος η πραγματική ταυτότητα του πελάτη να μην είναι η δηλωθείσα ταυτότητα·

γ) ο κίνδυνος απώλειας, κλοπής, αναστολής, ανάκλησης ή λήξης του αποδεικτικού στοιχείου ταυτότητας, συμπεριλαμβανομένων, κατά περίπτωση, των εργαλείων εντοπισμού και πρόληψης κρουσμάτων υποκλοπής ταυτότητας.