I

(Νομοθετικές πράξεις)

ΚΑΝΟΝΙΣΜΟΙ

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2022/2554 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 14ης Δεκεμβρίου 2022

σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 114,

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Κεντρικής Τράπεζας ([1]),

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής ([2]),

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία ([3]),

Εκτιμώντας τα ακόλουθα:

(1) Στην ψηφιακή εποχή, οι τεχνολογίες των πληροφοριών και των επικοινωνιών (ΤΠΕ) υποστηρίζουν σύνθετα συστήματα που χρησιμοποιούνται για καθημερινές δραστηριότητες. Διασφαλίζουν την αδιάλειπτη λειτουργία των οικονομιών μας σε βασικούς τομείς, συμπεριλαμβανομένου του χρηματοοικονομικού τομέα, και ενισχύουν τη λειτουργία της εσωτερικής αγοράς. Η αυξημένη ψηφιοποίηση και διασυνδεσιμότητα εντείνουν επίσης τους κινδύνους ΤΠΕ, οι οποίοι καθιστούν την κοινωνία συνολικά —και ειδικότερα το χρηματοοικονομικό σύστημα— πιο ευάλωτη σε κυβερνοαπειλές ή διαταραχές των ΤΠΕ. Μολονότι η καθολική χρήση των συστημάτων ΤΠΕ και ο υψηλός βαθμός ψηφιοποίησης και συνδεσιμότητας αποτελούν σήμερα βασικά χαρακτηριστικά των δραστηριοτήτων των χρηματοοικονομικών οντοτήτων της Ένωσης, η ψηφιακή τους ανθεκτικότητα δεν έχει ακόμη αντιμετωπιστεί και ενσωματωθεί καλύτερα στα ευρύτερα επιχειρησιακά τους πλαίσια.

(2) Κατά τις προηγούμενες δεκαετίες, η χρήση ΤΠΕ έχει κατακτήσει καθοριστικό ρόλο στην παροχή χρηματοοικονομικών υπηρεσιών, σε σημείο που έχει πλέον αποκτήσει κρίσιμη σημασία για τη διασφάλιση των συνήθων καθημερινών λειτουργιών όλων των χρηματοοικονομικών οντοτήτων. Η ψηφιοποίηση καλύπτει πλέον, για παράδειγμα, τις πληρωμές, οι οποίες από τα μετρητά και τα έντυπα μέσα στρέφονται πλέον ολοένα και περισσότερο στη χρήση ψηφιακών λύσεων, καθώς και την εκκαθάριση και τον διακανονισμό τίτλων, τις ηλεκτρονικές και αλγοριθμικές συναλλαγές, τις πράξεις δανεισμού και χρηματοδότησης, τη χρηματοδότηση μεταξύ ομοτίμων, την αξιολόγηση πιστοληπτικής ικανότητας, τη διαχείριση

([1]) ΕΕ C 343 της 26.8.2021, σ. 1.
([2]) ΕΕ C 155 της 30.4.2021, σ. 38.
([3]) Θέση του Ευρωπαϊκού Κοινοβουλίου της 10ης Νοεμβρίου 2022 (δεν έχει ακόμη δημοσιευθεί στην Επίσημη Εφημερίδα) και απόφαση του Συμβουλίου της 28ης Νοεμβρίου 2022.

απαιτήσεων και τις υπηρεσίες υποστήριξης (back-office). Η χρήση ΤΠΕ μετασχημάτισε επίσης τον ασφαλιστικό τομέα, από την εμφάνιση ασφαλιστικών διαμεσολαβητών που προσφέρουν τις υπηρεσίες τους μέσω διαδικτύου και λειτουργούν με την InsurTech, έως την ψηφιακή ανάληψη ασφαλιστικών κινδύνων. Εκτός του υψηλού βαθμού ψηφιοποίησης σε ολόκληρο τον χρηματοοικονομικό τομέα, η ψηφιοποίηση έχει εμβαθύνει επίσης τις διασυνδέσεις και τις εξαρτήσεις εντός του χρηματοοικονομικού τομέα, καθώς και με τρίτους παρόχους υποδομών και υπηρεσιών.

(3) Σε έκθεση του 2020 σχετικά με τον συστημικό κίνδυνο στον κυβερνοχώρο, το Ευρωπαϊκό Συμβούλιο Συστημικών Κινδύνων (ΕΣΣΚ) επιβεβαίωσε τον τρόπο με τον οποίο το υφιστάμενο υψηλό επίπεδο διασυνδεσιμότητας μεταξύ των χρηματοοικονομικών οντοτήτων, των χρηματοοικονομικών αγορών και των υποδομών χρηματοοικονομικών αγορών, και ιδίως οι αλληλεξαρτήσεις των οικείων συστημάτων ΤΠΕ, θα μπορούσε να αποτελέσει συστημική ευπάθεια, δεδομένου ότι τοπικά κυβερνοπεριστατικά θα μπορούσαν να εξαπλωθούν ταχέως από οποιαδήποτε από τις περίπου 22 000 χρηματοοικονομικές οντότητες της Ένωσης σε ολόκληρο το χρηματοοικονομικό σύστημα, χωρίς να εμποδίζονται από τα γεωγραφικά σύνορα. Οι σοβαρές παραβιάσεις των ΤΠΕ που ανακύπτουν στον χρηματοοικονομικό τομέα δεν επηρεάζουν μόνο μεμονωμένες χρηματοοικονομικές οντότητες. Διευκολύνουν επίσης τη διάδοση τοπικών ευπαθειών στους διαύλους μετάδοσης και μπορούν να έχουν δυσμενείς συνέπειες για τη σταθερότητα του χρηματοοικονομικού συστήματος της Ένωσης, φέρ' ειπείν προκαλώντας εκροές ρευστότητας και συνολική απώλεια της αξιοπιστίας των χρηματοοικονομικών αγορών και της εμπιστοσύνης σε αυτές.

(4) Κατά τα τελευταία έτη, οι κίνδυνοι ΤΠΕ έχουν προσελκύσει την προσοχή διεθνών ενωσιακών και εθνικών φορέων χάραξης πολιτικής, ρυθμιστικών αρχών και οργανισμών τυποποίησης, στο πλαίσιο μιας απόπειρας να ενισχυθεί η ψηφιακή ανθεκτικότητα, να καθοριστούν πρότυπα και να συντονιστούν οι ρυθμιστικές ή εποπτικές εργασίες. Σε διεθνές επίπεδο, η Επιτροπή της Βασιλείας για την Τραπεζική Εποπτεία, η Επιτροπή Πληρωμών και Υποδομών Αγορών, το Συμβούλιο Χρηματοπιστωτικής Σταθερότητας, το Ίδρυμα Χρηματοπιστωτικής Σταθερότητας, καθώς και οι G7 και G20, έχουν θέσει ως στόχο την παροχή εργαλείων στις αρμόδιες αρχές και στους διαχειριστές αγοράς σε διάφορες δικαιοδοσίες για την ενίσχυση της ανθεκτικότητας των χρηματοοικονομικών τους συστημάτων. Το έργο αυτό υπαγορεύθηκε επίσης από την ανάγκη να ληφθούν δεόντως υπόψη οι κίνδυνοι ΤΠΕ στο πλαίσιο ενός εξαιρετικά διασυνδεδεμένου παγκόσμιου χρηματοοικονομικού συστήματος και να επιδιωχθεί μεγαλύτερη συνοχή των σχετικών βέλτιστων πρακτικών.

(5) Παρά την ανάληψη ενωσιακών και εθνικών πολιτικών και νομοθετικών πρωτοβουλιών, οι κίνδυνοι ΤΠΕ εξακολουθούν να συνιστούν πρόκληση για την επιχειρησιακή ανθεκτικότητα, τις επιδόσεις και τη σταθερότητα του χρηματοοικονομικού συστήματος της Ένωσης. Οι μεταρρυθμίσεις που ακολούθησαν τη χρηματοοικονομική κρίση του 2008 ενίσχυσαν πρωτίστως τη χρηματοοικονομική ανθεκτικότητα του χρηματοοικονομικού τομέα της Ένωσης και είχε ως στόχο τη διασφάλιση της ανταγωνιστικότητας και της σταθερότητας της Ένωσης από την οπτική γωνία της οικονομίας, της προληπτικής εποπτείας και της δεοντολογίας της αγοράς. Μολονότι η ασφάλεια των ΤΠΕ και η ψηφιακή ανθεκτικότητα αποτελούν μέρος του επιχειρησιακού κινδύνου, δεν τέθηκαν δεόντως στο επίκεντρο του κανονιστικού θεματολογίου μετά τη χρηματοοικονομική κρίση, ενώ έχουν αναπτυχθεί μόνο σε ορισμένους τομείς του πολιτικού και κανονιστικού πλαισίου της Ένωσης για τις χρηματοοικονομικές υπηρεσίες ή μόνο σε μερικά κράτη μέλη.

(6) Στην ανακοίνωσή της της 8ης Μαρτίου 2018 με τίτλο «Σχέδιο δράσης για τη χρηματοοικονομική τεχνολογία: Για έναν πιο ανταγωνιστικό και καινοτόμο ευρωπαϊκό χρηματοπιστωτικό τομέα», η Επιτροπή επισήμανε τη θεμελιώδη σημασία της ενίσχυσης της ανθεκτικότητας του χρηματοοικονομικού τομέα της Ένωσης, μεταξύ άλλων, από επιχειρησιακής πλευράς για τη διασφάλιση της τεχνολογικής ασφάλειας και της άρτιας λειτουργίας του, καθώς και της ταχείας ανάκαμψής του από παραβιάσεις και συμβάντα που σχετίζονται με τις ΤΠΕ, ώστε να καταστεί εντέλει δυνατή η αποτελεσματική και ομαλή παροχή χρηματοοικονομικών υπηρεσιών σε ολόκληρη την Ένωση, μεταξύ άλλων υπό συνθήκες ακραίων καταστάσεων, ενώ θα διατηρείται παράλληλα η αξιοπιστία της αγοράς και η εμπιστοσύνη των καταναλωτών σε αυτήν.

(7) Τον Απρίλιο του 2019, η Ευρωπαϊκή Εποπτική Αρχή (Ευρωπαϊκή Αρχή Τραπεζών) (ΕΑΤ), η οποία συγκροτήθηκε με τον κανονισμό (ΕΕ) αριθ. 1093/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([4]), η Ευρωπαϊκή Εποπτική Αρχή (Ευρωπαϊκή Αρχή Ασφαλίσεων και Επαγγελματικών Συντάξεων) («ΕΑΑΕΣ»), η οποία συγκροτήθηκε με τον κανονισμό (ΕΕ) αριθ. 1094/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([5]), και η Ευρωπαϊκή Εποπτική Αρχή (Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών) (ΕΑΚΑΑ), η οποία συγκροτήθηκε με τον κανονισμό (ΕΕ) αριθ. 1095/2010 του

([4]) 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).

([5]) Κανονισμός (ΕΕ) αριθ. 1094/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Νοεμβρίου 2010, για τη σύσταση Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Ασφαλίσεων και Επαγγελματικών Συντάξεων), την τροποποίηση της απόφασης αριθ. 716/2009/ΕΚ και την κατάργηση της απόφασης 2009/79/ΕΚ της Επιτροπής (ΕΕ L 331 της 15.12.2010, σ. 48).

Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6]) (συλλογικά γνωστές ως «Ευρωπαϊκές Εποπτικές Αρχές» ή «ΕΕΑ»), εξέδωσαν από κοινού τεχνικές γνωμοδοτήσεις, στις οποίες διατύπωναν έκκληση για συνεκτική προσέγγιση όσον αφορά τους κινδύνους ΤΠΕ στον χρηματοοικονομικό τομέα και σύσταση για ενίσχυση της ψηφιακής επιχειρησιακής ανθεκτικότητας του κλάδου των χρηματοοικονομικών υπηρεσιών, κατά τρόπο αναλογικό, μέσω ειδικής τομεακής πρωτοβουλίας της Ένωσης.

(8) Ο χρηματοοικονομικός τομέας της Ένωσης ρυθμίζεται από ενιαίο εγχειρίδιο κανόνων και διέπεται από το ευρωπαϊκό σύστημα χρηματοοικονομικής εποπτείας. Ωστόσο, οι διατάξεις που αφορούν την ψηφιακή επιχειρησιακή ανθεκτικότητα και την ασφάλεια ΤΠΕ δεν έχουν εναρμονιστεί ακόμη πλήρως ή με συνεκτικό τρόπο, παρά το γεγονός ότι η ψηφιακή επιχειρησιακή ανθεκτικότητα είναι ζωτικής σημασίας για τη διασφάλιση της χρηματοοικονομικής σταθερότητας και της ακεραιότητας της αγοράς στην ψηφιακή εποχή και είναι εξίσου σημαντική, για παράδειγμα, με τα κοινά πρότυπα προληπτικής εποπτείας ή δεοντολογίας της αγοράς. Κατά συνέπεια, το ενιαίο εγχειρίδιο κανόνων και το σύστημα εποπτείας θα πρέπει να εξελιχθούν ώστε να καλύπτουν και την ψηφιακή επιχειρησιακή ανθεκτικότητα, με την ενίσχυση των εντολών των αρμόδιων αρχών για να μπορούν να εποπτεύουν τη διαχείριση των κινδύνων ΤΠΕ στον χρηματοοικονομικό τομέα, προκειμένου να προστατεύουν την ακεραιότητα και την αποτελεσματικότητα της εσωτερικής αγοράς και να διευκολύνουν την εύρυθμη λειτουργία της.

(9) Οι νομοθετικές διαφορές και οι ανομοιόμορφες εθνικές κανονιστικές και εποπτικές προσεγγίσεις όσον αφορά τους κινδύνους ΤΠΕ εγείρουν φραγμούς στη λειτουργία της εσωτερικής αγοράς χρηματοοικονομικών υπηρεσιών, παρεμποδίζοντας με τον τρόπο αυτόν την απρόσκοπτη άσκηση της ελευθερίας εγκατάστασης και της παροχής υπηρεσιών για τις χρηματοοικονομικές οντότητες που λειτουργούν σε διασυνοριακή βάση. Είναι επίσης πιθανό να προκαλούνται στρεβλώσεις στον ανταγωνισμό μεταξύ των χρηματοοικονομικών οντοτήτων του ίδιου τύπου που δραστηριοποιούνται σε διαφορετικά κράτη μέλη. Αυτό ισχύει, ιδίως, για τομείς στους οποίους η εναρμόνιση της Ένωσης είναι εξαιρετικά περιορισμένη, όπως οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας, ή απούσα, όπως η παρακολούθηση των κινδύνων τρίτων παρόχων ΤΠΕ. Οι διαφορές που απορρέουν από τις εξελίξεις που προβλέπονται σε εθνικό επίπεδο θα μπορούσαν να δημιουργήσουν περαιτέρω φραγμούς για τη λειτουργία της εσωτερικής αγοράς εις βάρος των συμμετεχόντων στην αγορά και της χρηματοοικονομικής σταθερότητας.

(10) Έως τούδε, επειδή οι σχετικές με τους κινδύνους ΤΠΕ διατάξεις έχουν εξεταστεί μόνο μερικώς σε επίπεδο Ένωσης, υπάρχουν κενά ή αλληλεπικαλύψεις σε σημαντικούς τομείς, όπως η αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ και οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας, και ασυνέπειες ως αποτέλεσμα αναδυόμενων αποκλινόντων εθνικών κανόνων ή μη αποδοτικής ως προς το κόστος εφαρμογής των αλληλεπικαλυπτόμενων κανόνων. Η κατάσταση αυτή είναι ιδιαίτερα επιζήμια για τους εντατικούς χρήστες ΤΠΕ, όπως ο χρηματοοικονομικός τομέας, δεδομένου ότι οι τεχνολογικοί κίνδυνοι δεν έχουν σύνορα και ο χρηματοοικονομικός τομέας αναπτύσσει τις υπηρεσίες του σε ευρεία διασυνοριακή βάση, τόσο εντός όσο και εκτός της Ένωσης. Οι μεμονωμένες χρηματοοικονομικές οντότητες που δραστηριοποιούνται σε διασυνοριακή βάση ή είναι κάτοχοι πολλών αδειών (π.χ. μια χρηματοοικονομική οντότητα μπορεί να διαθέτει άδεια λειτουργίας τραπεζικού ιδρύματος, επιχείρησης επενδύσεων και ιδρύματος πληρωμών, καθεμία από τις οποίες έχει εκδοθεί από διαφορετική αρμόδια αρχή σε ένα ή περισσότερα κράτη μέλη) βρίσκονται αντιμέτωπες με επιχειρησιακές προκλήσεις διότι καλούνται να αντιμετωπίσουν τους κινδύνους ΤΠΕ και να μετριάσουν τις δυσμενείς επιπτώσεις συμβάντων ΤΠΕ μεμονωμένα και με συνεκτικό και οικονομικά αποδοτικό τρόπο.

(11) Δεδομένου ότι το ενιαίο εγχειρίδιο κανόνων δεν συνοδεύεται από ολοκληρωμένο πλαίσιο για τους κινδύνους ΤΠΕ ή τους λειτουργικούς κινδύνους, απαιτείται περαιτέρω εναρμόνιση των βασικών απαιτήσεων ψηφιακής επιχειρησιακής ανθεκτικότητας για όλες τις χρηματοοικονομικές οντότητες. Η ανάπτυξη ικανοτήτων ΤΠΕ και συνολικής ανθεκτικότητας από τις χρηματοοικονομικές οντότητες, σύμφωνα με τις εν λόγω βασικές απαιτήσεις, με σκοπό την αντιμετώπιση διακοπών λειτουργίας, θα συμβάλει στη διατήρηση της σταθερότητας και της ακεραιότητας των χρηματοοικονομικών αγορών της Ένωσης και, κατ' επέκταση, στη διασφάλιση υψηλού επιπέδου προστασίας των επενδυτών και των καταναλωτών στην Ένωση. Λαμβανομένου υπόψη ότι ο παρών κανονισμός έχει ως στόχο να συμβάλει στην εύρυθμη λειτουργία της εσωτερικής αγοράς, θα πρέπει να βασίζεται στις διατάξεις του άρθρου 114 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), όπως ερμηνεύονται σύμφωνα με την πάγια νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης (Δικαστήριο).

(12) Ο παρών κανονισμός αποσκοπεί στην ενοποίηση και την αναβάθμιση των απαιτήσεων για τους κινδύνους ΤΠΕ στο πλαίσιο των απαιτήσεων για τους λειτουργικούς κινδύνους, οι οποίες, έως το σημείο αυτό, έχουν εξεταστεί χωριστά σε διάφορες νομικές πράξεις της Ένωσης. Παρότι οι εν λόγω πράξεις κάλυπταν τις κύριες κατηγορίες χρηματοοικονομικών κινδύνων (π. χ. πιστωτικό κίνδυνο, κίνδυνο αγοράς, πιστωτικό κίνδυνο αντισυμβαλλομένου και κίνδυνο ρευστότητας, κίνδυνο συμπεριφοράς της αγοράς), δεν αντιμετώπισαν συνολικά, κατά τον χρόνο έκδοσής τους, όλες τις συνιστώσες της επιχειρησιακής ανθεκτικότητας. Οι κανόνες για λειτουργικούς κινδύνους, όταν αναπτύσσονταν περαιτέρω στις εν λόγω νομικές πράξεις της Ένωσης, ευνοούσαν συχνά την υιοθέτηση παραδοσιακής ποσοτικής προσέγγισης για την αντιμετώπιση του κινδύνου (κυρίως με την πρόβλεψη κεφαλαιακής απαίτησης για την κάλυψη των κινδύνων ΤΠΕ), αντί της έγκρισης

([6]) Κανονισμός (ΕΕ) αριθ. 1095/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Νοεμβρίου 2010, σχετικά με τη σύσταση Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών), την τροποποίηση της απόφασης αριθ. 716/2009/ΕΚ και την κατάργηση της απόφασης 2009/77/ΕΚ (ΕΕ L 331 της 15.12.2010, σ. 84).

στοχευμένων ποιοτικών κανόνων για την προστασία, τον εντοπισμό, τον περιορισμό, την αποκατάσταση και την επιδιόρθωση συμβάντων σχετικών με τις ΤΠΕ και για τις ικανότητες αναφοράς και ψηφιακών δοκιμών. Οι εν λόγω πράξεις είχαν ως πρωταρχικό στόχο την κάλυψη και την επικαιροποίηση βασικών κανόνων προληπτικής εποπτείας, ακεραιότητας ή δεοντολογίας της αγοράς. Μέσω της ενοποίησης και της αναβάθμισης των κανόνων σχετικά με τον κίνδυνο ΤΠΕ, όλες οι διατάξεις που αφορούν τον ψηφιακό κίνδυνο στον χρηματοοικονομικό τομέα θα πρέπει να συγκεντρωθούν για πρώτη φορά με συνεκτικό τρόπο σε μια ενιαία νομοθετική πράξη. Κατά συνέπεια, ο παρών κανονισμός καλύπτει τα κενά ή διορθώνει τις ασυνέπειες που παρουσιάζουν ορισμένες από τις πρότερες νομικές πράξεις, μεταξύ άλλων σε σχέση με την ορολογία που χρησιμοποιείται σε αυτές, και αναφέρεται ρητά στους κινδύνους ΤΠΕ μέσω στοχευμένων κανόνων για τις ικανότητες διαχείρισης κινδύνων ΤΠΕ, την αναφορά συμβάντων, τις δοκιμές επιχειρησιακής ανθεκτικότητας και την παρακολούθηση των κινδύνων τρίτων παρόχων ΤΠΕ. Ως εκ τούτου, ο παρών κανονισμός θα πρέπει επίσης να ευαισθητοποιήσει σχετικά με τους κινδύνους ΤΠΕ και να αναγνωρίσει ότι τα συμβάντα ΤΠΕ και η έλλειψη επιχειρησιακής ανθεκτικότητας ενδέχεται να θέσουν σε κίνδυνο την ευρωστία των χρηματοοικονομικών οντοτήτων.

(13) Οι χρηματοοικονομικές οντότητες θα πρέπει να ακολουθούν την ίδια προσέγγιση και τους ίδιους κανόνες βάσει αρχών κατά την αντιμετώπιση των κινδύνων ΤΠΕ, λαμβάνοντας υπόψη το μέγεθός τους και το συνολικό προφίλ κινδύνου τους και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών τους. Η συνοχή συμβάλλει στην ενίσχυση της εμπιστοσύνης στο χρηματοοικονομικό σύστημα και στη διατήρηση της σταθερότητάς του, ιδίως σε περιόδους υψηλής εξάρτησης από συστήματα, πλατφόρμες και υποδομές ΤΠΕ, η οποία συνεπάγεται αυξημένο ψηφιακό κίνδυνο. Κατά την τήρηση βασικής κυβερνοϋγιεινής θα πρέπει επίσης να αποφεύγεται η επιβολή υψηλών δαπανών στην οικονομία με την ελαχιστοποίηση των επιπτώσεων και του κόστους των διαταραχών ΤΠΕ.

(14) Ένας κανονισμός συμβάλλει στη μείωση της πολυπλοκότητας του κανονιστικού πλαισίου, ενισχύει την εποπτική σύγκλιση και αυξάνει την ασφάλεια δικαίου, ενώ βοηθά επίσης στον περιορισμό του κόστους συμμόρφωσης, ιδίως για τις χρηματοοικονομικές οντότητες που δραστηριοποιούνται διασυνοριακά, καθώς και στη μείωση των στρεβλώσεων του ανταγωνισμού. Ως εκ τούτου, η επιλογή κανονισμού για τη θέσπιση κοινού πλαισίου για την ψηφιακή επιχειρησιακή ανθεκτικότητα των χρηματοοικονομικών οντοτήτων συνιστά τον πλέον κατάλληλο τρόπο για τη διασφάλιση ομοιογενούς και συνεκτικής εφαρμογής όλων των συνιστωσών της διαχείρισης κινδύνων ΤΠΕ από τον χρηματοοικονομικό τομέα της Ένωσης.

(15) Η οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([7]) ήταν το πρώτο οριζόντιο πλαίσιο κυβερνοασφάλειας που θεσπίστηκε σε επίπεδο Ένωσης, το οποίο εφαρμόζεται επίσης σε τρεις τύπους χρηματοοικονομικών οντοτήτων, δηλαδή τα πιστωτικά ιδρύματα, τους τόπους διαπραγμάτευσης και τους κεντρικούς αντισυμβαλλομένους. Ωστόσο, αφότου ότι η οδηγία (ΕΕ) 2016/1148 θέσπισε μηχανισμό προσδιορισμού, σε εθνικό επίπεδο, των φορέων εκμετάλλευσης βασικών υπηρεσιών, μόνο ορισμένα πιστωτικά ιδρύματα, τόποι διαπραγμάτευσης και κεντρικοί αντισυμβαλλόμενοι που προσδιορίστηκαν από τα κράτη μέλη εμπίπτουν πρακτικά στο πεδίο εφαρμογής της και, κατά συνέπεια, υποχρεούνται να συμμορφώνονται με τις απαιτήσεις σχετικά με την ασφάλεια ΤΠΕ και την κοινοποίηση συμβάντων που προβλέπονται σε αυτήν. Η οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([8]) θεσπίζει ενιαίο κριτήριο για τον προσδιορισμό των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της (κανόνας για τα ανώτατα όρια μεγέθους), διατηρώντας παράλληλα τους τρεις τύπους χρηματοοικονομικών οντοτήτων στο πεδίο εφαρμογής της.

(16) Ωστόσο, λαμβανομένου υπόψη ότι ο παρών κανονισμός αυξάνει το επίπεδο εναρμόνισης των διάφορων συνιστωσών ψηφιακής ανθεκτικότητας, με τη θέσπιση απαιτήσεων σχετικά με τη διαχείριση κινδύνων ΤΠΕ και την αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ, οι οποίες είναι αυστηρότερες σε σύγκριση με τις απαιτήσεις που προβλέπονται στην ισχύουσα νομοθεσία της Ένωσης για τις χρηματοοικονομικές υπηρεσίες, αυτό το υψηλότερο επίπεδο συνιστά αυξημένη εναρμόνιση σε σύγκριση με τις απαιτήσεις που καθορίζονται στην οδηγία (ΕΕ) 2022/2555 Συνεπώς, ο παρών κανονισμός συνιστά lex specialis ως προς την οδηγία (ΕΕ) 2022/2555 Ταυτόχρονα, είναι καίριας σημασίας να διατηρηθεί ισχυρή σχέση μεταξύ του χρηματοοικονομικού τομέα και του οριζόντιου πλαισίου της Ένωσης για την κυβερνοασφάλεια, όπως ορίζεται επί του παρόντος στην οδηγία (ΕΕ) 2022/2555 ώστε να διασφαλιστεί η συνοχή με τις στρατηγικές κυβερνοασφάλειας που έχουν θεσπίσει τα κράτη μέλη και να εξασφαλιστεί η δυνατότητα ενημέρωσης των αρχών χρηματοοικονομικής εποπτείας για κυβερνοπεριστατικά τα οποία έχουν αντίκτυπο σε άλλους τομείς που καλύπτονται από την εν λόγω οδηγία.

([7]) Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (ΕΕ L 194 της 19.7.2016, σ. 1).

([8]) Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972 και την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2) (βλέπε σελίδα 80 της παρούσας Επίσημης Εφημερίδας).

(17) Σύμφωνα με το άρθρο 4 παράγραφος 2 της Συνθήκης για την Ευρωπαϊκή Ένωση και με την επιφύλαξη του δικαστικού ελέγχου από το Δικαστήριο, ο παρών κανονισμός δεν θα πρέπει να θίγει την ευθύνη των κρατών μελών όσον αφορά τις ουσιώδεις λειτουργίες του κράτους που αφορούν τη δημόσια ασφάλεια, την άμυνα και την προστασία της εθνικής ασφάλειας, για παράδειγμα όσον αφορά την παροχή πληροφοριών που θα ήταν αντίθετες προς την προστασία της εθνικής ασφάλειας.

(18) Για να καταστεί δυνατή η διατομεακή μάθηση και να αξιοποιηθούν αποτελεσματικά οι εμπειρίες από άλλους τομείς όσον αφορά την αντιμετώπιση κυβερνοαπειλών, οι χρηματοοικονομικές οντότητες που αναφέρονται στην οδηγία (ΕΕ) 2022/2555 θα πρέπει να εξακολουθήσουν να αποτελούν μέρος του «οικοσυστήματος» της εν λόγω οδηγίας (επί παραδείγματι, ομάδα συνεργασίας και ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT)). Οι ΕΕΑ και οι εθνικές αρμόδιες αρχές θα πρέπει να είναι σε θέση να συμμετέχουν στις συζητήσεις στρατηγικής πολιτικής και στις τεχνικές εργασίες της ομάδας συνεργασίας βάσει της εν λόγω οδηγίας και να ανταλλάσσουν πληροφορίες και να συνεργάζονται περαιτέρω με τα ενιαία κέντρα επαφής που ορίζονται ή συστήνονται σύμφωνα με την εν λόγω οδηγία. Οι αρμόδιες αρχές δυνάμει του παρόντος κανονισμού θα πρέπει επίσης να διαβουλεύονται και να συνεργάζονται με τις CSIRT. Οι αρμόδιες αρχές θα πρέπει επίσης να μπορούν να ζητούν τεχνικές συμβουλές από τις αρμόδιες αρχές που ορίζονται ή συστήνονται σύμφωνα με την οδηγία (ΕΕ) 2022/2555 και να θεσπίζουν ρυθμίσεις συνεργασίας που αποσκοπούν στη διασφάλιση αποτελεσματικών μηχανισμών συντονισμού ταχείας απόκρισης.

(19) Δεδομένων των ισχυρών διασυνδέσεων μεταξύ της ψηφιακής ανθεκτικότητας και της υλικής ανθεκτικότητας των χρηματοοικονομικών οντοτήτων, είναι αναγκαία μια συνεκτική προσέγγιση όσον αφορά την ανθεκτικότητα των κρίσιμων οντοτήτων στον παρόντα κανονισμό και στην οδηγία (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([9]). Δεδομένου ότι η υλική ανθεκτικότητα των χρηματοοικονομικών οντοτήτων αντιμετωπίζεται με ολοκληρωμένο τρόπο από τις υποχρεώσεις διαχείρισης και αναφοράς κινδύνων ΤΠΕ που καλύπτονται από τον παρόντα κανονισμό, οι υποχρεώσεις που ορίζονται στα κεφάλαια III και IV της οδηγίας (ΕΕ) 2022/2557 δεν θα πρέπει να εφαρμόζονται στις χρηματοοικονομικές οντότητες που εμπίπτουν στο πεδίο εφαρμογής της εν λόγω οδηγίας.

(20) Οι πάροχοι υπηρεσιών υπολογιστικού νέφους αποτελούν μία κατηγορία υποδομών που καλύπτονται από την οδηγία (ΕΕ) 2022/2555 Το ενωσιακό πλαίσιο εποπτείας («πλαίσιο εποπτείας») που θεσπίζεται με τον παρόντα κανονισμό εφαρμόζεται σε όλους τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, συμπεριλαμβανομένων των παρόχων υπηρεσιών υπολογιστικού νέφους, όταν παρέχουν υπηρεσίες ΤΠΕ σε χρηματοοικονομικές οντότητες, και θα πρέπει να θεωρείται συμπληρωματικό της εποπτείας δυνάμει της οδηγίας (ΕΕ) 2022/2555.Επιπλέον, το πλαίσιο εποπτείας που θεσπίζεται με τον παρόντα κανονισμό θα πρέπει να καλύπτει τους παρόχους υπηρεσιών υπολογιστικού νέφους ελλείψει ενωσιακού οριζόντιου πλαισίου για τη σύσταση αρχής ψηφιακής εποπτείας.

(21) Προκειμένου να διατηρηθεί ο πλήρης έλεγχος των κινδύνων ΤΠΕ, οι χρηματοοικονομικές οντότητες χρειάζεται να διαθέτουν ολοκληρωμένες ικανότητες που να επιτρέπουν την αυστηρή και αποτελεσματική διαχείριση κινδύνων ΤΠΕ, παράλληλα με ειδικούς μηχανισμούς και πολιτικές για τον χειρισμό όλων των συμβάντων που σχετίζονται με τις ΤΠΕ και για την αναφορά μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ. Ομοίως, οι χρηματοοικονομικές οντότητες θα πρέπει να εφαρμόζουν πολιτικές για τη δοκιμή συστημάτων, δικλείδων ασφάλειας και διαδικασιών ΤΠΕ, καθώς και για τη διαχείριση των κινδύνων τρίτων παρόχων ΤΠΕ. Η βάση αναφοράς για το επίπεδο ψηφιακής επιχειρησιακής ανθεκτικότητας για τις χρηματοοικονομικές οντότητες θα πρέπει να αυξηθεί, επιτρέποντας παράλληλα αναλογική εφαρμογή των απαιτήσεων για ορισμένες χρηματοοικονομικές οντότητες, ιδίως για τις πολύ μικρές επιχειρήσεις, καθώς και για τις χρηματοοικονομικές οντότητες που υπόκεινται σε απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ. Για να διευκολυνθεί η αποτελεσματική εποπτεία των ιδρυμάτων επαγγελματικών συνταξιοδοτικών παροχών που είναι αναλογική και ανταποκρίνεται στην ανάγκη μείωσης του διοικητικού φόρτου για τις αρμόδιες αρχές, οι σχετικές εθνικές εποπτικές ρυθμίσεις όσον αφορά τις εν λόγω χρηματοοικονομικές οντότητες θα πρέπει να λαμβάνουν υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου τους και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών τους, ακόμη και όταν σημειώνεται υπέρβαση των σχετικών κατώτατων ορίων που καθορίζονται στο άρθρο 5 της οδηγίας (ΕΕ) 2016/2341 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([10]). Ειδικότερα, οι εποπτικές δραστηριότητες θα πρέπει να επικεντρώνονται πρωτίστως στην ανάγκη αντιμετώπισης σοβαρών κινδύνων που συνδέονται με τη διαχείριση κινδύνων ΤΠΕ συγκεκριμένης οντότητας.

([9]) Οδηγία (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων και την κατάργηση της οδηγίας 2008/114/ΕΚ (βλέπε σελίδα 164 της παρούσας Επίσημης Εφημερίδας).

([10]) Οδηγία (ΕΕ) 2016/2341 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2016, για τις δραστηριότητες και την εποπτεία των ιδρυμάτων επαγγελματικών συνταξιοδοτικών παροχών (ΙΕΣΠ) (ΕΕ L 354 της 23.12.2016, σ. 37).

Οι αρμόδιες αρχές θα πρέπει επίσης να διατηρούν μια προσέγγιση επαγρύπνησης, αλλά αναλογική, σε σχέση με την εποπτεία των ιδρυμάτων επαγγελματικών συνταξιοδοτικών παροχών τα οποία, σύμφωνα με το άρθρο 31 της οδηγίας (ΕΕ) 2016/2341, αναθέτουν σε παρόχους υπηρεσιών σημαντικό μέρος των βασικών δραστηριοτήτων τους, όπως η διαχείριση περιουσιακών στοιχείων, οι αναλογιστικοί υπολογισμοί, η λογιστική και η διαχείριση δεδομένων.

(22) Τα κατώτατα όρια αναφοράς συμβάντων και οι ταξινομήσεις που σχετίζονται με τις ΤΠΕ παρουσιάζουν σημαντικές διαφοροποιήσεις σε εθνικό επίπεδο. Μολονότι μπορεί να επιτευχθεί κοινή βάση μέσω των σχετικών εργασιών που έχουν αναλάβει ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) που συστάθηκε με τον κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([11]) και η ομάδα συνεργασίας δυνάμει της οδηγίας (ΕΕ) 2022/2555 όσον αφορά τον καθορισμό κατώτατων ορίων και τη χρήση ταξινομήσεων εξακολουθούν να υπάρχουν αποκλίνουσες προσεγγίσεις ή μπορεί να προκύψουν για τις υπόλοιπες χρηματοοικονομικές οντότητες. Λόγω των εν λόγω αποκλίσεων, υπάρχουν πολλαπλές απαιτήσεις τις οποίες πρέπει να τηρούν οι χρηματοοικονομικές οντότητες, ιδίως όταν δραστηριοποιούνται σε διάφορα κράτη μέλη και όταν ανήκουν σε χρηματοοικονομικό όμιλο. Επιπλέον, οι αποκλίσεις αυτές θα μπορούσαν να παρεμποδίσουν τη δημιουργία περαιτέρω ενιαίων ή κεντρικών μηχανισμών της Ένωσης για την επιτάχυνση της διαδικασίας αναφορών και την υποστήριξη της ταχείας και ομαλής ανταλλαγής πληροφοριών μεταξύ των αρμόδιων αρχών, η οποία είναι καίριας σημασίας για την αντιμετώπιση των κινδύνων ΤΠΕ σε περίπτωση επιθέσεων μεγάλης κλίμακας με δυνητικά συστημικές συνέπειες.

(23) Για να μειωθούν ο διοικητικός φόρτος και οι ενδεχομένως αλληλεπικαλυπτόμενες υποχρεώσεις αναφοράς για ορισμένες χρηματοοικονομικές οντότητες, η απαίτηση για την αναφορά συμβάντων σύμφωνα με την οδηγία (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([12]) θα πρέπει να παύσει να ισχύει για τους παρόχους υπηρεσιών πληρωμών που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού. Κατά συνέπεια, τα πιστωτικά ιδρύματα, τα ιδρύματα ηλεκτρονικού χρήματος, τα ιδρύματα πληρωμών και οι πάροχοι υπηρεσιών πληροφοριών λογαριασμού, όπως αναφέρονται στο άρθρο 33 παράγραφος 1 της εν λόγω οδηγίας, θα πρέπει από την ημερομηνία εφαρμογής του παρόντος κανονισμού να αναφέρουν, σύμφωνα με τον παρόντα κανονισμό, όλα τα λειτουργικά συμβάντα ή συμβάντα ασφάλειας που σχετίζονται με πληρωμές και τα οποία έχουν αναφερθεί προηγουμένως δυνάμει της εν λόγω οδηγίας, ανεξάρτητα αν τα εν λόγω συμβάντα σχετίζονται με τις ΤΠΕ.

(24) Προκειμένου οι αρμόδιες αρχές να είναι σε θέση να επιτελούν τους εποπτικούς ρόλους, αποκτώντας ολοκληρωμένη εικόνα ως προς τη φύση, τη συχνότητα, τη σημασία και τις επιπτώσεις των συμβάντων που σχετίζονται με τις ΤΠΕ, και να προωθούν την ανταλλαγή πληροφοριών μεταξύ των αρμόδιων δημόσιων αρχών, συμπεριλαμβανομένων των αρχών επιβολής του νόμου και των αρχών εξυγίανσης, ο παρών κανονισμός θα πρέπει να θεσπίσει ισχυρό καθεστώς αναφοράς συμβάντων που σχετίζονται με τις ΤΠΕ σύμφωνα με το οποίο οι σχετικές απαιτήσεις αντιμετωπίζουν τα σημερινά κενά του δικαίου για τις χρηματοοικονομικές υπηρεσίες και θα εξαλείψουν τις υφιστάμενες αλληλεπικαλύψεις και επαναλήψεις για την ελάφρυνση του κόστους. Είναι σημαντικό να διασφαλιστεί η εναρμόνιση του καθεστώτος αναφοράς συμβάντων που σχετίζονται με τις ΤΠΕ με την επιβολή της υποχρέωσης σε όλες τις χρηματοοικονομικές οντότητες να αναφέρουν συμβάντα στις οικείες αρμόδιες αρχές μέσω ενός ενιαίου εξορθολογισμένου πλαισίου, όπως ορίζεται στον παρόντα κανονισμό. Επιπροσθέτως, οι ΕΕΑ θα πρέπει να έχουν την αρμοδιότητα να προσδιορίζουν περαιτέρω σχετικά στοιχεία για το πλαίσιο αναφοράς συμβάντων που σχετίζονται με τις ΤΠΕ, όπως η ταξινόμηση, τα χρονοδιαγράμματα, τα σύνολα δεδομένων, τα υποδείγματα και τα εφαρμοστέα κατώτατα όρια. Προκειμένου να διασφαλιστεί πλήρης συμμόρφωση με την οδηγία (ΕΕ) 2022/2555 οι χρηματοοικονομικές οντότητες θα πρέπει να μπορούν, σε προαιρετική βάση, να γνωστοποιούν σημαντικές κυβερνοαπειλές στη σχετική αρμόδια αρχή, όταν θεωρούν ότι η απειλή είναι σημαντική για το χρηματοοικονομικό σύστημα, τους χρήστες υπηρεσιών ή τους πελάτες.

(25) Σε ορισμένους χρηματοοικονομικούς υποτομείς έχουν αναπτυχθεί απαιτήσεις δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας που καθορίζουν πλαίσια τα οποία δεν είναι πάντοτε πλήρως ευθυγραμμισμένα. Αυτό οδηγεί σε πιθανή αλληλεπικάλυψη του κόστους για τις διασυνοριακές χρηματοοικονομικές οντότητες και καθιστά περίπλοκη την αμοιβαία αναγνώριση των αποτελεσμάτων των δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας, η οποία, με τη σειρά της, μπορεί να κατακερματίσει την εσωτερική αγορά.

([11]) Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) (ΕΕ L 151 της 7.6.2019, σ. 15).

([12]) Οδηγία (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2015, σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 2002/65/ΕΚ, 2009/110/ΕΚ και 2013/36/ΕΕ και του κανονισμού (ΕΕ) αριθ. 1093/2010 και την κατάργηση της οδηγίας 2007/64/ΕΚ (ΕΕ L 337 της 23.12.2015, σ. 35).

(26) Επιπλέον, όταν δεν απαιτούνται δοκιμές ΤΠΕ, οι ευπάθειες εξακολουθούν να μην εντοπίζονται, με αποτέλεσμα να εκθέτουν σε κινδύνους ΤΠΕ μια χρηματοοικονομική οντότητα και, εντέλει, να προκαλούν υψηλότερο κίνδυνο για τη σταθερότητα και την ακεραιότητα του χρηματοοικονομικού τομέα. Χωρίς την παρέμβαση της Ένωσης, οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας θα εξακολουθήσουν να είναι ανομοιογενείς και δεν θα περιλαμβάνουν σύστημα αμοιβαίας αναγνώρισης των αποτελεσμάτων των δοκιμών ΤΠΕ σε διάφορες δικαιοδοσίες. Επιπρόσθετα, λαμβανομένου υπόψη ότι είναι απίθανο άλλοι χρηματοοικονομικοί υποτομείς να υιοθετήσουν συστήματα δοκιμών σε ουσιαστική κλίμακα, θα χάσουν τα δυνητικά οφέλη πλαισίου δοκιμών, όσον αφορά την αποκάλυψη ευπαθειών και κινδύνων ΤΠΕ και τις δοκιμές των ικανοτήτων άμυνας και της επιχειρησιακής συνέχειας, που συμβάλλει στην αύξηση της εμπιστοσύνης των πελατών, των προμηθευτών και των επιχειρηματικών εταίρων. Για τη διόρθωση αυτών των αλληλεπικαλύψεων, αποκλίσεων και κενών, είναι απαραίτητο να θεσπιστούν κανόνες για ένα συντονισμένο καθεστώς δοκιμών και, με τον τρόπο αυτό, να διευκολυνθεί η αμοιβαία αναγνώριση των προηγμένων δοκιμών για χρηματοοικονομικές οντότητες που πληρούν τα κριτήρια που καθορίζονται στον παρόντα κανονισμό.

(27) Η στήριξη των χρηματοοικονομικών οντοτήτων στη χρήση υπηρεσιών ΤΠΕ οφείλεται εν μέρει στην ανάγκη προσαρμογής τους σε μια αναδυόμενη ανταγωνιστική ψηφιακή παγκόσμια οικονομία, με σκοπό την ενίσχυση της επιχειρηματικής τους απόδοσης και την κάλυψη της ζήτησης των καταναλωτών. Η φύση και η έκταση της στήριξης αυτής εξελίσσονται διαρκώς κατά τα πρόσφατα έτη, με αποτέλεσμα τη μείωση του κόστους της χρηματοοικονομικής διαμεσολάβησης, την εξασφάλιση της δυνατότητας επέκτασης των επιχειρήσεων και κλιμάκωσης όσον αφορά την ανάπτυξη χρηματοοικονομικών δραστηριοτήτων, ενώ προσφέρεται παράλληλα ευρύ φάσμα εργαλείων ΤΠΕ για τη διαχείριση πολύπλοκων εσωτερικών διαδικασιών.

(28) Η εκτεταμένη χρήση υπηρεσιών ΤΠΕ αποδεικνύεται από πολύπλοκες συμβατικές ρυθμίσεις, στο πλαίσιο των οποίων οι χρηματοοικονομικές οντότητες αντιμετωπίζουν συχνά δυσκολίες στη διαπραγμάτευση συμβατικών όρων που είναι προσαρμοσμένοι στα πρότυπα προληπτικής εποπτείας ή σε άλλες ρυθμιστικές απαιτήσεις στις οποίες υπόκεινται ή με άλλον τρόπο στην άσκηση συγκεκριμένων δικαιωμάτων, όπως δικαιώματα πρόσβασης ή ελέγχου, ακόμη και σε περίπτωση που τα δικαιώματα αυτά κατοχυρώνονται στις συμβατικές ρυθμίσεις τους. Επιπλέον, πολλές από τις εν λόγω συμβατικές ρυθμίσεις δεν προβλέπουν επαρκείς διασφαλίσεις που να επιτρέπουν την πλήρη παρακολούθηση των διαδικασιών υπεργολαβίας, στερώντας με τον τρόπο αυτόν από τη χρηματοοικονομική οντότητα την ικανότητά της να αξιολογεί τους συναφείς κινδύνους. Επιπροσθέτως, λαμβανομένου υπόψη ότι οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ παρέχουν συχνά τυποποιημένες υπηρεσίες σε διαφορετικούς τύπους πελατών, οι συμβατικές ρυθμίσεις αυτού του είδους ενδέχεται να μην ανταποκρίνονται πάντα επαρκώς στις επιμέρους ή ειδικές ανάγκες των παραγόντων του χρηματοοικονομικού κλάδου.

(29) Μολονότι το δίκαιο της Ένωσης για τις χρηματοοικονομικές υπηρεσίες περιλαμβάνει ορισμένους γενικούς κανόνες για την εξωτερική ανάθεση, η παρακολούθηση της συμβατικής διάστασης δεν θεμελιώνεται πλήρως στο δίκαιο της Ένωσης. Ελλείψει της εφαρμογής σαφών και εξειδικευμένων ενωσιακών προτύπων στις συμβατικές ρυθμίσεις που συνάπτονται με τρίτους παρόχους υπηρεσιών ΤΠΕ, η εξωτερική πηγή κινδύνων ΤΠΕ δεν αντιμετωπίζεται με ολοκληρωμένο τρόπο. Ως εκ τούτου, είναι απαραίτητο να καθοριστούν ορισμένες βασικές αρχές για την καθοδήγηση της διαχείρισης των κινδύνων τρίτων παρόχων ΤΠΕ από τις χρηματοοικονομικές οντότητες, οι οποίες είναι ιδιαίτερα σημαντικές όταν οι χρηματοοικονομικές οντότητες καταφεύγουν σε τρίτους παρόχους υπηρεσιών ΤΠΕ για την υποστήριξη των κρίσιμων ή σημαντικών λειτουργιών τους. Οι εν λόγω αρχές θα πρέπει να συνοδεύονται από ένα σύνολο βασικών συμβατικών δικαιωμάτων σε σχέση με διάφορα στοιχεία της εκτέλεσης και της καταγγελίας των συμβατικών ρυθμίσεων, με σκοπό την παροχή ορισμένων ελάχιστων διασφαλίσεων προκειμένου να ενισχύουν την ικανότητα των χρηματοοικονομικών οντοτήτων να παρακολουθούν αποτελεσματικά όλους τους κινδύνους ΤΠΕ που ανακύπτουν σε επίπεδο τρίτων παρόχων υπηρεσιών. Οι εν λόγω αρχές είναι συμπληρωματικές προς το τομεακό δίκαιο που διέπει την εξωτερική ανάθεση.

(30) Σήμερα είναι προφανής μια ορισμένη έλλειψη ομοιογένειας και σύγκλισης όσον αφορά την παρακολούθηση των κινδύνων τρίτων παρόχων ΤΠΕ και των εξαρτήσεων από τρίτους παρόχους ΤΠΕ. Παρά την καταβολή προσπαθειών για την αντιμετώπιση της εξωτερικής ανάθεσης, όπως οι κατευθυντήριες γραμμές της ΕΑΤ του 2019 και οι κατευθυντήριες γραμμές της ΕΑΚΑΑ του 2021 για την εξωτερική ανάθεση σε παρόχους υπηρεσιών υπολογιστικού νέφους, το ευρύτερο ζήτημα της καταπολέμησης του συστημικού κινδύνου που ενδέχεται να ανακύψει από την έκθεση του χρηματοοικονομικού τομέα σε περιορισμένο αριθμό κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ δεν αντιμετωπίζεται επαρκώς από το ενωσιακό δίκαιο. Η έλλειψη κανόνων σε επίπεδο Ένωσης επιδεινώνεται από την απουσία εθνικών κανόνων περί ειδικών εντολών και εργαλείων που επιτρέπουν στις αρχές χρηματοοικονομικής εποπτείας να κατανοούν δεόντως τις εξαρτήσεις από τρίτους παρόχους ΤΠΕ και να παρακολουθούν επαρκώς τους κινδύνους που ανακύπτουν λόγω της συγκέντρωσης εξαρτήσεων από τρίτους παρόχους ΤΠΕ.

(31) Λαμβανομένου υπόψη του δυνητικού συστημικού κινδύνου που συνεπάγεται η αύξηση των πρακτικών εξωτερικής ανάθεσης και η συγκέντρωση τρίτων παρόχων ΤΠΕ και έχοντας επίγνωση της ανεπάρκειας εθνικών μηχανισμών να παρέχουν στις αρχές χρηματοοικονομικής εποπτείας τα κατάλληλα εργαλεία για τη δυνατότητα ποσοτικού προσδιορισμού, χαρακτηρισμού και αποκατάστασης των επιπτώσεων των κινδύνων ΤΠΕ που αφορούν κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, είναι απαραίτητο να θεσπιστεί κατάλληλο πλαίσιο εποπτείας, το οποίο θα επιτρέπει τη διαρκή παρακολούθηση των δραστηριοτήτων τρίτων παρόχων υπηρεσιών ΤΠΕ που είναι κρίσιμοι πάροχοι υπηρεσιών ΤΠΕ σε χρηματοοικονομικές οντότητες, διασφαλίζοντας, παράλληλα, τη διατήρηση της εμπιστευτικότητας και της ασφάλειας των πελατών, πλην των χρηματοοικονομικών οντοτήτων. Ενώ η ενδοομιλική παροχή υπηρεσιών ΤΠΕ συνεπάγεται ειδικούς κινδύνους και οφέλη, δεν θα πρέπει να θεωρείται αυτομάτως λιγότερο επικίνδυνη από την παροχή υπηρεσιών ΤΠΕ από παρόχους εκτός χρηματοοικονομικού ομίλου και, ως εκ τούτου, θα πρέπει να υπόκειται στο ίδιο ρυθμιστικό πλαίσιο. Ωστόσο, όταν οι υπηρεσίες ΤΠΕ παρέχονται από τον ίδιο χρηματοοικονομικό όμιλο, οι χρηματοοικονομικές οντότητες ενδέχεται να έχουν υψηλότερο επίπεδο ελέγχου επί των ενδοομιλικών παρόχων, το οποίο θα πρέπει να λαμβάνεται υπόψη στη συνολική εκτίμηση κινδύνου.

(32) Καθώς οι κίνδυνοι ΤΠΕ εξελίσσονται και περιπλέκονται ολοένα και πιο πολύ, τα καλά μέτρα για τον εντοπισμό και την πρόληψη των κινδύνων ΤΠΕ εξαρτώνται σε μεγάλο βαθμό από την τακτική ανταλλαγή πληροφοριών σχετικά με απειλές και ευπάθειες μεταξύ των χρηματοοικονομικών οντοτήτων. Η ανταλλαγή πληροφοριών συμβάλλει στην αύξηση της ευαισθητοποίησης σχετικά με τις κυβερνοαπειλές. Αυτό με τη σειρά του ενισχύει την ικανότητα των χρηματοοικονομικών οντοτήτων να αποτρέπουν τη μετατροπή απειλών σε πραγματικά συμβάντα που σχετίζονται με τις ΤΠΕ και παρέχει στις χρηματοοικονομικές οντότητες τη δυνατότητα να περιορίζουν αποτελεσματικότερα τις επιπτώσεις των συμβάντων που σχετίζονται με τις ΤΠΕ και να ανακάμπτουν ταχύτερα. Ελλείψει καθοδήγησης σε επίπεδο Ένωσης, φαίνεται ότι η παρεμπόδιση της ανταλλαγής στοιχείων αυτού του είδους οφείλεται σε διάφορους παράγοντες, κυρίως στην αβεβαιότητα ως προς τη συμβατότητα με τους κανόνες προστασίας δεδομένων, τους αντιμονοπωλιακούς κανόνες και τους κανόνες περί ευθύνης.

(33) Επιπροσθέτως, οι αμφιβολίες ως προς το είδος των πληροφοριών που μπορούν να γνωστοποιούνται σε άλλους συμμετέχοντες στην αγορά ή σε μη εποπτικές αρχές (όπως ο ENISA, για σκοπούς ανάλυσης, ή η Ευρωπόλ, για σκοπούς επιβολής του νόμου) έχουν ως αποτέλεσμα την απόκρυψη χρήσιμων πληροφοριών. Κατά συνέπεια, η έκταση και η ποιότητα της ανταλλαγής πληροφοριών παραμένει επί του παρόντος περιορισμένη και κατακερματισμένη, με την πραγματοποίηση των σχετικών ανταλλαγών κυρίως σε τοπικό επίπεδο (μέσω εθνικών πρωτοβουλιών) και χωρίς συνεκτικές ρυθμίσεις, σε επίπεδο Ένωσης, για την ανταλλαγή πληροφοριών κατάλληλα προσαρμοσμένων στις ανάγκες ενός ενοποιημένου χρηματοοικονομικού συστήματος. Ως εκ τούτου, είναι σημαντικό να ενισχυθούν αυτοί οι δίαυλοι επικοινωνίας.

(34) Οι χρηματοοικονομικές οντότητες θα πρέπει να ενθαρρύνονται να ανταλλάσσουν μεταξύ τους πληροφορίες και στοιχεία περί κυβερνοαπειλών και να αξιοποιούν συλλογικά τις επιμέρους γνώσεις και την πρακτική εμπειρία που διαθέτουν σε στρατηγικό, τακτικό και επιχειρησιακό επίπεδο, με σκοπό την ενίσχυση των ικανοτήτων τους, ώστε να είναι σε θέση να αξιολογούν, να παρακολουθούν, να υπερασπίζονται και να αντιμετωπίζουν δεόντως κυβερνοαπειλές, συμμετέχοντας σε ρυθμίσεις ανταλλαγής πληροφοριών. Ως εκ τούτου, είναι απαραίτητο να καταστεί δυνατή η δημιουργία, σε επίπεδο Ένωσης, μηχανισμών για τη θέσπιση προαιρετικών ρυθμίσεων ανταλλαγής πληροφοριών, οι οποίοι, όταν θα εφαρμόζονται σε αξιόπιστο περιβάλλον, θα διευκολύνουν την κοινότητα του χρηματοοικονομικού κλάδου να αποτρέπει απειλές και να αντιδρά συλλογικά σε αυτές, περιορίζοντας ταχέως την εξάπλωση των κινδύνων ΤΠΕ και εμποδίζοντας την πιθανή μετάδοσή τους σε όλους τους χρηματοοικονομικούς διαύλους. Οι εν λόγω μηχανισμοί θα πρέπει να συμμορφώνονται με τους ισχύοντες κανόνες του ενωσιακού δικαίου περί ανταγωνισμού που ορίζονται στην ανακοίνωση της Επιτροπής, της 14ης Ιανουαρίου 2011, με τίτλο «Κατευθυντήριες γραμμές για την εφαρμογή του άρθρου 101 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης στις συμφωνίες οριζόντιας συνεργασίας», καθώς και με τους κανόνες της Ένωσης για την προστασία των δεδομένων, ιδίως με τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([13]). Θα πρέπει να λειτουργούν με βάση τη χρήση μίας ή περισσότερων από τις νομικές βάσεις που ορίζονται στο άρθρο 6 του εν λόγω κανονισμού, όπως στο πλαίσιο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα που είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, όπως αναφέρεται στο άρθρο 6 παράγραφος 1 στοιχείο στ) του εν λόγω κανονισμού, καθώς και στο πλαίσιο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα που είναι απαραίτητη για τη συμμόρφωση προς νομική υποχρέωση στην οποία υπόκειται ο υπεύθυνος επεξεργασίας, αναγκαία για την εκπλήρωση καθήκοντος το οποίο εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, όπως αναφέρεται στο άρθρο 6 παράγραφος 1 στοιχεία γ) και ε), αντίστοιχα, του εν λόγω κανονισμού.

([13]) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

(35) Προκειμένου ολόκληρος ο χρηματοοικονομικός τομέας να διατηρεί υψηλό επίπεδο ψηφιακής επιχειρησιακής ανθεκτικότητας και ταυτόχρονα να συμβαδίζει με τις τεχνολογικές εξελίξεις, ο παρών κανονισμός θα πρέπει να αντιμετωπίζει τους κινδύνους που απορρέουν από όλα τα είδη υπηρεσιών ΤΠΕ. Για τον σκοπό αυτόν, ο ορισμός των υπηρεσιών ΤΠΕ στο πλαίσιο του παρόντος κανονισμού θα πρέπει να ερμηνεύεται ευρέως, περιλαμβάνοντας τις ψηφιακές υπηρεσίες και τις υπηρεσίες δεδομένων που παρέχονται μέσω συστημάτων ΤΠΕ σε έναν ή περισσότερους εσωτερικούς ή εξωτερικούς χρήστες σε συνεχή βάση. Ο εν λόγω ορισμός θα πρέπει, για παράδειγμα, να περιλαμβάνει τις λεγόμενες «επιφυείς (over the top)» υπηρεσίες, οι οποίες εμπίπτουν στην κατηγορία των υπηρεσιών ηλεκτρονικών επικοινωνιών. Θα πρέπει να εξαιρεθεί μόνο η περιορισμένη κατηγορία παραδοσιακών αναλογικών τηλεφωνικών υπηρεσιών που χαρακτηρίζονται ως υπηρεσίες δημόσιου τηλεφωνικού δικτύου μεταγωγής (PSTN), υπηρεσίες επίγειου δικτύου, απλές παλιές τηλεφωνικές υπηρεσίες (POTS) ή υπηρεσίες σταθερής τηλεφωνίας.

(36) Παρά την ευρεία κάλυψη που επιδιώκεται με τον παρόντα κανονισμό, η εφαρμογή των κανόνων για την ψηφιακή επιχειρησιακή ανθεκτικότητα θα πρέπει να λαμβάνει υπόψη τις σημαντικές διαφορές μεταξύ των χρηματοοικονομικών οντοτήτων όσον αφορά το μέγεθος και το συνολικό προφίλ κινδύνου τους. Ως γενική αρχή, κατά την κατανομή πόρων και ικανοτήτων για την εφαρμογή του πλαισίου διαχείρισης κινδύνων ΤΠΕ, οι χρηματοοικονομικές οντότητες θα πρέπει να εξισορροπούν δεόντως τις σχετικές με τις ΤΠΕ ανάγκες τους με το μέγεθος και το συνολικό προφίλ κινδύνου των χρηματοοικονομικών οντοτήτων και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών τους, ενώ οι αρμόδιες αρχές θα πρέπει να συνεχίσουν να αξιολογούν και να επανεξετάζουν την προσέγγιση της εν λόγω κατανομής.

(37) Οι πάροχοι υπηρεσιών πληροφοριών λογαριασμού, οι οποίοι αναφέρονται στο άρθρο 33 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366, περιλαμβάνονται ρητά στο πεδίο εφαρμογής του παρόντος κανονισμού, λαμβανομένων υπόψη της ιδιαίτερης φύσης των δραστηριοτήτων τους και των κινδύνων που απορρέουν από αυτές. Επιπλέον, τα ιδρύματα ηλεκτρονικού χρήματος και τα ιδρύματα πληρωμών που εξαιρούνται δυνάμει του άρθρου 9 παράγραφος 1 της οδηγίας 2009/110/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([14]) και του άρθρου 32 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366 περιλαμβάνονται στο πεδίο εφαρμογής του παρόντος κανονισμού, ακόμη και αν δεν τους έχει χορηγηθεί άδεια σύμφωνα με την οδηγία 2009/110/ΕΚ για την έκδοση ηλεκτρονικού χρήματος ή δεν τους έχει χορηγηθεί άδεια σύμφωνα με την οδηγία (ΕΕ) 2015/2366 για την παροχή και την εκτέλεση υπηρεσιών πληρωμών. Ωστόσο, τα γραφεία ταχυδρομικών επιταγών, που αναφέρονται στο άρθρο 2 παράγραφος 5 σημείο 3) της οδηγίας 2013/36/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([15]), εξαιρούνται από το πεδίο εφαρμογής του παρόντος κανονισμού. Η αρμόδια αρχή για τα ιδρύματα πληρωμών, τα οποία εξαιρούνται δυνάμει της οδηγίας (ΕΕ) 2015/2366, τα ιδρύματα ηλεκτρονικού χρήματος, τα οποία εξαιρούνται δυνάμει της οδηγίας 2009/110/ΕΚ, και τους παρόχους υπηρεσιών πληροφοριών λογαριασμού, όπως αναφέρονται στο άρθρο 33 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366, θα πρέπει να είναι η αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 22 της οδηγίας (ΕΕ) 2015/2366.

(38) Δεδομένου ότι οι μεγαλύτερες χρηματοοικονομικές οντότητες ενδέχεται να διαθέτουν ευρύτερους πόρους και μπορούν να κινητοποιούν άμεσα κεφάλαια για την ανάπτυξη δομών διακυβέρνησης και τη χάραξη διαφόρων εταιρικών στρατηγικών, μόνο οι χρηματοοικονομικές οντότητες που δεν είναι πολύ μικρές επιχειρήσεις κατά την έννοια του παρόντος κανονισμού θα πρέπει να υποχρεούνται να θεσπίζουν πιο πολύπλοκες ρυθμίσεις διακυβέρνησης. Οντότητες αυτού του είδους είναι καλύτερα εξοπλισμένες, ιδίως για τη δημιουργία ειδικών λειτουργιών διαχείρισης όσον αφορά τις εποπτικές ρυθμίσεις με τρίτους παρόχους υπηρεσιών ΤΠΕ ή τη διασφάλιση της διαχείρισης κρίσεων για την οργάνωση της διαχείρισης κινδύνων ΤΠΕ σύμφωνα με το μοντέλο των τριών γραμμών άμυνας ή τη δημιουργία εσωτερικού μοντέλου διαχείρισης κινδύνων και ελέγχου, καθώς και για την υποβολή του οικείου πλαισίου διαχείρισης κινδύνων ΤΠΕ σε εσωτερικές επιθεωρήσεις.

(39) Ορισμένες χρηματοοικονομικές οντότητες επωφελούνται από εξαιρέσεις ή υπόκεινται σε πολύ χαλαρό ρυθμιστικό πλαίσιο βάσει του τομεακού ενωσιακού δικαίου. Στις εν λόγω χρηματοοικονομικές οντότητες περιλαμβάνονται οι διαχειριστές οργανισμών εναλλακτικών επενδύσεων που αναφέρονται στο άρθρο 3 παράγραφος 2 της οδηγίας 2011/61/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([16]), οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις που αναφέρονται στο άρθρο 4 της οδηγίας 2009/138/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([17]) και τα ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών που διαχειρίζονται συνταξιοδοτικά συστήματα τα οποία από κοινού δεν έχουν

([14]) Οδηγία 2009/110/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Σεπτεμβρίου 2009, για την ανάληψη, άσκηση και προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος, την τροποποίηση των οδηγιών 2005/60/ΕΚ και 2006/48/ΕΚ και την κατάργηση της οδηγίας 2000/46/ΕΚ (ΕΕ L 267 της 10.10.2009, σ. 7).

([15]) Οδηγία 2013/36/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και το Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με την πρόσβαση στη δραστηριότητα των πιστωτικών ιδρυμάτων και την προληπτική εποπτεία των πιστωτικών ιδρυμάτων, την τροποποίηση της οδηγίας 2002/87/ΕΚ και την κατάργηση των οδηγιών 2006/48/ΕΚ και 2006/49/ΕΚ (ΕΕ L 176 της 27.6.2013, σ. 338).

([16]) Οδηγία 2011/61/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 8ης Ιουνίου 2011, σχετικά με τους διαχειριστές οργανισμών εναλλακτικών επενδύσεων και για την τροποποίηση των οδηγιών 2003/41/ΕΚ και 2009/65/ΕΚ και των κανονισμών (ΕΚ) αριθ. 1060/2009 και (ΕΕ) αριθ. 1095/2010 (ΕΕ L 174 της 1.7.2011, σ. 1).

([17]) Οδηγία 2009/138/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009, σχετικά με την ανάληψη και την άσκηση δραστηριοτήτων ασφάλισης και αντασφάλισης (Φερεγγυότητα ΙΙ) (ΕΕ L 335 της 17.12.2009, σ. 1).

περισσότερα από 15 μέλη συνολικά. Υπό το πρίσμα των εν λόγω εξαιρέσεων, δεν θα ήταν αναλογικό να συμπεριληφθούν οι εν λόγω χρηματοοικονομικές οντότητες στο πεδίο εφαρμογής του παρόντος κανονισμού. Επιπλέον, ο παρών κανονισμός αναγνωρίζει τις ιδιαιτερότητες της δομής της αγοράς ασφαλιστικής διαμεσολάβησης, με αποτέλεσμα οι ασφαλιστικοί διαμεσολαβητές, οι αντασφαλιστικοί διαμεσολαβητές και οι ασφαλιστικοί διαμεσολαβητές που ασκούν ως δευτερεύουσα δραστηριότητα την ασφαλιστική διαμεσολάβηση, που χαρακτηρίζονται ως πολύ μικρές επιχειρήσεις ή ως μικρές ή μεσαίες επιχειρήσεις, να μην υπόκεινται στον παρόντα κανονισμό.

(40) Δεδομένου ότι οι οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 5 σημεία 4) έως 23) της οδηγίας 2013/36/ΕΕ εξαιρούνται από το πεδίο εφαρμογής της εν λόγω οδηγίας, τα κράτη μέλη θα πρέπει, κατά συνέπεια, να έχουν τη δυνατότητα να εξαιρούν από την εφαρμογή του παρόντος κανονισμού τις εν λόγω οντότητες που είναι εγκατεστημένες στις αντίστοιχες επικράτειές τους.

(41) Ομοίως, προκειμένου να ευθυγραμμιστεί ο παρών κανονισμός με το πεδίο εφαρμογής της οδηγίας 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([18]), είναι επίσης σκόπιμο να εξαιρεθούν από το πεδίο εφαρμογής του παρόντος κανονισμού τα φυσικά και νομικά πρόσωπα που αναφέρονται στα άρθρα 2 και 3 της εν λόγω οδηγίας, τα οποία επιτρέπεται να παρέχουν επενδυτικές υπηρεσίες χωρίς να χρειάζεται να λάβουν άδεια δυνάμει της οδηγίας 2014/65/ΕΕ. Ωστόσο, το άρθρο 2 της οδηγίας 2014/65/ΕΕ εξαιρεί επίσης από το πεδίο εφαρμογής της εν λόγω οδηγίας οντότητες που θεωρούνται χρηματοοικονομικές οντότητες για τους σκοπούς του παρόντος κανονισμού, όπως τα κεντρικά αποθετήρια τίτλων, οι οργανισμοί συλλογικών επενδύσεων ή οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις. Η εξαίρεση από το πεδίο εφαρμογής του παρόντος κανονισμού των προσώπων και των οντοτήτων που αναφέρονται στα άρθρα 2 και 3 της εν λόγω οδηγίας δεν θα πρέπει να περιλαμβάνει τα εν λόγω κεντρικά αποθετήρια τίτλων, οργανισμούς συλλογικών επενδύσεων ή ασφαλιστικές και αντασφαλιστικές επιχειρήσεις.

(42) Σύμφωνα με το τομεακό ενωσιακό δίκαιο, ορισμένες χρηματοοικονομικές οντότητες υπόκεινται σε λιγότερο αυστηρές απαιτήσεις ή εξαιρέσεις για λόγους οι οποίοι σχετίζονται με το μέγεθός τους ή τις υπηρεσίες που παρέχουν. Σε αυτήν την κατηγορία χρηματοοικονομικών οντοτήτων περιλαμβάνονται μικρές και μη διασυνδεδεμένες επιχειρήσεις επενδύσεων, μικρά ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών που μπορούν να εξαιρεθούν από το πεδίο εφαρμογής της οδηγίας (ΕΕ) 2016/2341, υπό τις προϋποθέσεις που ορίζονται στο άρθρο 5 της εν λόγω οδηγίας από το οικείο κράτος μέλος, και διαχειρίζονται συνταξιοδοτικά συστήματα τα οποία από κοινού δεν έχουν περισσότερα από 100 μέλη συνολικά, καθώς και ιδρύματα που εξαιρούνται δυνάμει της οδηγίας 2013/36/ΕΕ. Ως εκ τούτου, σύμφωνα με την αρχή της αναλογικότητας και για να διατηρηθεί το πνεύμα του τομεακού ενωσιακού δικαίου, είναι επίσης σκόπιμο να υπαχθούν οι εν λόγω χρηματοοικονομικές οντότητες σε απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ δυνάμει του παρόντος κανονισμού. Ο αναλογικός χαρακτήρας του πλαισίου διαχείρισης κινδύνων ΤΠΕ που καλύπτει τις εν λόγω χρηματοοικονομικές οντότητες δεν θα πρέπει να τροποποιείται από τα ρυθμιστικά τεχνικά πρότυπα που πρόκειται να εκπονηθούν από τις ΕΕΑ. Επιπλέον, σύμφωνα με την αρχή της αναλογικότητας, είναι σκόπιμο να υπαχθούν επίσης τα ιδρύματα πληρωμών που αναφέρονται στο άρθρο 32 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366 και τα ιδρύματα ηλεκτρονικού χρήματος που αναφέρονται στο άρθρο 9 της οδηγίας 2009/110/ΕΚ, σύμφωνα με τη μεταφορά των εν λόγω νομικών πράξεων της Ένωσης στο εθνικό δίκαιο, σε απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ δυνάμει του παρόντος κανονισμού, ενώ τα ιδρύματα πληρωμών και τα ιδρύματα ηλεκτρονικού χρήματος που δεν έχουν εξαιρεθεί σύμφωνα με την αντίστοιχη μεταφορά του τομεακού δικαίου της Ένωσης στο εθνικό τους δίκαιο θα πρέπει να συμμορφώνονται με το γενικό πλαίσιο που θεσπίζεται με τον παρόντα κανονισμό.

(43) Ομοίως, οι χρηματοοικονομικές οντότητες που χαρακτηρίζονται πολύ μικρές επιχειρήσεις ή υπόκεινται στο απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ δυνάμει του παρόντος κανονισμού δεν θα πρέπει να υποχρεούνται να καθορίζουν ρόλο για την παρακολούθηση των ρυθμίσεων που συνάπτουν με τρίτους παρόχους υπηρεσιών ΤΠΕ σχετικά με τη χρήση υπηρεσιών ΤΠΕ ή να ορίζουν ανώτερο διοικητικό στέλεχος υπεύθυνο για την εποπτεία της σχετικής έκθεσης σε κίνδυνο και τη σχετική τεκμηρίωση, να αναθέτουν την ευθύνη διαχείρισης και εποπτείας των κινδύνων ΤΠΕ σε λειτουργία ελέγχου και να διασφαλίζουν κατάλληλο επίπεδο ανεξαρτησίας της εν λόγω λειτουργίας ελέγχου, προκειμένου να αποφεύγονται συγκρούσεις συμφερόντων, να τεκμηριώνουν και να επανεξετάζουν τουλάχιστον μία φορά ετησίως το πλαίσιο διαχείρισης κινδύνων ΤΠΕ, να υποβάλλουν σε τακτική εσωτερική επιθεώρηση το πλαίσιο διαχείρισης κινδύνων ΤΠΕ, να διενεργούν εις βάθος αξιολογήσεις μετά από σημαντικές αλλαγές στις υποδομές και στις διαδικασίες των συστημάτων δικτύου και πληροφοριών τους, να προβαίνουν ανά τακτά χρονικά διαστήματα σε αναλύσεις κινδύνου για τα παρωχημένα συστήματα ΤΠΕ, να υποβάλλουν την εφαρμογή των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ σε ανεξάρτητες επανεξετάσεις εσωτερικής επιθεώρησης, να διαθέτουν λειτουργία διαχείρισης κρίσεων, να επεκτείνουν τις δοκιμές επιχειρησιακής συνέχειας και τα σχέδια αντιμετώπισης και ανάκαμψης, ώστε να σχεδιάζουν σενάρια μετάβασης μεταξύ της κύριας υποδομής ΤΠΕ και των εφεδρικών εγκαταστάσεων, να υποβάλλουν στις αρμόδιες αρχές, κατόπιν αιτήματός τους,

([18]) Οδηγία 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και την τροποποίηση της οδηγίας 2002/92/ΕΚ και της οδηγίας 2011/61/ΕΕ (ΕΕ L 173 της 12.6.2014, σ. 349).

εκτίμηση των συγκεντρωτικών ετήσιων δαπανών και ζημιών οι οποίες προκαλούνται από μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ, να διατηρούν εφεδρικές χωρητικότητες ΤΠΕ, να κοινοποιούν στις εθνικές αρμόδιες αρχές τις αλλαγές που εφαρμόστηκαν κατόπιν επανεξετάσεων μετά από συμβάντα που σχετίζονται με τις ΤΠΕ, να παρακολουθούν σε συνεχή βάση τις σχετικές τεχνολογικές εξελίξεις, να θεσπίζουν ολοκληρωμένο πρόγραμμα δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας ως αναπόσπαστο μέρος του πλαισίου διαχείρισης κινδύνων ΤΠΕ που προβλέπεται στον παρόντα κανονισμό ή να εγκρίνουν και να επανεξετάζουν τακτικά στρατηγική για τους κινδύνους τρίτου παρόχου ΤΠΕ. Επιπλέον, οι πολύ μικρές επιχειρήσεις θα πρέπει μόνο να υποχρεούνται να αξιολογούν την ανάγκη διατήρησης αυτών των εφεδρικών χωρητικοτήτων ΤΠΕ με βάση το προφίλ κινδύνου τους. Οι πολύ μικρές επιχειρήσεις θα πρέπει να επωφελούνται από ένα πιο ευέλικτο καθεστώς όσον αφορά τα προγράμματα δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας. Κατά την εξέταση του είδους και της συχνότητας των δοκιμών που πρέπει να διενεργούνται, θα πρέπει να εξισορροπούν δεόντως τον στόχο της διατήρησης υψηλής ψηφιακής επιχειρησιακής ανθεκτικότητας, τους διαθέσιμους πόρους και το συνολικό προφίλ κινδύνου τους. Οι πολύ μικρές επιχειρήσεις και οι χρηματοοικονομικές οντότητες που υπόκεινται στο απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ βάσει του παρόντος κανονισμού θα πρέπει να εξαιρούνται από την απαίτηση διενέργειας προηγμένων δοκιμών σε εργαλεία, συστήματα και διαδικασίες ΤΠΕ που βασίζονται σε δοκιμές παρείσδυσης βάσει απειλών (TLPT), καθώς μόνο οι χρηματοοικονομικές οντότητες που πληρούν τα κριτήρια που καθορίζονται στον παρόντα κανονισμό θα πρέπει να υποχρεούνται να διενεργούν τις εν λόγω δοκιμές. Λόγω των περιορισμένων ικανοτήτων τους, οι πολύ μικρές επιχειρήσεις θα πρέπει να είναι σε θέση να συμφωνήσουν με τον τρίτο πάροχο υπηρεσιών ΤΠΕ να αναθέσουν τα δικαιώματα πρόσβασης, επιθεώρησης και ελέγχου της χρηματοοικονομικής οντότητας σε ανεξάρτητο τρίτο μέρος, το οποίο θα οριστεί από τον τρίτο πάροχο υπηρεσιών ΤΠΕ, υπό την προϋπόθεση ότι η χρηματοοικονομική οντότητα είναι σε θέση να ζητήσει, ανά πάσα στιγμή, όλες τις σχετικές πληροφορίες και διασφαλίσεις σχετικά με τις επιδόσεις του τρίτου παρόχου υπηρεσιών ΤΠΕ από το αντίστοιχο ανεξάρτητο τρίτο μέρος.

(44) Δεδομένου ότι μόνο οι χρηματοοικονομικές οντότητες που ταυτοποιούνται για τους σκοπούς των προηγμένων δοκιμών ψηφιακής ανθεκτικότητας θα πρέπει να υποχρεούνται να διενεργούν δοκιμές παρείσδυσης βάσει απειλών, οι διοικητικές διαδικασίες και το οικονομικό κόστος που συνεπάγεται η διενέργεια των δοκιμών αυτών θα πρέπει να βαρύνουν μικρό ποσοστό των χρηματοοικονομικών οντοτήτων.

(45) Για τους σκοπούς της διασφάλισης της πλήρους ευθυγράμμισης και της συνολικής συνοχής μεταξύ των επιχειρηματικών στρατηγικών των χρηματοοικονομικών οντοτήτων, αφενός, και της άσκησης της διαχείρισης κινδύνων ΤΠΕ, αφετέρου, τα διοικητικά όργανα των χρηματοοικονομικών οντοτήτων θα πρέπει να υποχρεούνται να επιτελούν καίριο και ενεργό ρόλο στον προσανατολισμό και στην προσαρμογή του πλαισίου διαχείρισης κινδύνων ΤΠΕ, καθώς και της συνολικής στρατηγικής για την ψηφιακή λειτουργική ανθεκτικότητα. Η προσέγγιση που οφείλουν να υιοθετούν τα διοικητικά όργανα δεν θα πρέπει να επικεντρώνεται μόνο στα μέσα διασφάλισης της ανθεκτικότητας των συστημάτων ΤΠΕ, αλλά θα πρέπει επίσης να καλύπτει τα άτομα και τις διαδικασίες μέσω μιας δέσμης πολιτικών που καλλιεργούν, σε κάθε εταιρικό επίπεδο και για το σύνολο των μελών του προσωπικού, ισχυρό αίσθημα ευαισθητοποίησης όσον αφορά τους κινδύνους στον κυβερνοχώρο, καθώς και την ανάληψη δέσμευσης για την τήρηση αυστηρής κυβερνοϋγιεινής σε όλα τα επίπεδα. Η τελική ευθύνη του διοικητικού οργάνου για τη διαχείριση κινδύνων ΤΠΕ της χρηματοοικονομικής οντότητας θα πρέπει να αποτελεί γενική αρχή της εν λόγω ολοκληρωμένης προσέγγισης, η οποία θα μετουσιώνεται περαιτέρω στη διαρκή συμμετοχή του διοικητικού οργάνου στον έλεγχο της παρακολούθησης της διαχείρισης κινδύνων ΤΠΕ.

(46) Επιπλέον, η αρχή της πλήρους και τελικής ευθύνης του διοικητικού οργάνου για τη διαχείριση κινδύνων ΤΠΕ της χρηματοοικονομικής οντότητας συμβαδίζει με την ανάγκη εξασφάλισης επιπέδου επενδύσεων που σχετίζονται με τις ΤΠΕ και συνολικού προϋπολογισμού για τη χρηματοοικονομική οντότητα που θα επιτρέψουν στη χρηματοοικονομική οντότητα να επιτύχει υψηλό επίπεδο ψηφιακής επιχειρησιακής ανθεκτικότητας.

(47) Βάσει σχετικών διεθνών, εθνικών και κλαδικών βέλτιστων πρακτικών, κατευθυντήριων γραμμών, συστάσεων και προσεγγίσεων για τη διαχείριση των κινδύνων στον κυβερνοχώρο, ο παρών κανονισμός προάγει μια σειρά αρχών που διευκολύνουν τη συνολική διάρθρωση της διαχείρισης κινδύνων ΤΠΕ. Κατά συνέπεια, στον βαθμό που οι κύριες ικανότητες τις οποίες διαθέτουν οι χρηματοοικονομικές οντότητες ανταποκρίνονται στις διάφορες λειτουργίες στη διαχείριση κινδύνων ΤΠΕ (προσδιορισμός, προστασία και πρόληψη, εντοπισμός, αντιμετώπιση και ανάκαμψη, μάθηση και εξέλιξη και επικοινωνία) που καθορίζονται στον παρόντα κανονισμό, οι χρηματοοικονομικές οντότητες θα πρέπει να εξακολουθήσουν να έχουν τη διακριτική ευχέρεια να χρησιμοποιούν μοντέλα διαχείρισης κινδύνων ΤΠΕ τα οποία πλαισιώνονται ή κατηγοριοποιούνται με διαφορετικό τρόπο.

(48) Προκειμένου να συμβαδίζουν με το εξελισσόμενο τοπίο των κυβερνοαπειλών, οι χρηματοοικονομικές οντότητες θα πρέπει να διατηρούν επικαιροποιημένα συστήματα ΤΠΕ, τα οποία είναι αξιόπιστα και ικανά να εξασφαλίζουν όχι μόνο την επεξεργασία δεδομένων που απαιτείται για τις υπηρεσίες τους, αλλά και επαρκή τεχνολογική ανθεκτικότητα που θα τους επιτρέπει να ανταποκρίνονται δεόντως στις πρόσθετες ανάγκες επεξεργασίας λόγω ακραίων συνθηκών της αγοράς ή άλλων αντίξοων καταστάσεων.

(49) Απαιτούνται αποτελεσματικά σχέδια επιχειρησιακής συνέχειας και ανάκαμψης ώστε οι χρηματοοικονομικές οντότητες να είναι σε θέση να επιλύουν άμεσα και γρήγορα συμβάντα που σχετίζονται με τις ΤΠΕ, ιδίως κυβερνοεπιθέσεις, περιορίζοντας τις ζημίες και δίνοντας προτεραιότητα στην επανέναρξη των δραστηριοτήτων και στην ανάληψη δράσεων ανάκαμψης, σύμφωνα με τις πολιτικές τους για τη δημιουργία εφεδρικών συστημάτων. Ωστόσο, η επανέναρξη αυτή δεν θα πρέπει σε καμία περίπτωση να θέτει σε κίνδυνο την ακεραιότητα και την ασφάλεια των συστημάτων δικτύου και πληροφοριών ή τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων.

(50) Μολονότι ο παρών κανονισμός παρέχει στις χρηματοοικονομικές οντότητες τη δυνατότητα να καθορίζουν τους στόχους τους για τον χρόνο ανάκαμψης και το σημείο ανάκαμψης με ευέλικτο τρόπο και, κατ' επέκταση, να θέτουν τέτοιους στόχους λαμβάνοντας πλήρως υπόψη τη φύση και την κρισιμότητα των σχετικών λειτουργιών, καθώς και τυχόν ειδικών επιχειρηματικών αναγκών, θα πρέπει, ωστόσο, να τις υποχρεώνει να αξιολογούν τις συνολικές δυνητικές επιπτώσεις στην αποτελεσματικότητα της αγοράς, κατά τον καθορισμό των εν λόγω στόχων.

(51) Οι φορείς διάδοσης κυβερνοεπιθέσεων τείνουν να επιδιώκουν οικονομικά οφέλη απευθείας στην πηγή, εκθέτοντας έτσι τις χρηματοοικονομικές οντότητες σε σημαντικές συνέπειες. Για να προληφθεί η απώλεια της ακεραιότητας ή της διαθεσιμότητας των συστημάτων ΤΠΕ και, ως εκ τούτου, να αποφευχθούν οι παραβιάσεις δεδομένων και η ζημία σε υλική υποδομή ΤΠΕ, η αναφορά μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ από χρηματοοικονομικές οντότητες θα πρέπει να βελτιωθεί και να εξορθολογιστεί σημαντικά. Η αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ θα πρέπει να εναρμονιστεί μέσω της θέσπισης απαίτησης για όλες τις χρηματοοικονομικές οντότητες να υποβάλλουν αναφορά απευθείας στις οικείες αρμόδιες αρχές τους. Όταν μια χρηματοοικονομική οντότητα υπόκειται σε εποπτεία από περισσότερες από μία εθνικές αρμόδιες αρχές, τα κράτη μέλη θα πρέπει να ορίζουν μία μόνο αρμόδια αρχή ως αποδέκτη της εν λόγω αναφοράς. Τα πιστωτικά ιδρύματα που ταξινομούνται ως σημαντικά σύμφωνα με το άρθρο 6 παράγραφος 4 του κανονισμού (ΕΕ) αριθ. 1024/2013 του Συμβουλίου ([19]) θα πρέπει να υποβάλλουν την εν λόγω αναφορά στις εθνικές αρμόδιες αρχές, οι οποίες θα πρέπει στη συνέχεια να διαβιβάζουν την αναφορά στην Ευρωπαϊκή Κεντρική Τράπεζα (ΕΚΤ).

(52) Η απευθείας αναφορά θα πρέπει να επιτρέπει στις αρχές χρηματοοικονομικής εποπτείας να έχουν άμεση πρόσβαση σε πληροφορίες για μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ. Οι αρχές χρηματοοικονομικής εποπτείας θα πρέπει με τη σειρά τους να διαβιβάζουν λεπτομέρειες σχετικά με μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ σε δημόσιες μη χρηματοοικονομικές αρχές (όπως οι αρμόδιες αρχές και τα ενιαία σημεία επαφής βάσει της οδηγίας (ΕΕ) 2022/2555 εθνικές αρχές προστασίας δεδομένων και αρχές επιβολής του νόμου για μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ ποινικού χαρακτήρα), προκειμένου να ενισχυθεί η ευαισθητοποίηση των εν λόγω αρχών σχετικά με αυτά τα συμβάντα και, στην περίπτωση των CSIRT, να διευκολυνθεί η άμεση συνδρομή που μπορεί να παρέχεται στις χρηματοοικονομικές οντότητες, κατά περίπτωση. Επιπλέον, τα κράτη μέλη θα πρέπει να είναι σε θέση να καθορίζουν ότι οι ίδιες οι χρηματοοικονομικές οντότητες θα πρέπει να παρέχουν τις πληροφορίες αυτές σε δημόσιες αρχές εκτός του τομέα των χρηματοοικονομικών υπηρεσιών. Οι εν λόγω ροές πληροφοριών θα πρέπει να επιτρέπουν στις χρηματοοικονομικές οντότητες να επωφελούνται άμεσα από κάθε σχετική τεχνική συμβολή, συμβουλές σχετικά με τα διορθωτικά μέτρα και επακόλουθη παρακολούθηση από τις εν λόγω αρχές. Η διοχέτευση πληροφοριών για μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ θα πρέπει να είναι αμοιβαία: οι αρχές χρηματοοικονομικής εποπτείας θα πρέπει να παρέχουν στη χρηματοοικονομική οντότητα κάθε αναγκαία παρατήρηση ή καθοδήγηση, ενώ οι ΕΕΑ θα πρέπει να ανταλλάσσουν ανωνυμοποιημένα δεδομένα σχετικά με κυβερνοαπειλές και ευπάθειες που σχετίζονται με ένα συμβάν, με σκοπό την ενίσχυση της ευρύτερης συλλογικής άμυνας.

(53) Ενώ όλες οι χρηματοοικονομικές οντότητες θα πρέπει να υπόκεινται στην υποχρέωση αναφοράς συμβάντων, η απαίτηση αυτή δεν αναμένεται να τις επηρεάσει όλες με τον ίδιο τρόπο. Πράγματι, τα σχετικά κατώτατα όρια σημαντικότητας, καθώς και τα χρονοδιαγράμματα υποβολής αναφορών, θα πρέπει να προσαρμόζονται δεόντως, στο πλαίσιο των κατ' εξουσιοδότηση πράξεων που βασίζονται στα ρυθμιστικά τεχνικά πρότυπα που θα αναπτύξουν οι ΕΕΑ, με σκοπό την κάλυψη μόνο μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ. Επιπλέον, οι ιδιαιτερότητες των χρηματοοικονομικών οντοτήτων θα πρέπει να λαμβάνονται υπόψη κατά τον καθορισμό χρονοδιαγραμμάτων για τις υποχρεώσεις υποβολής αναφορών.

(54) Ο παρών κανονισμός θα πρέπει να απαιτεί από τα πιστωτικά ιδρύματα, τα ιδρύματα πληρωμών, τους παρόχους υπηρεσιών πληροφοριών λογαριασμού και τα ιδρύματα ηλεκτρονικού χρήματος να αναφέρουν όλα τα λειτουργικά συμβάντα ή τα συμβάντα ασφάλειας που σχετίζονται με πληρωμές —τα οποία έχουν αναφερθεί προηγουμένως βάσει της οδηγίας (ΕΕ) 2015/2366— ανεξάρτητα από τη φύση του συμβάντος όσον αφορά τις ΤΠΕ.

([19]) Κανονισμός (ΕΕ) αριθ. 1024/2013 του Συμβουλίου, της 15ης Οκτωβρίου 2013, για την ανάθεση ειδικών καθηκόντων στην Ευρωπαϊκή Κεντρική Τράπεζα σχετικά με τις πολιτικές που αφορούν την προληπτική εποπτεία των πιστωτικών ιδρυμάτων (ΕΕ L 287 της 29.10.2013, σ. 63).

(55) Οι ΕΕΑ θα πρέπει να επιφορτιστούν με την αξιολόγηση της σκοπιμότητας και των προϋποθέσεων για πιθανή συγκέντρωση των αναφορών συμβάντων που σχετίζονται με τις ΤΠΕ σε επίπεδο Ένωσης. Η συγκέντρωση αυτή θα μπορούσε να συνίσταται σε ενιαίο κόμβο της ΕΕ για αναφορά μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ, είτε με την άμεση παραλαβή των σχετικών εκθέσεων και την αυτόματη κοινοποίησή τους στις εθνικές αρμόδιες αρχές είτε με τη συγκέντρωση απλώς των σχετικών εκθέσεων που διαβιβάζονται από τις εθνικές αρμόδιες αρχές και την άσκηση, κατ' αυτόν τον τρόπο, συντονιστικού ρόλου. Θα πρέπει να ανατεθεί στις ΕΕΑ να εκπονήσουν, σε διαβούλευση με την ΕΚΤ και τον ENISA, κοινή έκθεση στην οποία θα διερευνάται η σκοπιμότητα της δημιουργίας ενιαίου κόμβου της ΕΕ.

(56) Για τους σκοπούς της διασφάλισης υψηλού επιπέδου ψηφιακής επιχειρησιακής ανθεκτικότητας, και σύμφωνα τόσο με τα σχετικά διεθνή πρότυπα (π.χ. τα θεμελιώδη στοιχεία της G7 για τις δοκιμές παρείσδυσης βάσει απειλών), όσο και με τα πλαίσια που εφαρμόζονται στην Ένωση, όπως το TIBER–EU, οι χρηματοοικονομικές οντότητες θα πρέπει να υποβάλλουν τακτικά σε δοκιμή τα οικεία συστήματα ΤΠΕ και το προσωπικό τους το οποίο έχει αρμοδιότητες σχετικές με τις ΤΠΕ ως προς την αποτελεσματικότητα των ικανοτήτων τους όσον αφορά την πρόληψη, τον εντοπισμό, την αντιμετώπιση και την ανάκαμψη, ώστε να αποκαλύπτουν και να αντιμετωπίζουν πιθανές ευπάθειες των ΤΠΕ. Για τη συνεκτίμηση των διαφορών που υπάρχουν τόσο μεταξύ όσο και εντός των διαφόρων χρηματοοικονομικών υποτομέων όσον αφορά το επίπεδο ετοιμότητας των χρηματοοικονομικών οντοτήτων στον τομέα της κυβερνοασφάλειας, οι δοκιμές θα πρέπει να περιλαμβάνουν ευρύ φάσμα εργαλείων και δράσεων, που εκτείνονται από την αξιολόγηση βασικών απαιτήσεων (π.χ. αξιολογήσεις και σαρώσεις ευπάθειας, αναλύσεις ανοικτής πηγής, αξιολογήσεις ασφάλειας δικτύου, αναλύσεις ελλείψεων, επισκοπήσεις υλικής ασφάλειας, λύσεις λογισμικού ερωτηματολογίων και σάρωσης, επανεξετάσεις πηγαίου κώδικα όπου αυτό είναι εφικτό, δοκιμές βάσει σεναρίων, δοκιμές συμβατότητας, δοκιμές επιδόσεων ή διατερματικές δοκιμές), έως πιο προηγμένες δοκιμές μέσω TLPT. Αυτού του είδους οι προηγμένες δοκιμές θα πρέπει να απαιτούνται μόνο από τις χρηματοοικονομικές οντότητες που παρουσιάζουν επαρκή βαθμό ωριμότητας από πλευράς ΤΠΕ, ώστε να τις διενεργούν εύλογα. Συνεπώς, οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας που απαιτούνται βάσει του παρόντος κανονισμού θα πρέπει να είναι πιο απαιτητικές για τις χρηματοοικονομικές οντότητες που πληρούν τα κριτήρια που καθορίζονται στον παρόντα κανονισμό (για παράδειγμα, μεγάλα, συστημικά και ώριμα για ΤΠΕ πιστωτικά ιδρύματα, χρηματιστήρια, κεντρικά αποθετήρια τίτλων και κεντρικοί αντισυμβαλλόμενοι) από ό,τι για άλλες χρηματοοικονομικές οντότητες. Ταυτόχρονα, οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας μέσω TLPT θα πρέπει να είναι περισσότερο σημαντικές για χρηματοοικονομικές οντότητες οι οποίες δραστηριοποιούνται σε βασικούς υποτομείς χρηματοοικονομικών υπηρεσιών και διαδραματίζουν συστημικό ρόλο (για παράδειγμα, πληρωμές, τράπεζες και εκκαθάριση και διακανονισμός) και λιγότερο σημαντικές για άλλους υποτομείς (για παράδειγμα, διαχειριστές περιουσιακών στοιχείων και οργανισμοί αξιολόγησης της πιστοληπτικής ικανότητας).

(57) Οι χρηματοοικονομικές οντότητες οι οποίες ασχολούνται με διασυνοριακές δραστηριότητες και ασκούν το δικαίωμα ελεύθερης εγκατάστασης ή παροχής υπηρεσιών εντός της Ένωσης θα πρέπει να συμμορφώνονται με ένα ενιαίο σύνολο απαιτήσεων προηγμένων δοκιμών (δηλαδή TLPT) στο κράτος μέλος προέλευσής τους που θα πρέπει να περιλαμβάνει τις υποδομές ΤΠΕ σε όλες τις δικαιοδοσίες στις οποίες δραστηριοποιείται ο διασυνοριακός χρηματοοικονομικός όμιλος εντός της Ένωσης, ώστε να διασφαλίζεται ότι αυτοί οι διασυνοριακοί χρηματοοικονομικοί όμιλοι επιβαρύνονται με το κόστος δοκιμών που σχετίζονται με τις ΤΠΕ μόνο σε μία δικαιοδοσία.

(58) Προκειμένου να αξιοποιηθεί η εμπειρογνωσία που έχει ήδη αποκτηθεί από ορισμένες αρμόδιες αρχές, ιδίως όσον αφορά την εφαρμογή του πλαισίου TIBER–EU, ο παρών κανονισμός θα πρέπει να επιτρέπει στα κράτη μέλη να ορίζουν μία μόνο δημόσια αρχή ως υπεύθυνη στον χρηματοοικονομικό τομέα, σε εθνικό επίπεδο, για όλα τα θέματα TLPT, ή στις αρμόδιες αρχές να αναθέτουν, ελλείψει τέτοιου ορισμού, την άσκηση καθηκόντων που σχετίζονται με TLPT σε άλλη εθνική χρηματοοικονομική αρμόδια αρχή.

(59) Δεδομένου ότι ο παρών κανονισμός δεν απαιτεί από τις χρηματοοικονομικές οντότητες να καλύπτουν όλες τις κρίσιμες ή σημαντικές λειτουργίες σε μία και μόνη δοκιμή παρείσδυσης βάσει απειλών, οι χρηματοοικονομικές οντότητες θα πρέπει να είναι ελεύθερες να καθορίζουν ποιες και πόσες κρίσιμες ή σημαντικές λειτουργίες θα πρέπει να περιλαμβάνονται στο πεδίο εφαρμογής της εν λόγω δοκιμής.

(60) Οι ομαδικές δοκιμές κατά την έννοια του παρόντος κανονισμού —που περιλαμβάνουν τη συμμετοχή διαφόρων χρηματοοικονομικών οντοτήτων σε μια TLPT και για τις οποίες ένας τρίτος πάροχος υπηρεσιών ΤΠΕ μπορεί να συνάψει απευθείας συμβατικές ρυθμίσεις με εξωτερικό δοκιμαστή— θα πρέπει να επιτρέπονται μόνο όταν η ποιότητα ή η ασφάλεια των υπηρεσιών που παρέχονται από τον τρίτο πάροχο υπηρεσιών ΤΠΕ σε πελάτες που είναι οντότητες οι οποίες δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού ή η εμπιστευτικότητα των δεδομένων που σχετίζονται με τις εν λόγω υπηρεσίες αναμένεται ευλόγως να επηρεαστούν αρνητικά. Οι ομαδικές δοκιμές θα πρέπει επίσης να υπόκεινται σε διασφαλίσεις (κατεύθυνση από καθορισμένη χρηματοοικονομική οντότητα, βαθμονόμηση του αριθμού των συμμετεχουσών χρηματοοικονομικών οντοτήτων), ώστε να διασφαλίζεται η διενέργεια αυστηρών δοκιμών για τις εμπλεκόμενες χρηματοοικονομικές οντότητες που πληρούν τους στόχους της TLPT σύμφωνα με τον παρόντα κανονισμό.

(61) Προκειμένου να αξιοποιηθούν οι εσωτερικοί πόροι που διατίθενται σε εταιρικό επίπεδο, ο παρών κανονισμός θα πρέπει να επιτρέπει τη χρήση εσωτερικών δοκιμαστών για τους σκοπούς της διεξαγωγής TLPT, υπό την προϋπόθεση ότι υπάρχει εποπτική έγκριση, δεν υπάρχουν συγκρούσεις συμφερόντων και υπάρχει περιοδική εναλλαγή χρήσης εσωτερικών και εξωτερικών δοκιμαστών (κάθε τρεις δοκιμές), απαιτώντας παράλληλα από τον πάροχο των πληροφοριών σχετικά με τις απειλές στο πλαίσιο TLPT να είναι πάντα εξωτερικός σε σχέση με τη χρηματοοικονομική οντότητα. Η χρηματοοικονομική οντότητα θα πρέπει να εξακολουθεί να ευθύνεται πλήρως για τη διεξαγωγή TLPT. Οι βεβαιώσεις που παρέχονται από τις αρχές θα πρέπει να εξυπηρετούν αποκλειστικά τον σκοπό της αμοιβαίας αναγνώρισης και δεν θα πρέπει να αποκλείουν τυχόν επακόλουθες ενέργειες που απαιτούνται για την αντιμετώπιση των κινδύνων ΤΠΕ στους οποίους είναι εκτεθειμένη η χρηματοοικονομική οντότητα, ούτε θα πρέπει να θεωρούνται ως εποπτική έγκριση των ικανοτήτων διαχείρισης και μετριασμού των κινδύνων ΤΠΕ μιας χρηματοοικονομικής οντότητας.

(62) Για τη διασφάλιση της ορθής παρακολούθησης των κινδύνων τρίτων παρόχων ΤΠΕ στον χρηματοοικονομικό τομέα, είναι απαραίτητη η θέσπιση ενός συνόλου κανόνων βάσει αρχών, ώστε να παρέχεται καθοδήγηση στις χρηματοοικονομικές οντότητες, όταν παρακολουθούν κίνδυνο που προκύπτει στο πλαίσιο λειτουργιών που αποτελούν αντικείμενο εξωτερικής ανάθεσης σε τρίτους παρόχους υπηρεσιών ΤΠΕ, ιδίως για υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες καθώς και, γενικότερα, στο πλαίσιο όλων των εξαρτήσεων από τρίτους παρόχους ΤΠΕ.

(63) Για να αντιμετωπιστεί η πολυπλοκότητα των διάφορων πηγών κινδύνων ΤΠΕ, λαμβανομένων παράλληλα υπόψη της πληθώρας και της ποικιλομορφίας των παρόχων τεχνολογικών λύσεων που επιτρέπουν την ομαλή παροχή χρηματοοικονομικών υπηρεσιών, ο παρών κανονισμός θα πρέπει να καλύπτει ευρύ φάσμα τρίτων παρόχων υπηρεσιών ΤΠΕ, συμπεριλαμβανομένων των παρόχων υπηρεσιών υπολογιστικού νέφους, λογισμικού, υπηρεσιών ανάλυσης δεδομένων και παρόχων υπηρεσιών κέντρου δεδομένων. Ομοίως, δεδομένου ότι οι χρηματοοικονομικές οντότητες θα πρέπει να εντοπίζουν και να διαχειρίζονται αποτελεσματικά και συνεκτικά όλα τα είδη κινδύνων, μεταξύ άλλων στο πλαίσιο των υπηρεσιών ΤΠΕ που παρέχονται στο πλαίσιο ενός χρηματοοικονομικού ομίλου, θα πρέπει να διευκρινιστεί ότι επιχειρήσεις που αποτελούν μέρος χρηματοοικονομικού ομίλου και παρέχουν υπηρεσίες ΤΠΕ κυρίως στη μητρική τους επιχείρηση ή σε θυγατρικές ή υποκαταστήματα της μητρικής τους επιχείρησης, καθώς και χρηματοοικονομικές οντότητες που παρέχουν υπηρεσίες ΤΠΕ σε άλλες χρηματοοικονομικές οντότητες, θα πρέπει επίσης να θεωρούνται τρίτοι πάροχοι υπηρεσιών ΤΠΕ δυνάμει του παρόντος κανονισμού. Τέλος, δεδομένου ότι η εξελισσόμενη αγορά υπηρεσιών πληρωμών εξαρτάται όλο και περισσότερο από πολύπλοκες τεχνικές λύσεις, και λόγω των αναδυόμενων τύπων υπηρεσιών πληρωμών και λύσεων που σχετίζονται με τις πληρωμές, οι συμμετέχοντες στο οικοσύστημα υπηρεσιών πληρωμών, οι οποίοι παρέχουν δραστηριότητες επεξεργασίας πληρωμών ή λειτουργούν υποδομές πληρωμών, θα πρέπει επίσης να θεωρούνται τρίτοι πάροχοι υπηρεσιών ΤΠΕ δυνάμει του παρόντος κανονισμού, με εξαίρεση τις κεντρικές τράπεζες κατά τη λειτουργία συστημάτων πληρωμών ή διακανονισμού αξιογράφων και τις δημόσιες αρχές όταν παρέχουν υπηρεσίες που σχετίζονται με τις ΤΠΕ στο πλαίσιο της εκπλήρωσης κρατικών λειτουργιών.

(64) Οι χρηματοοικονομικές οντότητες θα πρέπει να φέρουν ανά πάσα στιγμή την πλήρη ευθύνη για τη συμμόρφωση με τις υποχρεώσεις τους που απορρέουν από τον παρόντα κανονισμό. Οι χρηματοοικονομικές οντότητες θα πρέπει να εφαρμόζουν αναλογική προσέγγιση όσον αφορά την παρακολούθηση κινδύνων που ανακύπτουν σε επίπεδο τρίτων παρόχων υπηρεσιών ΤΠΕ, λαμβανομένων δεόντως υπόψη της φύσης, της κλίμακας, της πολυπλοκότητας και της σημασίας των εξαρτήσεών τους που σχετίζονται με τις ΤΠΕ, της κρισιμότητας ή της σημασίας των υπηρεσιών, των διαδικασιών ή των λειτουργιών που υπόκεινται στις συμβατικές ρυθμίσεις και, εντέλει, βάσει προσεκτικής αξιολόγησης κάθε δυνητικού αντικτύπου στη συνέχεια και στην ποιότητα των χρηματοοικονομικών υπηρεσιών σε μεμονωμένο επίπεδο και σε επίπεδο ομίλου, ανάλογα με την περίπτωση.

(65) Για την άσκηση καθηκόντων παρακολούθησης αυτού του είδους θα πρέπει να ακολουθείται μια στρατηγική προσέγγιση ως προς τους κινδύνους τρίτων παρόχων ΤΠΕ, η οποία θα επισημοποιείται μέσω της υιοθέτησης, από το διοικητικό όργανο της χρηματοοικονομικής οντότητας, ειδικής στρατηγικής κινδύνων τρίτου παρόχου ΤΠΕ που θα βασίζεται στον διαρκή έλεγχο όλων των εξαρτήσεων από τρίτους παρόχους ΤΠΕ. Για τη βελτίωση της ευαισθητοποίησης όσον αφορά την εποπτεία των εξαρτήσεων από τρίτους παρόχους ΤΠΕ και με σκοπό την περαιτέρω στήριξη των εργασιών εντός του πλαισίου εποπτείας που θεσπίζεται με τον παρόντα κανονισμό, όλες οι χρηματοοικονομικές οντότητες θα πρέπει να υποχρεούνται να τηρούν μητρώο πληροφοριών με όλες τις συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ οι οποίες παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ. Οι αρχές χρηματοοικονομικής εποπτείας θα πρέπει να είναι σε θέση να ζητούν το πλήρες μητρώο ή συγκεκριμένα τμήματά του και, ως εκ τούτου, να λαμβάνουν βασικές πληροφορίες για την ευρύτερη κατανόηση των εξαρτήσεων των χρηματοοικονομικών οντοτήτων από τις ΤΠΕ.

(66) Μια διεξοδική ανάλυση πριν από την ανάθεση θα πρέπει να στηρίζει και να προηγείται της επίσημης σύναψης συμβατικών ρυθμίσεων, εστιάζοντας ιδίως σε στοιχεία όπως η κρισιμότητα ή η σημασία των υπηρεσιών που υποστηρίζονται από την προβλεπόμενη σύμβαση ΤΠΕ, οι αναγκαίες εποπτικές εγκρίσεις ή άλλοι όροι, ο πιθανός συνεπαγόμενος κίνδυνος συγκέντρωσης, καθώς και η εφαρμογή της δέουσας επιμέλειας κατά τη διαδικασία επιλογής και αξιολόγησης τρίτων παρόχων υπηρεσιών ΤΠΕ και η αξιολόγηση πιθανών συγκρούσεων συμφερόντων. Όσον αφορά τις συμβατικές ρυθμίσεις οι οποίες αφορούν κρίσιμες ή σημαντικές λειτουργίες, οι χρηματοοικονομικές οντότητες θα πρέπει να λαμβάνουν δεόντως υπόψη τη χρήση από τρίτους παρόχους υπηρεσιών ΤΠΕ των πλέον επικαιροποιημένων και ύψιστων προτύπων ασφάλειας πληροφοριών. Η καταγγελία των συμβατικών ρυθμίσεων θα μπορούσε να οφείλεται τουλάχιστον σε σύνολο περιστάσεων που παρουσιάζουν ελλείψεις σε επίπεδο τρίτου παρόχου υπηρεσιών ΤΠΕ, ιδίως σημαντικές παραβιάσεις νόμων ή

συμβατικών όρων, περιστάσεις που αποκαλύπτουν πιθανή μεταβολή της εκτέλεσης των καθηκόντων που προβλέπονται στις συμβατικές ρυθμίσεις, αποδεικτικά στοιχεία αδυναμιών του τρίτου παρόχου υπηρεσιών ΤΠΕ στη συνολική διαχείριση κινδύνων ΤΠΕ ή περιστάσεις που υποδεικνύουν την αδυναμία της σχετικής αρμόδιας αρχής να εποπτεύει αποτελεσματικά τη χρηματοοικονομική οντότητα.

(67) Για την αντιμετώπιση των συστημικών επιπτώσεων του κινδύνου συγκέντρωσης τρίτων παρόχων ΤΠΕ, ο παρών κανονισμός προάγει ισορροπημένη λύση μέσω της υιοθέτησης ευέλικτης και σταδιακής προσέγγισης στον εν λόγω κίνδυνο συγκέντρωσης, δεδομένου ότι η επιβολή τυχόν αυστηρών ανώτατων ορίων ή αυστηρών περιορισμών ενδέχεται να εμποδίσει τη διεξαγωγή επιχειρήσεων και να περιορίσει τη συμβατική ελευθερία. Οι χρηματοοικονομικές οντότητες θα πρέπει να αξιολογούν ενδελεχώς τις συμβατικές ρυθμίσεις τις οποίες προβλέπουν για τον προσδιορισμό της πιθανότητας εμφάνισης κινδύνου αυτού του είδους, μεταξύ άλλων μέσω εμπεριστατωμένων αναλύσεων των ρυθμίσεων υπεργολαβίας, ιδίως όταν συνάπτονται με τρίτους παρόχους υπηρεσιών ΤΠΕ που είναι εγκατεστημένοι σε τρίτη χώρα. Στο παρόν στάδιο, και για τους σκοπούς της επίτευξης δίκαιης ισορροπίας μεταξύ της επιτακτικής ανάγκης για διατήρηση της συμβατικής ελευθερίας και της ανάγκης για διασφάλιση της χρηματοοικονομικής σταθερότητας, δεν κρίνεται σκόπιμη η θέσπιση κανόνων περί αυστηρών ανώτατων ορίων και περιορισμών όσον αφορά την έκθεση σε κινδύνους τρίτων παρόχων ΤΠΕ. Εντός του πλαισίου εποπτείας, ο κύριος εποπτικός φορέας που έχει οριστεί σύμφωνα με τον παρόντα κανονισμό θα πρέπει, όσον αφορά τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, να δίνει ιδιαίτερη προσοχή στην πλήρη κατανόηση της έκτασης των αλληλεξαρτήσεων, να ανακαλύπτει συγκεκριμένες περιπτώσεις στις οποίες ο υψηλός βαθμός συγκέντρωσης κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ στην Ένωση είναι πιθανό να ασκήσει πιέσεις στη σταθερότητα και στην ακεραιότητα του χρηματοοικονομικού συστήματος της Ένωσης και να διατηρεί διάλογο με κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, όταν εντοπίζεται ο συγκεκριμένος κίνδυνος.

(68) Για την αξιολόγηση και την παρακολούθηση σε τακτική βάση της ικανότητας τρίτου παρόχου υπηρεσιών ΤΠΕ να παρέχει με ασφάλεια υπηρεσίες σε χρηματοοικονομική οντότητα χωρίς δυσμενείς επιπτώσεις στην ψηφιακή επιχειρησιακή ανθεκτικότητά της, θα πρέπει να εναρμονιστούν διάφορα βασικά συμβατικά στοιχεία με τρίτους παρόχους υπηρεσιών ΤΠΕ. Η εναρμόνιση αυτή θα πρέπει να καλύπτει ελάχιστους τομείς που είναι ζωτικής σημασίας για την πλήρη παρακολούθηση από τη χρηματοοικονομική οντότητα των κινδύνων που θα μπορούσαν να προκύψουν από τον τρίτο πάροχο υπηρεσιών ΤΠΕ, από την άποψη της ανάγκης μιας χρηματοοικονομικής οντότητας να διασφαλίσει την ψηφιακή ανθεκτικότητά της, διότι εξαρτάται σε μεγάλο βαθμό από τη σταθερότητα, τη λειτουργικότητα, τη διαθεσιμότητα και την ασφάλεια των υπηρεσιών ΤΠΕ που λαμβάνει.

(69) Κατά την επαναδιαπραγμάτευση συμβατικών ρυθμίσεων με σκοπό την ευθυγράμμιση με τις απαιτήσεις του παρόντος κανονισμού, οι χρηματοοικονομικές οντότητες και οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ θα πρέπει να διασφαλίζουν την κάλυψη των βασικών συμβατικών διατάξεων, όπως προβλέπεται στον παρόντα κανονισμό.

(70) Ο ορισμός της «κρίσιμης ή σημαντικής λειτουργίας» που προβλέπεται στον παρόντα κανονισμό περιλαμβάνει τον ορισμό των «κρίσιμων λειτουργιών», όπως προβλέπεται στο άρθρο 2 παράγραφος 1 σημείο 35) της οδηγίας 2014/59/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([20]). Ως εκ τούτου, οι λειτουργίες που θεωρούνται κρίσιμες σύμφωνα με την οδηγία 2014/59/ΕΕ περιλαμβάνονται στον ορισμό των κρίσιμων λειτουργιών κατά την έννοια του παρόντος κανονισμού.

(71) Ανεξάρτητα από την κρισιμότητα ή τη σημασία της λειτουργίας που υποστηρίζεται από τις υπηρεσίες ΤΠΕ, οι συμβατικές ρυθμίσεις θα πρέπει να προβλέπουν ειδικότερα την πλήρη περιγραφή των λειτουργιών και των υπηρεσιών, των τοποθεσιών στις οποίες παρέχονται οι εν λόγω λειτουργίες και των τοποθεσιών στις οποίες τα δεδομένα θα υποβάλλονται σε επεξεργασία, καθώς και περιγραφή του επιπέδου υπηρεσιών. Άλλα ουσιώδη στοιχεία για να καταστεί δυνατή η παρακολούθηση των κινδύνων τρίτων μερών ΤΠΕ από μια χρηματοοικονομική οντότητα είναι: οι συμβατικές διατάξεις που καθορίζουν τον τρόπο με τον οποίο ο τρίτος πάροχος υπηρεσιών ΤΠΕ διασφαλίζει την προσβασιμότητα, τη διαθεσιμότητα, την ακεραιότητα, την ασφάλεια και την προστασία των δεδομένων προσωπικού χαρακτήρα, οι διατάξεις οι οποίες προβλέπουν τις σχετικές διασφαλίσεις που καθιστούν δυνατές την πρόσβαση, την ανάκτηση και την επιστροφή δεδομένων σε περίπτωση αφερεγγυότητας, εξυγίανσης ή διακοπής των επιχειρηματικών δραστηριοτήτων του τρίτου παρόχου υπηρεσιών ΤΠΕ, καθώς και οι διατάξεις που απαιτούν από τον τρίτο πάροχο υπηρεσιών ΤΠΕ να παρέχει συνδρομή σε περίπτωση συμβάντων ΤΠΕ σε σχέση με τις παρεχόμενες υπηρεσίες, χωρίς πρόσθετο κόστος ή με κόστος που καθορίζεται

([20]) Οδηγία 2014/59/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τη θέσπιση πλαισίου για την ανάκαμψη και την εξυγίανση πιστωτικών ιδρυμάτων και επιχειρήσεων επενδύσεων και για την τροποποίηση της οδηγίας 82/891/ΕΟΚ του Συμβουλίου, και των οδηγιών 2001/24/ΕΚ, 2002/47/ΕΚ, 2004/25/ΕΚ, 2005/56/ΕΚ, 2007/36/ΕΚ, 2011/35/ΕΕ, 2012/30/ΕΕ και 2013/36/ΕΕ, καθώς και των κανονισμών του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ) αριθ. 1093/2010 και (ΕΕ) αριθ. 648/2012 (ΕΕ L 173 της 12.6.2014, σ. 190).

εκ των προτέρων· οι διατάξεις σχετικά με την υποχρέωση του τρίτου παρόχου υπηρεσιών ΤΠΕ να συνεργάζεται πλήρως με τις αρμόδιες αρχές και τις αρχές εξυγίανσης της χρηματοοικονομικής οντότητας· και οι διατάξεις σχετικά με τα δικαιώματα καταγγελίας και συναφείς ελάχιστες περιόδους προειδοποίησης για την καταγγελία των συμβατικών ρυθμίσεων, σύμφωνα με τις προσδοκίες των αρμόδιων αρχών και των αρχών εξυγίανσης.

(72) Εκτός από τις εν λόγω συμβατικές διατάξεις και προκειμένου να διασφαλιστεί ότι οι χρηματοοικονομικές οντότητες διατηρούν τον πλήρη έλεγχο όλων των εξελίξεων σε επίπεδο τρίτων μερών οι οποίες ενδέχεται να βλάψουν την ασφάλεια των ΤΠΕ τους, οι συμβάσεις για την παροχή υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες θα πρέπει επίσης να προβλέπουν τα ακόλουθα: πλήρεις περιγραφές σε επίπεδο υπηρεσιών, με ακριβείς ποσοτικούς και ποιοτικούς στόχους επιδόσεων, ώστε να καταστεί δυνατή η λήψη κατάλληλων διορθωτικών μέτρων, χωρίς αδικαιολόγητη καθυστέρηση, όταν δεν επιτυγχάνονται τα συμφωνηθέντα επίπεδα υπηρεσιών· τις σχετικές περιόδους προειδοποίησης και υποχρεώσεις αναφοράς για τον τρίτο πάροχο υπηρεσιών ΤΠΕ, σε περίπτωση εξελίξεων με δυνητικές σημαντικές επιπτώσεις στην ικανότητα του τρίτου παρόχου υπηρεσιών ΤΠΕ να παρέχει με αποτελεσματικό τρόπο τις αντίστοιχες υπηρεσίες ΤΠΕ· απαίτηση από τον τρίτο πάροχο υπηρεσιών ΤΠΕ να εφαρμόζει και να δοκιμάζει επιχειρησιακά σχέδια έκτακτης ανάγκης και να διαθέτει μέτρα, εργαλεία και πολιτικές ασφάλειας ΤΠΕ που επιτρέπουν την ασφαλή παροχή υπηρεσιών, καθώς και να συμμετέχει και να συνεργάζεται πλήρως στην TLPT που διενεργεί η χρηματοοικονομική οντότητα.

(73) Οι συμβάσεις για την παροχή υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες θα πρέπει επίσης να περιέχουν διατάξεις που διευκολύνουν την άσκηση των δικαιωμάτων πρόσβασης, επιθεώρησης και ελέγχου από τη χρηματοοικονομική οντότητα ή διορισμένο τρίτο και του δικαιώματος λήψης αντιγράφων ως μέσων καίριας σημασίας για τη συνεχή παρακολούθηση των επιδόσεων του τρίτου παρόχου υπηρεσιών ΤΠΕ από τις χρηματοοικονομικές οντότητες, σε συνδυασμό με την πλήρη συνεργασία του παρόχου υπηρεσιών κατά τη διάρκεια των επιθεωρήσεων. Ομοίως, η αρμόδια αρχή της χρηματοοικονομικής οντότητας θα πρέπει να έχει τη δυνατότητα να ασκεί, βάσει ειδοποιήσεων, τα δικαιώματα επιθεώρησης και ελέγχου του τρίτου παρόχου υπηρεσιών ΤΠΕ, με την επιφύλαξη της προστασίας εμπιστευτικών πληροφοριών.

(74) Οι εν λόγω συμβατικές ρυθμίσεις θα πρέπει επίσης να προβλέπουν εξειδικευμένες στρατηγικές εξόδου, ώστε να παρέχεται, ιδίως, η δυνατότητα καθορισμού υποχρεωτικών μεταβατικών περιόδων, κατά τη διάρκεια των οποίων οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ θα πρέπει να εξακολουθούν να παρέχουν τις σχετικές υπηρεσίες με στόχο τη μείωση του κινδύνου διαταραχών στο επίπεδο της χρηματοοικονομικής οντότητας ή την εξασφάλιση της δυνατότητας της χρηματοοικονομικής οντότητας να χρησιμοποιήσει άλλο τρίτο πάροχο υπηρεσιών ΤΠΕ ή να επιλέξει, εναλλακτικά, άλλες λύσεις εντός της επιχείρησης, ανάλογα με την πολυπλοκότητα των παρεχόμενων υπηρεσιών ΤΠΕ. Επιπλέον, οι χρηματοοικονομικές οντότητες που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας 2014/59/ΕΕ θα πρέπει να διασφαλίζουν ότι οι σχετικές συμβάσεις για υπηρεσίες ΤΠΕ είναι άρτιες και πλήρως εκτελεστές σε περίπτωση εξυγίανσης των εν λόγω χρηματοοικονομικών οντοτήτων. Κατά συνέπεια, σύμφωνα με τις προσδοκίες των αρχών εξυγίανσης, οι εν λόγω χρηματοοικονομικές οντότητες θα πρέπει να διασφαλίζουν ότι οι σχετικές συμβάσεις για υπηρεσίες ΤΠΕ είναι ανθεκτικές στην εξυγίανση. Εφόσον εξακολουθούν να εκπληρώνουν τις υποχρεώσεις πληρωμής τους, οι εν λόγω χρηματοοικονομικές οντότητες θα πρέπει να διασφαλίζουν, μεταξύ άλλων απαιτήσεων, ότι οι σχετικές συμβάσεις για υπηρεσίες ΤΠΕ περιέχουν ρήτρες μη καταγγελίας, μη αναστολής και μη τροποποίησης για λόγους αναδιάρθρωσης ή εξυγίανσης.

(75) Επιπλέον, η προαιρετική χρήση τυποποιημένων συμβατικών ρητρών που έχουν αναπτύξει δημόσιες αρχές ή όργανα της Ένωσης, ιδίως η χρήση συμβατικών ρητρών που έχει αναπτύξει η Επιτροπή για τις υπηρεσίες υπολογιστικού νέφους, θα μπορούσε να εξυπηρετεί ακόμη περισσότερο τις χρηματοοικονομικές οντότητες και τους τρίτους παρόχους υπηρεσιών ΤΠΕ, με την ενίσχυση του επιπέδου ασφάλειας δικαίου όσον αφορά τη χρήση υπηρεσιών υπολογιστικού νέφους στον χρηματοοικονομικό τομέα, σε πλήρη εναρμόνιση με τις απαιτήσεις και τις προσδοκίες που προβλέπονται στη νομοθεσία της Ένωσης για τις χρηματοοικονομικές υπηρεσίες. Η ανάπτυξη τυποποιημένων συμβατικών ρητρών βασίζονται σε μέτρα που προβλέπονται ήδη στο σχέδιο δράσης του 2018 για τη χρηματοοικονομική τεχνολογία, στο πλαίσιο του οποίου ανακοινώθηκε η πρόθεση της Επιτροπής να ενθαρρύνει και να διευκολύνει την ανάπτυξη τυποποιημένων συμβατικών ρητρών για την εξωτερική ανάθεση σε πάροχο υπηρεσιών υπολογιστικού νέφους από τις χρηματοοικονομικές οντότητες, με βάση τις διατομεακές προσπάθειες των συμφεροντούχων στον τομέα του υπολογιστικού νέφους που έχουν ήδη διευκολυνθεί από την Επιτροπή με την εξασφάλιση της συμμετοχής του χρηματοοικονομικού τομέα.

(76) Με σκοπό την προώθηση της σύγκλισης και της αποτελεσματικότητας σε σχέση με τις εποπτικές προσεγγίσεις κατά την αντιμετώπιση κινδύνων τρίτων παρόχων ΤΠΕ στον χρηματοοικονομικό τομέα, καθώς και την ενίσχυση της ψηφιακής επιχειρησιακής ανθεκτικότητας των χρηματοοικονομικών οντοτήτων που βασίζονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ για την παροχή υπηρεσιών ΤΠΕ που υποστηρίζουν την παροχή χρηματοοικονομικών υπηρεσιών και, κατ' επέκταση, τη συμβολή στη διατήρηση της σταθερότητας του χρηματοοικονομικού συστήματος της Ένωσης και της ακεραιότητας της εσωτερικής αγοράς χρηματοοικονομικών υπηρεσιών, οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ θα πρέπει να υπόκεινται σε ενωσιακό πλαίσιο εποπτείας. Ενώ η θέσπιση του πλαισίου εποπτείας δικαιολογείται από την προστιθέμενη αξία της ανάληψης δράσης σε επίπεδο Ένωσης και λόγω του εγγενούς ρόλου και των ιδιαιτεροτήτων της

χρήσης υπηρεσιών ΤΠΕ στην παροχή χρηματοοικονομικών υπηρεσιών, θα πρέπει να υπενθυμιστεί ταυτόχρονα ότι η λύση αυτή φαίνεται κατάλληλη μόνο στο πλαίσιο του παρόντος κανονισμού που αφορά ειδικά την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα. Ωστόσο, το εν λόγω πλαίσιο εποπτείας δεν θα πρέπει να θεωρείται νέο μοντέλο ενωσιακής εποπτείας στους τομείς των χρηματοοικονομικών υπηρεσιών και δραστηριοτήτων.

(77) Το πλαίσιο εποπτείας θα πρέπει να εφαρμόζεται μόνο σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ. Ως εκ τούτου, θα πρέπει να υπάρχει ένας μηχανισμός ορισμού που θα λαμβάνει υπόψη τη διάσταση και τη φύση της εξάρτησης του χρηματοοικονομικού τομέα από τους εν λόγω τρίτους παρόχους υπηρεσιών ΤΠΕ. Ο εν λόγω μηχανισμός θα πρέπει να περιλαμβάνει ένα σύνολο ποσοτικών και ποιοτικών κριτηρίων για τον καθορισμό των παραμέτρων κρισιμότητας ως βάσης για την ένταξη στο πλαίσιο εποπτείας. Προκειμένου να διασφαλιστεί η ακρίβεια της εν λόγω αξιολόγησης, και ανεξάρτητα από την εταιρική δομή του τρίτου παρόχου υπηρεσιών ΤΠΕ, τα εν λόγω κριτήρια θα πρέπει, στην περίπτωση τρίτου παρόχου υπηρεσιών ΤΠΕ που ανήκει σε ευρύτερο όμιλο, να λαμβάνουν υπόψη ολόκληρη τη δομή του ομίλου του τρίτου παρόχου υπηρεσιών ΤΠΕ. Αφενός, οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που δεν ορίζονται αυτομάτως δυνάμει της εφαρμογής των εν λόγω κριτηρίων θα πρέπει να έχουν τη δυνατότητα προαιρετικής συμμετοχής στο πλαίσιο εποπτείας· αφετέρου, οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που υπόκεινται ήδη σε πλαίσια μηχανισμού εποπτείας προς υποστήριξη της εκτέλεσης των καθηκόντων του Ευρωπαϊκού Συστήματος Κεντρικών Τραπεζών με σκοπό την υποστήριξη των καθηκόντων, όπως αναφέρονται στο άρθρο 127 παράγραφος 2 ΣΛΕΕ, θα πρέπει να εξαιρούνται.

(78) Ομοίως, οι χρηματοοικονομικές οντότητες που παρέχουν υπηρεσίες ΤΠΕ σε άλλες χρηματοοικονομικές οντότητες, μολονότι ανήκουν στην κατηγορία των τρίτων παρόχων υπηρεσιών ΤΠΕ βάσει του παρόντος κανονισμού, θα πρέπει επίσης να εξαιρούνται από το πλαίσιο εποπτείας, δεδομένου ότι υπόκεινται ήδη σε εποπτικούς μηχανισμούς που θεσπίζονται από το σχετικό ενωσιακό δίκαιο για τις χρηματοοικονομικές υπηρεσίες. Κατά περίπτωση, οι αρμόδιες αρχές θα πρέπει να λαμβάνουν υπόψη, στο πλαίσιο των εποπτικών δραστηριοτήτων τους, τους κινδύνους ΤΠΕ που εγκυμονούν για τις χρηματοοικονομικές οντότητες οι χρηματοοικονομικές οντότητες που παρέχουν υπηρεσίες ΤΠΕ. Ομοίως, λόγω των υφιστάμενων μηχανισμών παρακολούθησης κινδύνων σε επίπεδο ομίλου, θα πρέπει να θεσπιστεί η ίδια εξαίρεση για τους τρίτους παρόχους υπηρεσιών ΤΠΕ που παρέχουν υπηρεσίες κυρίως στις οντότητες του δικού τους ομίλου. Οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που παρέχουν υπηρεσίες ΤΠΕ αποκλειστικά σε ένα κράτος μέλος σε χρηματοοικονομικές οντότητες οι οποίες δραστηριοποιούνται μόνο στο εν λόγω κράτος μέλος θα πρέπει επίσης να εξαιρούνται από τον μηχανισμό ορισμού, λόγω των περιορισμένων δραστηριοτήτων τους και της έλλειψης διασυνοριακού αντικτύπου.

(79) Ο ψηφιακός μετασχηματισμός στον τομέα των χρηματοοικονομικών υπηρεσιών έχει οδηγήσει σε πρωτοφανές επίπεδο χρήσης υπηρεσιών ΤΠΕ και εξάρτησης από αυτές. Δεδομένου ότι έχει καταστεί αδιανόητο να παρέχονται χρηματοοικονομικές υπηρεσίες χωρίς τη χρήση υπηρεσιών υπολογιστικού νέφους, λύσεων λογισμικού και υπηρεσιών που σχετίζονται με δεδομένα, το χρηματοοικονομικό οικοσύστημα της Ένωσης εξαρτάται πλέον εγγενώς και από ορισμένες υπηρεσίες ΤΠΕ που παρέχονται από παρόχους υπηρεσιών ΤΠΕ. Ορισμένοι από αυτούς τους προμηθευτές, φορείς καινοτομίας στην ανάπτυξη και εφαρμογή τεχνολογιών που βασίζονται στις ΤΠΕ, διαδραματίζουν σημαντικό ρόλο στην παροχή χρηματοοικονομικών υπηρεσιών ή έχουν ενσωματωθεί στην αλυσίδα αξίας των χρηματοοικονομικών υπηρεσιών. Ως εκ τούτου, έχουν καταστεί ζωτικής σημασίας για τη σταθερότητα και την ακεραιότητα του χρηματοοικονομικού συστήματος της Ένωσης. Αυτή η ευρεία εξάρτηση από υπηρεσίες που παρέχονται από κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, σε συνδυασμό με την αλληλεξάρτηση των συστημάτων πληροφοριών διαφόρων φορέων της αγοράς, δημιουργεί άμεσο και δυνητικά σοβαρό κίνδυνο για το σύστημα χρηματοοικονομικών υπηρεσιών της Ένωσης και για τη συνέχεια της παροχής χρηματοοικονομικών υπηρεσιών σε περίπτωση που κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ επηρεαστούν από λειτουργικές διαταραχές ή μείζονα κυβερνοπεριστατικά. Τα κυβερνοπεριστατικά έχουν ιδιαίτερη ικανότητα να πολλαπλασιάζονται και να διαδίδονται σε ολόκληρο το χρηματοοικονομικό σύστημα με σημαντικά ταχύτερο ρυθμό από ό,τι άλλα είδη κινδύνου που παρακολουθούνται στον χρηματοοικονομικό τομέα και μπορούν να επεκταθούν σε διάφορους τομείς και πέραν των γεωγραφικών συνόρων. Έχουν τη δυνατότητα να εξελιχθούν σε συστημική κρίση, όπου η εμπιστοσύνη στο χρηματοοικονομικό σύστημα έχει διαβρωθεί λόγω της διαταραχής των λειτουργιών που στηρίζουν την πραγματική οικονομία, ή λόγω σημαντικών οικονομικών ζημιών, που φθάνουν σε επίπεδο κατά το οποίο το χρηματοοικονομικό σύστημα δεν είναι σε θέση να αντεπεξέλθει ή που απαιτεί την υλοποίηση αυστηρών μέτρων απορρόφησης των κραδασμών. Για να αποτραπεί η υλοποίηση αυτών των σεναρίων, πράγμα το οποίο θα έθετε σε κίνδυνο τη χρηματοοικονομική σταθερότητα και την ακεραιότητα της Ένωσης, είναι σημαντικό να εξασφαλιστεί η σύγκλιση των εποπτικών πρακτικών σχετικά με τους κινδύνους τρίτων μερών ΤΠΕ στον χρηματοοικονομικό τομέα, ιδίως μέσω νέων κανόνων που θα επιτρέπουν την ενωσιακή εποπτεία κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ.

(80) Το πλαίσιο εποπτείας εξαρτάται σε μεγάλο βαθμό από τον βαθμό συνεργασίας μεταξύ του κύριου εποπτικού φορέα και του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ που παρέχει σε χρηματοοικονομικές οντότητες υπηρεσίες που επηρεάζουν την παροχή χρηματοοικονομικών υπηρεσιών. Η επιτυχής εποπτεία βασίζεται, μεταξύ άλλων, στην ικανότητα του κύριου εποπτικού φορέα να διενεργεί αποτελεσματικά αποστολές παρακολούθησης και επιθεωρήσεις για την αξιολόγηση των κανόνων, των δικλείδων ασφάλειας και των διαδικασιών που χρησιμοποιούνται από τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, καθώς και για την αξιολόγηση του δυνητικού σωρευτικού αντικτύπου των δραστηριοτήτων τους στη χρηματοοικονομική σταθερότητα και την ακεραιότητα του χρηματοοικονομικού συστήματος. Ταυτόχρονα, είναι ζωτικής σημασίας οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ να ακολουθούν τις συστάσεις του κύριου εποπτικού φορέα και να αντιμετωπίζουν τους προβληματισμούς του. Δεδομένου ότι η έλλειψη συνεργασίας από κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ που παρέχει υπηρεσίες οι οποίες επηρεάζουν την παροχή χρηματοοικονομικών υπηρεσιών, όπως η άρνηση χορήγησης πρόσβασης στις εγκαταστάσεις του ή υποβολής πληροφοριών, θα στερούσε τελικά τον κύριο εποπτικό φορέα από τα βασικά εργαλεία του για την αξιολόγηση κινδύνου ΤΠΕ τρίτων και θα μπορούσε να επηρεάσει αρνητικά τη χρηματοοικονομική σταθερότητα και την ακεραιότητα του χρηματοοικονομικού συστήματος, είναι επίσης αναγκαίο να προβλεφθεί ανάλογο καθεστώς κυρώσεων.

(81) Στο πλαίσιο αυτό, η ανάγκη του κύριου εποπτικού φορέα να επιβάλει χρηματικές ποινές για να υποχρεώσει τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ να συμμορφώνονται με τις υποχρεώσεις διαφάνειας και πρόσβασης που ορίζονται στον παρόντα κανονισμό δεν θα πρέπει να υπονομεύεται από τις δυσκολίες οι οποίες ανακύπτουν από την επιβολή των εν λόγω χρηματικών ποινών σε σχέση με κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ που είναι εγκατεστημένοι σε τρίτες χώρες. Προκειμένου να διασφαλιστεί η εκτελεστότητα των εν λόγω ποινών και να καταστεί δυνατή η ταχεία εφαρμογή των διαδικασιών που διαφυλάσσουν τα κρίσιμα δικαιώματα υπεράσπισης των τρίτων παρόχων υπηρεσιών ΤΠΕ στο πλαίσιο του μηχανισμού ορισμού και της έκδοσης συστάσεων, θα πρέπει να απαιτείται από τους εν λόγω κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, οι οποίοι παρέχουν υπηρεσίες σε χρηματοοικονομικές οντότητες υπηρεσίες που επηρεάζουν την παροχή χρηματοοικονομικών υπηρεσιών, να διατηρούν επαρκή επιχειρηματική παρουσία στην Ένωση. Λόγω της φύσης της εποπτείας και της απουσίας συγκρίσιμων ρυθμίσεων σε άλλες δικαιοδοσίες, δεν υπάρχουν κατάλληλοι εναλλακτικοί μηχανισμοί που να διασφαλίζουν αυτόν τον στόχο μέσω της αποτελεσματικής συνεργασίας με τις αρχές χρηματοοικονομικής εποπτείας σε τρίτες χώρες σε σχέση με την παρακολούθηση του αντικτύπου των ψηφιακών λειτουργικών κινδύνων που εγκυμονούν οι συστημικοί τρίτοι πάροχοι υπηρεσιών ΤΠΕ, οι οποίοι χαρακτηρίζονται κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που είναι εγκατεστημένοι σε τρίτες χώρες. Ως εκ τούτου, προκειμένου να συνεχίσει την παροχή υπηρεσιών ΤΠΕ σε χρηματοοικονομικές οντότητες στην Ένωση, τρίτος πάροχος υπηρεσιών ΤΠΕ που είναι εγκατεστημένος σε τρίτη χώρα και έχει οριστεί ως κρίσιμος σύμφωνα με τον παρόντα κανονισμό θα πρέπει να προβεί, εντός 12 μηνών από τον εν λόγω ορισμό, σε όλες τις αναγκαίες ρυθμίσεις για να διασφαλίσει την ενσωμάτωσή του στην Ένωση, μέσω της σύστασης θυγατρικής, όπως ορίζεται σε ολόκληρο το κεκτημένο της Ένωσης, και συγκεκριμένα στην οδηγία 2013/34/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([21]).

(82) Η απαίτηση σύστασης θυγατρικής στην Ένωση δεν θα πρέπει να εμποδίζει τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ να παρέχει υπηρεσίες ΤΠΕ και σχετική τεχνική υποστήριξη από εγκαταστάσεις και υποδομές που βρίσκονται εκτός της Ένωσης. Ο παρών κανονισμός δεν επιβάλλει υποχρέωση γεωγραφικού περιορισμού δεδομένων, καθώς δεν απαιτεί αποθήκευση ή επεξεργασία δεδομένων στην Ένωση.

(83) Οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ θα πρέπει να είναι σε θέση να παρέχουν υπηρεσίες ΤΠΕ από οπουδήποτε στον κόσμο και όχι απαραίτητα ή όχι μόνο από εγκαταστάσεις που βρίσκονται στην Ένωση. Οι δραστηριότητες εποπτείας θα πρέπει πρώτα να διεξάγονται σε εγκαταστάσεις που βρίσκονται στην Ένωση και να αλληλεπιδρούν με οντότητες που βρίσκονται στην Ένωση, συμπεριλαμβανομένων των θυγατρικών που έχουν συσταθεί από κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ σύμφωνα με τον παρόντα κανονισμό. Ωστόσο, οι εν λόγω δράσεις εντός της Ένωσης ενδέχεται να μην επαρκούν για να επιτρέψουν στον κύριο εποπτικό φορέα να εκτελέσει πλήρως και αποτελεσματικά τα καθήκοντά του δυνάμει του παρόντος κανονισμού. Ως εκ τούτου, ο κύριος εποπτικός φορέας θα πρέπει επίσης να είναι σε θέση να ασκεί τις σχετικές εποπτικές εξουσίες του σε τρίτες χώρες. Η άσκηση των εν λόγω εξουσιών σε τρίτες χώρες θα πρέπει να επιτρέπει στον κύριο εποπτικό φορέα να εξετάζει τις εγκαταστάσεις από τις οποίες όντως παρέχονται ή αποτελούν αντικείμενο διαχείρισης οι υπηρεσίες ΤΠΕ ή οι υπηρεσίες τεχνικής υποστήριξης από τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ και θα πρέπει να επιτρέπει στον κύριο εποπτικό φορέα ολοκληρωμένη και επιχειρησιακή κατανόηση της διαχείρισης κινδύνων ΤΠΕ του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ. Η δυνατότητα του κύριου εποπτικού φορέα, ως οργανισμού της Ένωσης, να ασκεί εξουσίες εκτός της επικράτειας της Ένωσης θα πρέπει να πλαισιώνεται δεόντως από σχετικούς όρους, ιδίως από τη συγκατάθεση του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ. Ομοίως, οι αρμόδιες αρχές της τρίτης χώρας θα πρέπει να ενημερώνονται για την άσκηση των δραστηριοτήτων του κύριου εποπτικού φορέα στο έδαφός τους και να μην έχουν προβάλει σχετική αντίρρηση. Ωστόσο, προκειμένου να διασφαλιστεί η αποτελεσματική εφαρμογή, και με την επιφύλαξη των αντίστοιχων αρμοδιοτήτων των θεσμικών οργάνων και των κρατών μελών της Ένωσης, οι εξουσίες αυτές

([21]) Οδηγία 2013/34/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με τις ετήσιες οικονομικές καταστάσεις, τις ενοποιημένες οικονομικές καταστάσεις και συναφείς εκθέσεις επιχειρήσεων ορισμένων μορφών, την τροποποίηση της οδηγίας 2006/43/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και την κατάργηση των οδηγιών 78/660/ΕΟΚ και 83/349/ΕΟΚ του Συμβουλίου (ΕΕ L 182 της 29.6.2013, σ. 19).

είναι ανάγκη επίσης να βασίζονται πλήρως στη σύναψη ρυθμίσεων διοικητικής συνεργασίας με τις σχετικές αρχές της οικείας τρίτης χώρας. Ως εκ τούτου, ο παρών κανονισμός θα πρέπει να επιτρέπει στις ΕΕΑ να συνάπτουν ρυθμίσεις διοικητικής συνεργασίας με τις αρμόδιες αρχές τρίτων χωρών, οι οποίες δεν θα πρέπει διαφορετικά να δημιουργούν νομικές υποχρεώσεις έναντι της Ένωσης και των κρατών μελών της.

(84) Για τη διευκόλυνση της επικοινωνίας με τον κύριο εποπτικό φορέα και για τη διασφάλιση επαρκούς εκπροσώπησης, οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που αποτελούν μέρος ομίλου θα πρέπει να ορίζουν ένα νομικό πρόσωπο ως σημείο συντονισμού τους.

(85) Το πλαίσιο εποπτείας δεν θα πρέπει να θίγει την αρμοδιότητα των κρατών μελών να πραγματοποιούν δικές τους αποστολές εποπτείας ή παρακολούθησης όσον αφορά τρίτους παρόχους υπηρεσιών ΤΠΕ οι οποίοι δεν έχουν οριστεί ως κρίσιμοι βάσει του παρόντος κανονισμού αλλά θα μπορούσαν να θεωρηθούν σημαντικοί σε εθνικό επίπεδο.

(86) Για την αξιοποίηση της πολυεπίπεδης θεσμικής αρχιτεκτονικής στον τομέα των χρηματοοικονομικών υπηρεσιών, η μεικτή επιτροπή των ΕΕΑ θα πρέπει να συνεχίσει να διασφαλίζει τον συνολικό διατομεακό συντονισμό σε σχέση με όλα τα θέματα που αφορούν τους κινδύνους ΤΠΕ, σύμφωνα με τα καθήκοντά της για την κυβερνοασφάλεια. Θα πρέπει να υποστηρίζεται από νέα υποεπιτροπή («φόρουμ εποπτείας») που εκτελεί τις προπαρασκευαστικές εργασίες τόσο για τις μεμονωμένες αποφάσεις που απευθύνονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, όσο και για την έκδοση συλλογικών συστάσεων, ιδίως σχετικά με τη συγκριτική αξιολόγηση των προγραμμάτων εποπτείας κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ και τον προσδιορισμό βέλτιστων πρακτικών για την αντιμετώπιση ζητημάτων κινδύνου συγκέντρωσης ΤΠΕ.

(87) Προκειμένου να διασφαλιστεί η κατάλληλη και αποτελεσματική εποπτεία των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ σε ενωσιακό επίπεδο, ο παρών κανονισμός προβλέπει ότι οποιαδήποτε από τις τρεις ΕΕΑ θα μπορούσε να οριστεί ως κύριος εποπτικός φορέας. Η ατομική ανάθεση ενός κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ σε μία από τις τρεις ΕΕΑ θα πρέπει να προκύπτει από αξιολόγηση της κυριαρχίας των χρηματοοικονομικών οντοτήτων που δραστηριοποιούνται στους χρηματοοικονομικούς τομείς για τους οποίους η ΕΕΑ έχει αρμοδιότητες. Η προσέγγιση αυτή θα πρέπει να οδηγήσει σε ισόρροπη κατανομή καθηκόντων και αρμοδιοτήτων μεταξύ των τριών ΕΕΑ, στο πλαίσιο της άσκησης των λειτουργιών εποπτείας, και θα πρέπει να αξιοποιεί με τον καλύτερο δυνατό τρόπο τους ανθρώπινους πόρους και την τεχνική εμπειρογνωσία που διαθέτει καθεμία από τις τρεις ΕΕΑ.

(88) Θα πρέπει να χορηγηθούν στους κύριους εποπτικούς φορείς οι απαραίτητες εξουσίες για τη διεξαγωγή ερευνών, τη διενέργεια επιτόπιων και εξ αποστάσεως επιθεωρήσεων στις εγκαταστάσεις και τοποθεσίες κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ και την απόκτηση πλήρων και επικαιροποιημένων πληροφοριών. Οι εν λόγω εξουσίες θα πρέπει να επιτρέπουν στον κύριο εποπτικό φορέα να αποκτήσει πραγματική εικόνα ως προς το είδος, τη διάσταση και τον αντίκτυπο των κινδύνων τρίτων παρόχων ΤΠΕ για τις χρηματοοικονομικές οντότητες και, εντέλει, για το χρηματοοικονομικό σύστημα της Ένωσης. Η ανάθεση στις ΕΕΑ του κύριου εποπτικού ρόλου συνιστά προϋπόθεση για την κατανόηση και την αντιμετώπιση της συστημικής διάστασης των κινδύνων ΤΠΕ στον χρηματοοικονομικό τομέα. Ο αντίκτυπος των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ στον χρηματοοικονομικό τομέα της Ένωσης και τα πιθανά ζητήματα που προκαλούνται από τον συνεπαγόμενο κίνδυνο συγκέντρωσης ΤΠΕ απαιτούν την υιοθέτηση συλλογικής προσέγγισης σε επίπεδο Ένωσης. Η ταυτόχρονη άσκηση πολλαπλών δικαιωμάτων ελέγχων και πρόσβασης, χωριστά από πολλές αρμόδιες αρχές, με ελάχιστο ή μηδενικό συντονισμό μεταξύ τους, θα εμπόδιζε τις χρηματοοικονομικές εποπτικές αρχές να αποκτήσουν πλήρη και ολοκληρωμένη επισκόπηση των κινδύνων τρίτων μερών ΤΠΕ στην Ένωση, ενώ παράλληλα θα δημιουργούσε πλεονασμό, επιβάρυνση και πολυπλοκότητα για τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, εάν υπόκειντο σε πολυάριθμα αιτήματα παρακολούθησης και επιθεώρησης.

(89) Λόγω του σημαντικού αντικτύπου του ορισμού τους ως κρίσιμων, ο παρών κανονισμός θα πρέπει να διασφαλίζει ότι τα δικαιώματα των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ τηρούνται καθ' όλη τη διάρκεια εφαρμογής του πλαισίου εποπτείας. Πριν από τον ορισμό τους ως κρίσιμων, οι εν λόγω πάροχοι θα πρέπει, για παράδειγμα, να έχουν το δικαίωμα να υποβάλλουν στον κύριο εποπτικό φορέα αιτιολογημένη δήλωση που περιέχει κάθε σχετική πληροφορία για τους σκοπούς της αξιολόγησης που σχετίζεται με τον χαρακτηρισμό τους. Δεδομένου ότι ο κύριος εποπτικός φορέας θα πρέπει να εξουσιοδοτηθεί να υποβάλλει συστάσεις σχετικά με θέματα κινδύνων ΤΠΕ και κατάλληλα σχετικά διορθωτικά μέτρα, τα οποία περιλαμβάνουν την εξουσία εναντίωσης σε ορισμένες συμβατικές ρυθμίσεις που έχουν εντέλει αντίκτυπο στη σταθερότητα της χρηματοοικονομικής οντότητας ή του χρηματοοικονομικού συστήματος, οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ θα πρέπει επίσης να έχουν τη δυνατότητα να παρέχουν, πριν από την οριστικοποίηση των εν λόγω συστάσεων, εξηγήσεις σχετικά με τον αναμενόμενο αντίκτυπο των λύσεων που προβλέπονται στις συστάσεις σε πελάτες που είναι οντότητες οι οποίες δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού, καθώς και να διατυπώνουν λύσεις

για τον μετριασμό των κινδύνων. Οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που διαφωνούν με τις συστάσεις θα πρέπει να υποβάλουν αιτιολογημένη εξήγηση της πρόθεσής τους να μην εγκρίνουν τη σύσταση. Όταν η εν λόγω αιτιολογημένη εξήγηση δεν υποβάλλεται ή όταν κρίνεται ανεπαρκής, ο κύριος εποπτικός φορέας θα πρέπει να εκδίδει δημόσια ανακοίνωση στην οποία θα περιγράφεται συνοπτικά το ζήτημα της μη συμμόρφωσης.

(90) Οι αρμόδιες αρχές θα πρέπει να συμπεριλάβουν δεόντως το καθήκον της επαλήθευσης της ουσιαστικής συμμόρφωσης με τις συστάσεις που εκδίδει ο κύριος εποπτικός φορέας στα καθήκοντά τους όσον αφορά την προληπτική εποπτεία των χρηματοοικονομικών οντοτήτων. Οι αρμόδιες αρχές θα πρέπει να είναι σε θέση να απαιτούν από τις χρηματοοικονομικές οντότητες να λαμβάνουν πρόσθετα μέτρα για την αντιμετώπιση των κινδύνων που προσδιορίζονται στις συστάσεις του κύριου εποπτικού φορέα και θα πρέπει, σε εύθετο χρόνο, να εκδίδουν σχετικές κοινοποιήσεις. Όταν ο κύριος εποπτικός φορέας απευθύνει συστάσεις σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ που εποπτεύονται βάσει της οδηγίας (ΕΕ) 2022/2555 οι αρμόδιες αρχές θα πρέπει να μπορούν, σε προαιρετική βάση, και πριν από τη θέσπιση πρόσθετων μέτρων, να διαβουλεύονται με τις αρμόδιες αρχές βάσει της εν λόγω οδηγίας για την προώθηση συντονισμένης προσέγγισης όσον αφορά τους εν λόγω κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ.

(91) Η άσκηση της εποπτείας θα πρέπει να καθοδηγείται από τρεις επιχειρησιακές αρχές που αποσκοπούν στη διασφάλιση: α) στενής συνεργασίας μεταξύ των ΕΕΑ όσον αφορά τους κύριους εποπτικούς ρόλους τους, μέσω κοινού δικτύου εποπτείας (ΔΚΕ), β) συνέπειας με το πλαίσιο που θεσπίστηκε με την οδηγία (ΕΕ) 2022/2555 (μέσω προαιρετικής διαβούλευσης με οργανισμούς βάσει της εν λόγω οδηγίας για την αποφυγή επικάλυψης μέτρων τα οποία απευθύνονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ) και γ) επίδειξης επιμέλειας για την ελαχιστοποίηση του δυνητικού κινδύνου διαταραχής των υπηρεσιών οι οποίες παρέχονται από κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ σε πελάτες που είναι οντότητες μη εμπίπτουσες στο πεδίο εφαρμογής του παρόντος κανονισμού.

(92) Το πλαίσιο εποπτείας δεν θα πρέπει να αντικαθιστά ούτε να υποκαθιστά καθ' οιονδήποτε τρόπο και για κανένα μέρος την απαίτηση της διαχείρισης, από τις χρηματοοικονομικές οντότητες, των κινδύνων που συνεπάγεται η χρήση τρίτων παρόχων υπηρεσιών ΤΠΕ, συμπεριλαμβανομένης της υποχρέωσής τους να διατηρούν συνεχή παρακολούθηση συμβατικών ρυθμίσεων που συνάπτονται με κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ. Ομοίως, το πλαίσιο εποπτείας δεν θα πρέπει να επηρεάζει την πλήρη ευθύνη των χρηματοοικονομικών οντοτήτων όσον αφορά τη συμμόρφωσή τους με όλες τις νομικές υποχρεώσεις που περιλαμβάνονται στον παρόντα κανονισμό και στο σχετικό δίκαιο για τις χρηματοοικονομικές υπηρεσίες, καθώς και την εκπλήρωση αυτών.

(93) Για την αποφυγή επαναλήψεων και αλληλεπικαλύψεων, οι αρμόδιες αρχές θα πρέπει να αποφεύγουν τη λήψη μεμονωμένων μέτρων που αποσκοπούν στην παρακολούθηση των κινδύνων κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ και θα πρέπει, εν προκειμένω, να βασίζονται στη σχετική αξιολόγηση του κύριου εποπτικού φορέα. Όλα τα μέτρα θα πρέπει σε κάθε περίπτωση να συντονίζονται και να συμφωνούνται εκ των προτέρων με τον κύριο εποπτικό φορέα στο πλαίσιο της άσκησης των καθηκόντων του πλαισίου εποπτείας.

(94) Για την προώθηση της σύγκλισης σε διεθνές επίπεδο όσον αφορά τη χρήση βέλτιστων πρακτικών κατά την επανεξέταση και την παρακολούθηση της διαχείρισης ψηφιακών κινδύνων από τρίτους παρόχους υπηρεσιών ΤΠΕ, οι ΕΕΑ θα πρέπει να ενθαρρύνονται να συνάπτουν ρυθμίσεις συνεργασίας με τις αρμόδιες εποπτικές και ρυθμιστικές αρχές τρίτων χωρών.

(95) Για την αξιοποίηση των συγκεκριμένων αρμοδιοτήτων, των τεχνικών δεξιοτήτων και της εμπειρογνωσίας του προσωπικού που ειδικεύεται στους επιχειρησιακούς κινδύνους και κινδύνους ΤΠΕ στους κόλπους των αρμόδιων αρχών, των τριών ΕΑΑ και, σε προαιρετική βάση, των αρμόδιων αρχών δυνάμει της οδηγίας (ΕΕ) 2022/2555 ο κύριος εποπτικός φορέας θα πρέπει να αξιοποιεί τις εθνικές εποπτικές ικανότητες και γνώσεις και να συγκροτεί ειδικές εξεταστικές ομάδες για κάθε κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ, συγκεντρώνοντας διεπιστημονικές ομάδες για την υποστήριξη της προετοιμασίας και της εκτέλεσης των δραστηριοτήτων εποπτείας, συμπεριλαμβανομένων των γενικών ερευνών και επιθεωρήσεων κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ, καθώς και για οποιαδήποτε αναγκαία παρακολούθησή τους.

(96) Ενώ οι δαπάνες που προκύπτουν από τα καθήκοντα εποπτείας θα χρηματοδοτούνται πλήρως από τέλη που επιβάλλονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, οι ΕΕΑ είναι, ωστόσο, πιθανό να επιβαρυνθούν, πριν από την έναρξη του πλαισίου εποπτείας, με δαπάνες για την εφαρμογή ειδικών συστημάτων ΤΠΕ που υποστηρίζουν την επικείμενη εποπτεία, δεδομένου ότι θα πρέπει να αναπτυχθούν και να εφαρμοστούν εκ των προτέρων ειδικά συστήματα ΤΠΕ. Ως εκ τούτου, ο παρών κανονισμός προβλέπει ένα μοντέλο υβριδικής χρηματοδότησης, βάσει του οποίου το πλαίσιο εποπτείας θα χρηματοδοτείται πλήρως από τέλη, ενώ η ανάπτυξη των συστημάτων ΤΠΕ των ΕΕΑ θα χρηματοδοτείται από συνεισφορές της Ένωσης και των εθνικών αρμόδιων αρχών.

(97) Οι αρμόδιες αρχές θα πρέπει να διαθέτουν όλες τις απαιτούμενες εξουσίες εποπτείας, έρευνας και επιβολής κυρώσεων που είναι απαραίτητες για τη διασφάλιση της ορθής άσκησης των καθηκόντων τους δυνάμει του παρόντος κανονισμού. Θα πρέπει, καταρχήν, να δημοσιεύουν ανακοινώσεις σχετικά με τις διοικητικές κυρώσεις που επιβάλλουν. Δεδομένου ότι οι χρηματοοικονομικές οντότητες και οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ μπορούν να είναι εγκατεστημένοι σε διαφορετικά κράτη μέλη και να τελούν υπό την εποπτεία διαφορετικών αρμόδιων αρχών, η εφαρμογή του παρόντος κανονισμού θα πρέπει να διευκολύνεται, αφενός, από τη στενή συνεργασία μεταξύ των σχετικών αρμόδιων αρχών, συμπεριλαμβανομένης της ΕΚΤ όσον αφορά συγκεκριμένα καθήκοντα που της ανατίθενται βάσει του κανονισμού (ΕΕ) αριθ. 1024/2013 του Συμβουλίου, και, αφετέρου, από τη διαβούλευση με τις ΕΕΑ μέσω της αμοιβαίας ανταλλαγής πληροφοριών και της παροχής συνδρομής στο πλαίσιο των σχετικών εποπτικών δραστηριοτήτων.

(98) Για τον περαιτέρω ποσοτικό και ποιοτικό προσδιορισμό των κριτηρίων για τον ορισμό τρίτων παρόχων υπηρεσιών ΤΠΕ ως κρίσιμων και για την εναρμόνιση των τελών εποπτείας, θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία να εκδίδει πράξεις, σύμφωνα με το άρθρο 290 ΣΛΕΕ για τη συμπλήρωση του παρόντος κανονισμού, προσδιορίζοντας περαιτέρω τις συστημικές επιπτώσεις που θα μπορούσε να έχει η αθέτηση υποχρεώσεων ή η διακοπή λειτουργίας τρίτου παρόχου υπηρεσιών ΤΠΕ στις χρηματοοικονομικές οντότητες στις οποίες παρέχει υπηρεσίες ΤΠΕ, τον αριθμό των παγκόσμιων συστημικώς σημαντικών ιδρυμάτων (G-SII) ή άλλων συστημικώς σημαντικών ιδρυμάτων (O-SII) που βασίζονται στον αντίστοιχο τρίτο πάροχο υπηρεσιών ΤΠΕ, τον αριθμό των τρίτων παρόχων υπηρεσιών ΤΠΕ που δραστηριοποιούνται σε συγκεκριμένη αγορά, το κόστος μετάβασης δεδομένων και φόρτου εργασίας ΤΠΕ σε άλλον τρίτο πάροχο υπηρεσιών ΤΠΕ, καθώς και το ύψος των τελών εποπτείας και τον τρόπο με τον οποίο πρέπει να καταβάλλονται. Είναι ιδιαίτερα σημαντικό η Επιτροπή να διεξάγει, κατά τις προπαρασκευαστικές της εργασίες, τις κατάλληλες διαβουλεύσεις, μεταξύ άλλων σε επίπεδο εμπειρογνωμόνων, οι οποίες να πραγματοποιούνται σύμφωνα με τις αρχές που ορίζονται στη διοργανική συμφωνία της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου ([22]). Πιο συγκεκριμένα, προκειμένου να διασφαλιστεί η ίση συμμετοχή στην προετοιμασία των κατ' εξουσιοδότηση πράξεων, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο θα πρέπει να λαμβάνουν όλα τα έγγραφα κατά τον ίδιο χρόνο με τους εμπειρογνώμονες των κρατών μελών, και οι εμπειρογνώμονές τους θα πρέπει να έχουν συστηματικά πρόσβαση στις συνεδριάσεις των ομάδων εμπειρογνωμόνων της Επιτροπής που ασχολούνται με την προετοιμασία κατ' εξουσιοδότηση πράξεων.

(99) Η συνεκτική εναρμόνιση των απαιτήσεων που καθορίζονται στον παρόντα κανονισμό θα πρέπει να διασφαλίζεται με ρυθμιστικά τεχνικά πρότυπα. Σύμφωνα με τους ρόλους τους ως φορείς που διαθέτουν υψηλό επίπεδο εμπειρογνωσίας, οι ΕΑΑ θα πρέπει να αναπτύσσουν ρυθμιστικά τεχνικά πρότυπα που δεν συνεπάγονται επιλογές πολιτικής και τα οποία πρέπει να υποβάλλονται στην Επιτροπή. Θα πρέπει να αναπτυχθούν ρυθμιστικά τεχνικά πρότυπα στους τομείς της διαχείρισης κινδύνων ΤΠΕ, της αναφοράς μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ, των δοκιμών, καθώς και σε σχέση με βασικές απαιτήσεις για την ορθή παρακολούθηση των κινδύνων τρίτων παρόχων ΤΠΕ. Η Επιτροπή και οι ΕΕΑ θα πρέπει να διασφαλίζουν ότι τα εν λόγω πρότυπα και απαιτήσεις μπορούν να εφαρμόζονται από όλες τις χρηματοοικονομικές οντότητες κατά τρόπο ανάλογο προς το μέγεθος και το συνολικό προφίλ κινδύνου τους και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών τους. Θα πρέπει επίσης να ανατεθεί στην Επιτροπή η εξουσία να εγκρίνει τα εν λόγω ρυθμιστικά τεχνικά πρότυπα μέσω κατ' εξουσιοδότηση πράξεων δυνάμει του άρθρου 290 ΣΛΕΕ και σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

(100) Προκειμένου να διευκολυνθεί η συγκρισιμότητα των αναφορών μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ και μειζόνων λειτουργικών συμβάντων ή συμβάντων ασφάλειας που σχετίζονται με πληρωμές, καθώς και να διασφαλιστεί η διαφάνεια όσον αφορά τις συμβατικές ρυθμίσεις για τη χρήση των υπηρεσιών ΤΠΕ που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ, οι ΕΕΑ θα πρέπει να αναπτύσσουν σχέδια εκτελεστικών τεχνικών προτύπων για την κατάρτιση τυποποιημένων υποδειγμάτων, εντύπων και διαδικασιών, ώστε οι χρηματοοικονομικές οντότητες να είναι σε θέση να αναφέρουν μείζον συμβάν που σχετίζεται με τις ΤΠΕ και μείζον λειτουργικό συμβάν ή συμβάν ασφάλειας που σχετίζεται με πληρωμές, καθώς και τυποποιημένων υποδειγμάτων για το μητρώο πληροφοριών. Κατά την ανάπτυξη των εν λόγω προτύπων, οι ΕΕΑ θα πρέπει να λαμβάνουν υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου της χρηματοοικονομικής οντότητας και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της. Θα πρέπει επίσης να ανατεθεί στην Επιτροπή η εξουσία να εγκρίνει τα εν λόγω εκτελεστικά τεχνικά πρότυπα μέσω εκτελεστικών πράξεων δυνάμει του άρθρου 291 ΣΛΕΕ και του άρθρου 15 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

([22]) ΕΕ L 123 της 12.5.2016, σ. 1.

(101) Δεδομένου ότι έχουν ήδη καθοριστεί περαιτέρω απαιτήσεις μέσω κατ' εξουσιοδότηση και εκτελεστικών πράξεων βάσει ρυθμιστικών και εκτελεστικών τεχνικών προτύπων που περιλαμβάνονται στους κανονισμούς (ΕΚ) αριθ. 1060/2009 ([23]), (ΕΕ) αριθ. 648/2012 ([24]), (ΕΕ) αριθ. 600/2014 ([25]) και (ΕΕ) αριθ. 909/2014 ([26]) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, είναι σκόπιμο να ανατεθεί στις ΕΕΑ η εντολή, είτε μεμονωμένα είτε από κοινού μέσω της μεικτής επιτροπής, να υποβάλλουν ρυθμιστικά και εκτελεστικά τεχνικά πρότυπα στην Επιτροπή για την έκδοση κατ' εξουσιοδότηση και εκτελεστικών πράξεων με τις οποίες θα μεταφέρονται και θα επικαιροποιούνται οι υφιστάμενοι κανόνες διαχείρισης κινδύνων ΤΠΕ.

(102) Δεδομένου ότι ο παρών κανονισμός, σε συνδυασμό με την οδηγία (ΕΕ) 2022/2556 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([27]), συνεπάγεται την ενοποίηση των διατάξεων διαχείρισης κινδύνων ΤΠΕ που περιλαμβάνονται σε μεγάλο αριθμό κανονισμών και οδηγιών του κεκτημένου της Ένωσης στον τομέα των χρηματοοικονομικών υπηρεσιών, συμπεριλαμβανομένων των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και (ΕΕ) αριθ. 909/2014 και του κανονισμού (ΕΕ) 2016/1011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([28]), και για τους σκοπούς της διασφάλισης πλήρους διαφάνειας, οι εν λόγω κανονισμοί θα πρέπει να τροποποιηθούν ώστε να αποσαφηνιστεί ότι οι εφαρμοστέες διατάξεις που σχετίζονται με τους κινδύνους ΤΠΕ καθορίζονται στον παρόντα κανονισμό.

(103) Κατά συνέπεια, το πεδίο εφαρμογής των σχετικών άρθρων που αφορούν τον λειτουργικό κίνδυνο, βάσει των οποίων ασκήθηκαν οι εξουσιοδοτήσεις που προβλέπονται στους κανονισμούς (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 για την ανάθεση της εντολής έκδοσης κατ' εξουσιοδότηση και εκτελεστικών πράξεων, θα πρέπει να περιοριστεί ενόψει της μεταφοράς στον παρόντα κανονισμό όλων των διατάξεων που καλύπτουν τις πτυχές της ψηφιακής επιχειρησιακής ανθεκτικότητας και αποτελούν σήμερα μέρος των εν λόγω κανονισμών.

(104) Ο δυνητικός συστημικός κίνδυνος στον κυβερνοχώρο που συνδέεται με τη χρήση υποδομών ΤΠΕ οι οποίες καθιστούν δυνατή τη λειτουργία των συστημάτων πληρωμών και την παροχή δραστηριοτήτων επεξεργασίας πληρωμών θα πρέπει να αντιμετωπιστεί δεόντως σε επίπεδο Ένωσης μέσω εναρμονισμένων κανόνων ψηφιακής ανθεκτικότητας. Για τον σκοπό αυτό, η Επιτροπή θα πρέπει να αξιολογήσει ταχέως την ανάγκη επανεξέτασης του πεδίου εφαρμογής του παρόντος κανονισμού, ευθυγραμμίζοντας παράλληλα την εν λόγω επανεξέταση με το αποτέλεσμα της συνολικής επανεξέτασης που προβλέπεται στην οδηγία (ΕΕ) 2015/2366. Πολυάριθμες επιθέσεις μεγάλης κλίμακας κατά την τελευταία δεκαετία καταδεικνύουν τον τρόπο με τον οποίο τα συστήματα πληρωμών έχουν εκτεθεί σε κυβερνοαπειλές. Τα συστήματα πληρωμών και οι δραστηριότητες επεξεργασίας πληρωμών, που βρίσκονται στο επίκεντρο της αλυσίδας υπηρεσιών πληρωμών και παρουσιάζουν ισχυρές διασυνδέσεις με το συνολικό χρηματοοικονομικό σύστημα, απέκτησαν κρίσιμη σημασία για τη λειτουργία των χρηματοοικονομικών αγορών της Ένωσης. Οι κυβερνοεπιθέσεις σε τέτοια συστήματα μπορούν να προκαλέσουν σοβαρές επιχειρησιακές διαταραχές με άμεσες επιπτώσεις σε βασικές οικονομικές λειτουργίες, όπως η διευκόλυνση των πληρωμών, και έμμεσες επιπτώσεις στις σχετικές οικονομικές διαδικασίες. Έως ότου εφαρμοστούν εναρμονισμένο καθεστώς και η εποπτεία των φορέων εκμετάλλευσης συστημάτων πληρωμών και των οντοτήτων επεξεργασίας σε επίπεδο Ένωσης, τα κράτη μέλη μπορούν, με σκοπό την εφαρμογή παρόμοιων πρακτικών της αγοράς, να αντλούν έμπνευση από τις απαιτήσεις ψηφιακής επιχειρησιακής ανθεκτικότητας που ορίζονται στον παρόντα κανονισμό, κατά την εφαρμογή των κανόνων στους διαχειριστές συστημάτων πληρωμών και τις οντότητες επεξεργασίας που αποτελούν αντικείμενο εποπτείας υπό τη δικαιοδοσία τους.

([23]) Κανονισμός (ΕΚ) αριθ. 1060/2009 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Σεπτεμβρίου 2009, για τους οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας (ΕΕ L 302 της 17.11.2009, σ. 1).

([24]) Κανονισμός (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 4ης Ιουλίου 2012, για τα εξωχρηματιστηριακά παράγωγα, τους κεντρικούς αντισυμβαλλομένους και τα αρχεία καταγραφής συναλλαγών (ΕΕ L 201 της 27.7.2012, σ. 1).

([25]) Κανονισμός (ΕΕ) αριθ. 600/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 (ΕΕ L 173 της 12.6.2014, σ. 84).

([26]) Κανονισμός (ΕΕ) αριθ. 909/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με τη βελτίωση του διακανονισμού αξιογράφων στην Ευρωπαϊκή Ένωση και τα κεντρικά αποθετήρια τίτλων και για την τροποποίηση των οδηγιών 98/26/ΕΚ και 2014/65/ΕΕ και του κανονισμού (ΕΕ) αριθ. 236/2012 (ΕΕ L 257 της 28.8.2014, σ. 1).

([27]) Οδηγία (ΕΕ) 2022/2556 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, για την τροποποίηση των οδηγιών 2009/65/ΕΚ, 2009/138/ΕΚ, 2011/61/ΕΕ, 2013/36/ΕΕ, 2014/59/ΕΕ, 2014/65/ΕΕ, (ΕΕ) 2015/2366 και (ΕΕ) 2016/2341 όσον αφορά την ψηφιακή επιχειρησιακή ανθεκτικότητα για τον χρηματοοικονομικό τομέα (βλέπε σελίδα 153 της παρούσας Επίσημης Εφημερίδας).

([28]) Κανονισμός (ΕΕ) 2016/1011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 8ης Ιουνίου 2016, σχετικά με τους δείκτες που χρησιμοποιούνται ως δείκτες αναφοράς σε χρηματοπιστωτικά μέσα και χρηματοπιστωτικές συμβάσεις ή για τη μέτρηση της απόδοσης επενδυτικών κεφαλαίων, και για την τροποποίηση των οδηγιών 2008/48/ΕΚ και 2014/17/ΕΕ και του κανονισμού (ΕΕ) αριθ. 596/2014 (ΕΕ L 171 της 29.6.2016, σ. 1).

(105) Δεδομένου ότι ο στόχος του παρόντος κανονισμού, και συγκεκριμένα η διασφάλιση υψηλού επιπέδου ψηφιακής επιχειρησιακής ανθεκτικότητας για ρυθμιζόμενες χρηματοοικονομικές οντότητες, δεν μπορεί να επιτευχθεί επαρκώς από τα κράτη μέλη, διότι προϋποθέτει εναρμόνιση ποικίλων διαφορετικών κανόνων του ενωσιακού και εθνικού δικαίου, αλλά, λόγω της κλίμακας και των επιπτώσεών του, μπορεί να επιτευχθεί καλύτερα σε επίπεδο Ένωσης, η Ένωση δύναται να λάβει μέτρα σύμφωνα με την αρχή της επικουρικότητας, όπως διατυπώνεται στο άρθρο 5 της Συνθήκης για την Ευρωπαϊκή Ένωση. Σύμφωνα με την αρχή της αναλογικότητας, όπως διατυπώνεται στο εν λόγω άρθρο, ο παρών κανονισμός δεν βαίνει πέραν των αναγκαίων ορίων για την επίτευξη του επιδιωκόμενου στόχου.

(106) Ζητήθηκε, σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([29]), η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, που γνωμοδότησε στις 10 Μαΐου 2021 ([30]),

ΕΞΕΔΩΣΑΝ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

ΚΕΦΑΛΑΙΟ I

Γενικές διατάξεις

Άρθρο 1

Αντικείμενο

1. Προκειμένου να επιτευχθεί υψηλό κοινό επίπεδο ψηφιακής επιχειρησιακής ανθεκτικότητας, ο παρών κανονισμός καθορίζει ενιαίες απαιτήσεις σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών, τα οποία υποστηρίζουν τις επιχειρηματικές διαδικασίες των χρηματοοικονομικών οντοτήτων ως εξής:

α) απαιτήσεις που ισχύουν για τις χρηματοοικονομικές οντότητες όσον αφορά τα εξής:

   i) διαχείριση κινδύνων των τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ),

   ii) αναφορά μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ και κοινοποίηση, σε προαιρετική βάση, σημαντικών κυβερνοαπειλών στις αρμόδιες αρχές,

   iii) αναφορά μειζόνων λειτουργικών συμβάντων ή συμβάντων ασφάλειας που σχετίζονται με πληρωμές στις αρμόδιες αρχές από τις χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 στοιχεία α)έως δ),

   iv) δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας,

   v) ανταλλαγή πληροφοριών και στοιχείων σχετικά με κυβερνοαπειλές και ευπάθειες,

   vi) μέτρα για τη χρηστή διαχείριση των κινδύνων τρίτων παρόχων ΤΠΕ,

β) απαιτήσεις σε σχέση με τις συμβατικές ρυθμίσεις που συνάπτονται μεταξύ τρίτων παρόχων υπηρεσιών ΤΠΕ και χρηματοοικονομικών οντοτήτων,

γ) κανόνες για τον καθορισμό και τη λειτουργία του πλαισίου εποπτείας για κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ κατά την παροχή υπηρεσιών σε χρηματοοικονομικές οντότητες,

δ) κανόνες για τη συνεργασία μεταξύ των αρμόδιων αρχών και κανόνες για την εποπτεία και την επιβολή του νόμου από τις αρμόδιες αρχές σε σχέση με όλα τα ζητήματα που καλύπτονται από τον παρόντα κανονισμό.

2. Όσον αφορά τις χρηματοοικονομικές οντότητες που προσδιορίζονται ως βασικές ή σημαντικές οντότητες σύμφωνα με τους εθνικούς κανόνες που μεταφέρουν το άρθρο 3 της οδηγίας (ΕΕ) 2022/2555 στο εθνικό δίκαιο, ο παρών κανονισμός θεωρείται τομεακή νομική πράξη της Ένωσης για τους σκοπούς του άρθρου 4 της εν λόγω οδηγίας.

3. Ο παρών κανονισμός δεν θίγει την ευθύνη των κρατών μελών όσον αφορά βασικές λειτουργίες του κράτους σχετικά με τη δημόσια ασφάλεια, την άμυνα και την εθνική ασφάλεια σύμφωνα με το δίκαιο της Ένωσης.

([29]) Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (ΕΕ L 295 της 21.11.2018, σ. 39).

([30]) ΕΕ C 229 της 15.6.2021, σ. 16.

Άρθρο 2

Πεδίο εφαρμογής

1. Με την επιφύλαξη των παραγράφων 3 και 4, ο παρών κανονισμός εφαρμόζεται στις ακόλουθες οντότητες:

α) πιστωτικά ιδρύματα,

β) ιδρύματα πληρωμών, συμπεριλαμβανομένων των ιδρυμάτων πληρωμών που εξαιρούνται σύμφωνα με την οδηγία (ΕΕ) 2015/2366,

γ) παρόχους υπηρεσιών πληροφοριών λογαριασμού,

δ) ιδρύματα ηλεκτρονικού χρήματος, συμπεριλαμβανομένων των ιδρυμάτων ηλεκτρονικού χρήματος που εξαιρούνται σύμφωνα με την οδηγία 2009/110/ΕΚ,

ε) επιχειρήσεις επενδύσεων,

στ) παρόχους υπηρεσιών κρυπτοστοιχείων που έχουν λάβει άδεια βάσει κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τις αγορές κρυπτοστοιχείων και την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1093/2010 και (ΕΕ) αριθ. 1095/2010 και των οδηγιών 2013/36/ΕΕ and (ΕΕ) 2019/1937 («κανονισμός σχετικά με τις αγορές κρυπτοστοιχείων») και τους εκδότες ψηφιακών μαρκών με εγγύηση περιουσιακών στοιχείων,

ζ) κεντρικά αποθετήρια τίτλων,

η) κεντρικούς αντισυμβαλλομένους,

θ) τόπους διαπραγμάτευσης,

ι) αρχεία καταγραφής συναλλαγών,

ια) διαχειριστές οργανισμών εναλλακτικών επενδύσεων,

ιβ) εταιρείες διαχείρισης,

ιγ) παρόχους υπηρεσιών αναφοράς δεδομένων,

ιδ) ασφαλιστικές και αντασφαλιστικές επιχειρήσεις,

ιε) ασφαλιστικούς διαμεσολαβητές, αντασφαλιστικούς διαμεσολαβητές και ασφαλιστικούς διαμεσολαβητές που ασκούν ως δευτερεύουσα δραστηριότητα την ασφαλιστική διαμεσολάβηση,

ιστ) ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών,

ιζ) οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας,

ιη) διαχειριστές δεικτών αναφοράς κρίσιμης σημασίας,

ιθ) παρόχους υπηρεσιών συμμετοχικής χρηματοδότησης,

κ) αρχεία καταγραφής τιτλοποιήσεων,

κα) τρίτους παρόχους υπηρεσιών ΤΠΕ.

2. Για τους σκοπούς του παρόντος κανονισμού, οι οντότητες που αναφέρονται στην παράγραφο 1 στοιχεία α) έως κ) αναφέρονται συλλογικά ως «χρηματοοικονομικές οντότητες».

3. Ο παρών κανονισμός δεν εφαρμόζεται σε:

α) διαχειριστές οργανισμών εναλλακτικών επενδύσεων, όπως αναφέρονται στο άρθρο 3 παράγραφος 2 της οδηγίας 2011/61/ΕΕ,

β) ασφαλιστικές και αντασφαλιστικές επιχειρήσεις, όπως αναφέρονται στο άρθρο 4 της οδηγίας 2009/138/ΕΚ,

γ) ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών που διαχειρίζονται συνταξιοδοτικά συστήματα τα οποία συνολικά δεν έχουν περισσότερα από 15 μέλη,

δ) φυσικά ή νομικά πρόσωπα που εξαιρούνται σύμφωνα με τα άρθρα 2 και 3 της οδηγίας 2014/65/ΕΕ,

ε) ασφαλιστικούς διαμεσολαβητές, αντασφαλιστικούς διαμεσολαβητές και ασφαλιστικούς διαμεσολαβητές που ασκούν ως δευτερεύουσα δραστηριότητα την ασφαλιστική διαμεσολάβηση που είναι πολύ μικρές επιχειρήσεις ή μικρές ή μεσαίες επιχειρήσεις,

στ) γραφεία ταχυδρομικών επιταγών, όπως αναφέρονται στο άρθρο 2 παράγραφος 5 σημείο 3) της οδηγίας 2013/36/ΕΕ.

4. Τα κράτη μέλη μπορούν να εξαιρούν από το πεδίο εφαρμογής του παρόντος κανονισμού τις οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 5 σημεία 4) έως 23) της οδηγίας 2013/36/ΕΕ και οι οποίες είναι εγκατεστημένες στην αντίστοιχη επικράτειά τους. Όταν ένα κράτος μέλος κάνει χρήση της δυνατότητας αυτής, ενημερώνει σχετικά την Επιτροπή, καθώς και για κάθε μεταγενέστερη τροποποίησή της. Η Επιτροπή δημοσιοποιεί τις πληροφορίες αυτές στον ιστότοπό της ή σε άλλα εύκολα προσβάσιμα μέσα.

Άρθρο 3

Ορισμοί

Για τους σκοπούς του παρόντος κανονισμού, ισχύουν οι ακόλουθοι ορισμοί:

1) «ψηφιακή επιχειρησιακή ανθεκτικότητα»: η ικανότητα μιας χρηματοοικονομικής οντότητας να διαμορφώνει, να εξασφαλίζει και να επανεξετάζει την επιχειρησιακή ακεραιότητα και αξιοπιστία της, διασφαλίζοντας, άμεσα ή έμμεσα μέσω της χρήσης υπηρεσιών που προσφέρονται από τρίτους παρόχους υπηρεσιών ΤΠΕ, το πλήρες φάσμα των ικανοτήτων ΤΠΕ που απαιτούνται, ώστε να ανταποκρίνεται στην ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιεί η χρηματοοικονομική οντότητα και τα οποία υποστηρίζουν τη συνεχή παροχή χρηματοοικονομικών υπηρεσιών και την ποιότητά τους, μεταξύ άλλων καθ' όλη τη διάρκεια διαταραχών,

2) «σύστημα δικτύου και πληροφοριών»: σύστημα δικτύου και πληροφοριών, όπως ορίζεται στο άρθρο 6 σημείο 1) της οδηγίας (ΕΕ) 2022/2555

3) «παρωχημένο σύστημα ΤΠΕ»: σύστημα ΤΠΕ που έχει φτάσει στο τέλος του κύκλου ζωής του (τέλος κύκλου ζωής), το οποίο δεν είναι κατάλληλο για αναβαθμίσεις ή επιδιορθώσεις, για τεχνολογικούς ή εμπορικούς λόγους, ή δεν υποστηρίζεται πλέον από τον προμηθευτή του ή από τρίτο πάροχο υπηρεσιών ΤΠΕ, αλλά εξακολουθεί να χρησιμοποιείται και υποστηρίζει τις λειτουργίες της χρηματοοικονομικής οντότητας,

4) «ασφάλεια συστημάτων δικτύου και πληροφοριών»: η ασφάλεια των συστημάτων δικτύου και πληροφοριών, όπως ορίζεται στο άρθρο 6 σημείο 2) της οδηγίας (ΕΕ) 2022/2555

5) «κίνδυνος ΤΠΕ»: κάθε ευλόγως προσδιορίσιμη περίσταση σε σχέση με τη χρήση συστημάτων δικτύου και πληροφοριών η οποία, εάν επέλθει, ενδέχεται να θέσει σε κίνδυνο την ασφάλεια των συστημάτων δικτύου και πληροφοριών, κάθε εργαλείου ή διαδικασίας που εξαρτάται από την τεχνολογία, λειτουργιών και διαδικασιών ή της παροχής υπηρεσιών, προκαλώντας δυσμενείς επιπτώσεις στο ψηφιακό ή υλικό περιβάλλον,

6) «πληροφοριακός πόρος»: συλλογή πληροφοριών, ενσώματων ή άυλων, που αξίζουν να προστατευτούν,

7) «πόρος ΤΠΕ»: πόρος λογισμικού ή υλισμικού στα συστήματα δικτύου και πληροφοριών που χρησιμοποιεί η χρηματοοικονομική οντότητα,

8) «συμβάν που σχετίζεται με τις ΤΠΕ»: μεμονωμένο συμβάν ή σειρά συνδεδεμένων γεγονότων που δεν έχει προγραμματιστεί από τη χρηματοοικονομική οντότητα και θέτει σε κίνδυνο την ασφάλεια των συστημάτων δικτύου και πληροφοριών, και έχει δυσμενείς επιπτώσεις στη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων, ή στις υπηρεσίες που παρέχονται από τη χρηματοοικονομική οντότητα,

9) «λειτουργικό συμβάν ή συμβάν ασφάλειας που σχετίζεται με πληρωμές»: μεμονωμένο συμβάν ή σειρά συνδεδεμένων συμβάντων που δεν έχει προγραμματιστεί από τις χρηματοοικονομικές οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 στοιχεία α) έως δ), είτε σχετίζεται με τις ΤΠΕ είτε όχι, το οποίο έχει δυσμενείς επιπτώσεις στη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων που σχετίζονται με πληρωμές δεδομένων ή στις παρεχόμενες από τη χρηματοοικονομική οντότητα υπηρεσίες που σχετίζονται με πληρωμές,

10) «μείζον συμβάν που σχετίζεται με τις ΤΠΕ»: συμβάν που σχετίζεται με τις ΤΠΕ και το οποίο έχει εξαιρετικά δυσμενείς επιπτώσεις στα συστήματα δικτύου και πληροφοριών που υποστηρίζουν κρίσιμες λειτουργίες της χρηματοοικονομικής οντότητας,

11) «μείζον λειτουργικό συμβάν ή συμβάν ασφάλειας που σχετίζεται με πληρωμές»: λειτουργικό συμβάν ή συμβάν ασφάλειας που σχετίζεται με πληρωμές και το οποίο έχει εξαιρετικά δυσμενείς επιπτώσεις στις παρεχόμενες υπηρεσίες που σχετίζονται με πληρωμές,

12) «κυβερνοαπειλή»: κυβερνοαπειλή, όπως ορίζεται στο άρθρο 2 σημείο 8) του κανονισμού (ΕΕ) 2019/881,

13) «σημαντική κυβερνοαπειλή»: κυβερνοαπειλή της οποίας τα τεχνικά χαρακτηριστικά δείχνουν ότι θα μπορούσε να οδηγήσει σε μείζον συμβάν που σχετίζεται με τις ΤΠΕ ή σε μείζον λειτουργικό συμβάν ή συμβάν ασφάλειας που σχετίζεται με πληρωμές,

14) «κυβερνοεπίθεση»: κακόβουλο συμβάν που σχετίζεται με τις ΤΠΕ και προκαλείται μέσω απόπειρας καταστροφής, έκθεσης, μεταβολής, απενεργοποίησης, υποκλοπής ή απόκτησης μη εξουσιοδοτημένης πρόσβασης ή μη εξουσιοδοτημένης χρήσης πόρου, η οποία τελείται από οποιονδήποτε παράγοντα απειλής,

15) «πληροφορίες για απειλές»: πληροφορίες που έχουν συγκεντρωθεί, μετατραπεί, αναλυθεί, ερμηνευθεί ή εμπλουτιστεί με σκοπό την παροχή του απαραίτητου πλαισίου λήψης αποφάσεων και επιτρέπουν τη σχετική και επαρκή κατανόηση για τον μετριασμό των επιπτώσεων ενός συμβάντος που σχετίζεται με τις ΤΠΕ ή μιας κυβερνοαπειλής, συμπεριλαμβανομένων των τεχνικών λεπτομερειών μιας κυβερνοεπίθεσης, των προσώπων που ευθύνονται για την επίθεση και του τρόπου λειτουργίας και των κινήτρων τους,

16) «ευπάθεια»: αδυναμία, ευαισθησία ή ελάττωμα πόρου, συστήματος, διαδικασίας ή ελέγχου που μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης,

17) «δοκιμές παρείσδυσης βάσει απειλών (TLPT)»: πλαίσιο μίμησης των τακτικών, των τεχνικών και των διαδικασιών που χρησιμοποιούν πραγματικοί παράγοντες απειλής που θεωρείται ως γνήσια κυβερνοαπειλή, το οποίο παρέχει ελεγχόμενη, κατά παραγγελία και βάσει στοιχείων (κόκκινη ομάδα) δοκιμή των κρίσιμων συστημάτων παραγωγής της χρηματοοικονομικής οντότητας,

18) «κίνδυνος τρίτων παρόχων ΤΠΕ»: κίνδυνος ΤΠΕ που μπορεί να ανακύψει για χρηματοοικονομική οντότητα σε σχέση με τη χρήση υπηρεσιών ΤΠΕ που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ ή υπεργολάβους των παρόχων αυτών, μεταξύ άλλων μέσω ρυθμίσεων εξωτερικής ανάθεσης,

19) «τρίτος πάροχος υπηρεσιών ΤΠΕ»: επιχείρηση που παρέχει υπηρεσίες ΤΠΕ,

20) «ενδοομιλικός πάροχος υπηρεσιών ΤΠΕ»: επιχείρηση που αποτελεί μέρος χρηματοοικονομικού ομίλου και παρέχει κυρίως υπηρεσίες ΤΠΕ σε χρηματοοικονομικές οντότητες του ίδιου ομίλου ή σε χρηματοοικονομικές οντότητες που ανήκουν στο ίδιο θεσμικό σύστημα προστασίας, συμπεριλαμβανομένων των μητρικών επιχειρήσεων, των θυγατρικών και των υποκαταστημάτων τους ή άλλων οντοτήτων που τελούν υπό κοινή ιδιοκτησία ή έλεγχο,

21) «υπηρεσίες ΤΠΕ»: ψηφιακές υπηρεσίες και υπηρεσίες δεδομένων που παρέχονται μέσω συστημάτων ΤΠΕ σε έναν ή περισσότερους εσωτερικούς ή εξωτερικούς χρήστες σε συνεχή βάση, συμπεριλαμβανομένων του υλισμικού ως υπηρεσίας και υπηρεσιών υλισμικού που περιλαμβάνουν την παροχή τεχνικής υποστήριξης μέσω ενημερώσεων λογισμικού ή υλικολογισμικού από τον πάροχο υλισμικού, εξαιρουμένων των παραδοσιακών αναλογικών τηλεφωνικών υπηρεσιών,

22) «κρίσιμη ή σημαντική λειτουργία»: λειτουργία η διαταραχή της οποίας θα έβλαπτε ουσιωδώς τις οικονομικές επιδόσεις χρηματοοικονομικής οντότητας ή την ορθότητα ή τη συνέχεια των υπηρεσιών και δραστηριοτήτων της ή της οποίας η ασυνεχής, πλημμελής ή αποτυχημένη εκτέλεση θα έβλαπτε ουσιωδώς τη συνεχή συμμόρφωση μιας χρηματοοικονομικής οντότητας με τους όρους και τις υποχρεώσεις της άδειας λειτουργίας της ή με τις λοιπές υποχρεώσεις τις οποίες υπέχει βάσει του ισχύοντος δικαίου για τις χρηματοοικονομικές υπηρεσίες,

23) «κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ»: τρίτος πάροχος υπηρεσιών ο οποίος έχει οριστεί ως κρίσιμος σύμφωνα με το άρθρο 31,

24) «τρίτος πάροχος υπηρεσιών ΤΠΕ εγκατεστημένος σε τρίτη χώρα»: τρίτος πάροχος υπηρεσιών ΤΠΕ ο οποίος είναι νομικό πρόσωπο εγκατεστημένο σε τρίτη χώρα που έχει συνάψει συμβατικές ρυθμίσεις με χρηματοοικονομική οντότητα για την παροχή υπηρεσιών ΤΠΕ,

25) «θυγατρική»: θυγατρική επιχείρηση κατά την έννοια του άρθρου 2 σημείο 10) και του άρθρου 22 της οδηγίας 2013/34/ΕΕ,

26) «όμιλος»: όμιλος κατά την έννοια του άρθρου 2 σημείο 11) της οδηγίας 2013/34/ΕΕ,

27) «μητρική επιχείρηση»: μητρική επιχείρηση κατά την έννοια του άρθρου 2 σημείο 9) και του άρθρου 22 της οδηγίας 2013/34/ΕΕ,

28) «υπεργολάβος ΤΠΕ εγκατεστημένος σε τρίτη χώρα»: υπεργολάβος ΤΠΕ ο οποίος είναι νομικό πρόσωπο εγκατεστημένο σε τρίτη χώρα που έχει συνάψει συμβατικές ρυθμίσεις με τρίτο πάροχο υπηρεσιών ΤΠΕ ή με τρίτο πάροχο υπηρεσιών ΤΠΕ εγκατεστημένο σε τρίτη χώρα,

29) «κίνδυνος συγκέντρωσης ΤΠΕ»: έκθεση σε μεμονωμένους ή πολλαπλούς σχετιζόμενους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, η οποία δημιουργεί έναν βαθμό εξάρτησης από τους εν λόγω παρόχους, έτσι ώστε η μη διαθεσιμότητα, η αθέτηση υποχρεώσεων ή άλλου είδους αδυναμία του εν λόγω παρόχου να ενδέχεται να θέσει σε κίνδυνο την ικανότητα μιας χρηματοοικονομικής οντότητας να παρέχει κρίσιμες ή σημαντικές λειτουργίες ή να της προκαλέσει άλλες μορφές δυσμενών επιπτώσεων, συμπεριλαμβανομένων μεγάλων ζημιών, ή να θέσει σε κίνδυνο τη χρηματοοικονομική σταθερότητα της Ένωσης στο σύνολό της,

30) «διοικητικό όργανο»: διοικητικό όργανο, όπως ορίζεται στο άρθρο 4 παράγραφος 1 σημείο 36) της οδηγίας 2014/65/ΕΕ, στο άρθρο 3 παράγραφος 1 σημείο 7) της οδηγίας 2013/36/ΕΕ, στο άρθρο 2 παράγραφος 1 στοιχείο ιθ) της οδηγίας 2009/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([31]), στο άρθρο 2 παράγραφος 1 σημείο 45) του κανονισμού (ΕΕ) αριθ. 909/2014, στο άρθρο 3 παράγραφος 1 σημείο 20) του κανονισμού (ΕΕ) 2016/1011 και στις σχετικές διατάξεις του κανονισμού σχετικά με τις αγορές κρυπτοστοιχείων ή τα ισοδύναμα πρόσωπα που διευθύνουν πράγματι την οντότητα ή ασκούν βασικά καθήκοντα σύμφωνα με τη σχετική ενωσιακή ή εθνική νομοθεσία,

31) «πιστωτικό ίδρυμα»: πιστωτικό ίδρυμα όπως ορίζεται στο άρθρο 4 παράγραφος 1 σημείο 1) του κανονισμού (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([32]),

32) «ίδρυμα που εξαιρείται βάσει της οδηγίας 2013/36/ΕΕ»: οντότητα όπως αναφέρεται στο άρθρο 2 παράγραφος 5 σημεία 4) έως 23) της οδηγίας 2013/36/ΕΕ,

33) «επιχείρηση επενδύσεων»: επιχείρηση επενδύσεων όπως ορίζεται στο άρθρο 4 παράγραφος 1 σημείο 1) της οδηγίας 2014/65/ΕΕ,

34) «μικρή και μη διασυνδεδεμένη επιχείρηση επενδύσεων»: επιχείρηση επενδύσεων που πληροί τους όρους που ορίζονται στο άρθρο 12 παράγραφος 1 του κανονισμού (ΕΕ) 2019/2033 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([33]),

35) «ίδρυμα πληρωμών»: ίδρυμα πληρωμών όπως ορίζεται στο άρθρο 4 σημείο 4) της οδηγίας (ΕΕ) 2015/2366,

36) «ίδρυμα πληρωμών που εξαιρείται βάσει της οδηγίας (ΕΕ) 2015/2366»: ίδρυμα πληρωμών που εξαιρείται βάσει του άρθρου 32 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366,

37) «πάροχος υπηρεσιών πληροφοριών λογαριασμού»: πάροχος υπηρεσιών πληροφοριών λογαριασμού όπως αναφέρεται στο άρθρο 33 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366,

38) «ίδρυμα ηλεκτρονικού χρήματος»: ίδρυμα ηλεκτρονικού χρήματος όπως ορίζεται στο άρθρο 2 σημείο 1) της οδηγίας 2009/110/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου,

39) «ίδρυμα ηλεκτρονικού χρήματος που εξαιρείται βάσει της οδηγίας 2009/110/ΕΚ»: ίδρυμα ηλεκτρονικού χρήματος που δικαιούται απαλλαγής, όπως αναφέρεται στο άρθρο 9 παράγραφος 1 της οδηγίας 2009/110/ΕΚ,

40) «κεντρικός αντισυμβαλλόμενος»: κεντρικός αντισυμβαλλόμενος όπως ορίζεται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 648/2012,

41) «αρχείο καταγραφής συναλλαγών»: αρχείο καταγραφής συναλλαγών όπως ορίζεται στο άρθρο 2 σημείο 2) του κανονισμού (ΕΕ) αριθ. 648/2012,

42) «κεντρικό αποθετήριο τίτλων»: κεντρικό αποθετήριο τίτλων όπως ορίζεται στο άρθρο 2 παράγραφος 1 σημείο 1) του κανονισμού (ΕΕ) αριθ. 909/2014,

43) «τόπος διαπραγμάτευσης»: τόπος διαπραγμάτευσης όπως ορίζεται στο άρθρο 4 παράγραφος 1 σημείο 24) της οδηγίας 2014/65/ΕΕ,

44) «διαχειριστής οργανισμών εναλλακτικών επενδύσεων»: διαχειριστής οργανισμών εναλλακτικών επενδύσεων όπως ορίζεται στο άρθρο 4 παράγραφος 1 στοιχείο β) της οδηγίας 2011/61/ΕΕ,

45) «εταιρεία διαχείρισης»: εταιρεία διαχείρισης όπως ορίζεται στο άρθρο 2 παράγραφος 1 στοιχείο β) της οδηγίας 2009/65/ΕΚ,

46) «πάροχος υπηρεσιών αναφοράς δεδομένων»: πάροχος υπηρεσιών αναφοράς δεδομένων κατά την έννοια του κανονισμού (ΕΕ) αριθ. 600/2014, όπως αναφέρεται στο άρθρο 2 παράγραφος 1 σημεία 34) έως 36),

47) «ασφαλιστική επιχείρηση»: ασφαλιστική επιχείρηση όπως ορίζεται στο άρθρο 13 σημείο 1) της οδηγίας 2009/138/ΕΚ,

48) «αντασφαλιστική επιχείρηση»: αντασφαλιστική επιχείρηση όπως ορίζεται στο άρθρο 13 σημείο 4) της οδηγίας 2009/138/ΕΚ,

([31]) Οδηγία 2009/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουλίου 2009, για τον συντονισμό των νομοθετικών, κανονιστικών και διοικητικών διατάξεων σχετικά με ορισμένους οργανισμούς συλλογικών επενδύσεων σε κινητές αξίες (ΟΣΕΚΑ) (ΕΕ L 302 της 17.11.2009, σ. 32).

([32]) Κανονισμός (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με τις απαιτήσεις προληπτικής εποπτείας για πιστωτικά ιδρύματα και την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 (ΕΕ L 176 της 27.6.2013, σ. 1).

([33]) Κανονισμός (ΕΕ) 2019/2033 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Νοεμβρίου 2019, σχετικά με τις απαιτήσεις προληπτικής εποπτείας επιχειρήσεων επενδύσεων και την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 575/2013, (ΕΕ) αριθ. 600/2014 και (ΕΕ) αριθ. 806/2014 (ΕΕ L 314 της 5.12.2019, σ. 1).

49) «ασφαλιστικός διαμεσολαβητής»: ασφαλιστικός διαμεσολαβητής όπως ορίζεται στο άρθρο 2 παράγραφος 1 σημείο 3) της οδηγίας (ΕΕ) 2016/97 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([34]),

50) «ασφαλιστικός διαμεσολαβητής που ασκεί ως δευτερεύουσα δραστηριότητα την ασφαλιστική διαμεσολάβηση»: ασφαλιστικός διαμεσολαβητής που ασκεί ως δευτερεύουσα δραστηριότητα την ασφαλιστική διαμεσολάβηση, όπως ορίζεται στο άρθρο 2 παράγραφος 1 σημείο 4) της οδηγίας (ΕΕ) 2016/97,

51) «αντασφαλιστικός διαμεσολαβητής»: αντασφαλιστικός διαμεσολαβητής όπως ορίζεται στο άρθρο 2 παράγραφος 1 σημείο 5) της οδηγίας (ΕΕ) 2016/97,

52) «ίδρυμα επαγγελματικών συνταξιοδοτικών παροχών»: ίδρυμα επαγγελματικών συνταξιοδοτικών παροχών όπως ορίζεται στο άρθρο 6 σημείο 1) της οδηγίας (ΕΕ) 2016/2341,

53) «μικρό ίδρυμα επαγγελματικών συνταξιοδοτικών παροχών»: ίδρυμα επαγγελματικών συνταξιοδοτικών παροχών που διαχειρίζεται συνταξιοδοτικά συστήματα τα οποία έχουν συνολικά λιγότερα από 100 μέλη,

54) «οργανισμός αξιολόγησης πιστοληπτικής ικανότητας»: οργανισμός αξιολόγησης πιστοληπτικής ικανότητας όπως ορίζεται στο άρθρο 3 παράγραφος 1 στοιχείο β) του κανονισμού (ΕΚ) αριθ. 1060/2009,

55) «πάροχος υπηρεσιών κρυπτοστοιχείων»: πάροχος υπηρεσιών κρυπτοστοιχείων όπως ορίζεται στη σχετική διάταξη του κανονισμού σχετικά με τις αγορές κρυπτοστοιχείων,

56) «εκδότης ψηφιακών μαρκών με εγγύηση περιουσιακών στοιχείων»: εκδότης ψηφιακών μαρκών με εγγύηση περιουσιακών στοιχείων όπως ορίζεται στη σχετική διάταξη του κανονισμού σχετικά με τις αγορές κρυπτοστοιχείων,

57) «διαχειριστής δεικτών αναφοράς κρίσιμης σημασίας»: διαχειριστής δεικτών αναφοράς κρίσιμης σημασίας όπως ορίζεται στο άρθρο 3 παράγραφος 1 σημείο 25) του κανονισμού (ΕΕ) 2016/1011,

58) «πάροχος υπηρεσιών συμμετοχικής χρηματοδότησης»: πάροχος υπηρεσιών συμμετοχικής χρηματοδότησης όπως ορίζεται στο άρθρο 2 παράγραφος 1 στοιχείο ε) του κανονισμού (ΕΕ) 2020/1503 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([35]),

59) «αρχείο καταγραφής τιτλοποιήσεων»: αρχείο καταγραφής τιτλοποιήσεων όπως ορίζεται στο άρθρο 2 σημείο 23) του κανονισμού (ΕΕ) 2017/2402 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([36]),

60) «πολύ μικρή επιχείρηση»: χρηματοοικονομική οντότητα, εκτός από τόπο διαπραγμάτευσης, κεντρικό αντισυμβαλλόμενο, αρχείο καταγραφής συναλλαγών ή κεντρικό αποθετήριο τίτλων, η οποία απασχολεί λιγότερα από 10 άτομα και έχει ετήσιο κύκλο εργασιών και/ή ετήσιο σύνολο ισολογισμού που δεν υπερβαίνει τα 2 εκατομμύρια EUR,

61) «κύριος εποπτικός φορέας»: η Ευρωπαϊκή Εποπτική Αρχή που διορίζεται σύμφωνα με το άρθρο 31 παράγραφος 1 στοιχείο β) του παρόντος κανονισμού,

62) «μεικτή επιτροπή»: η επιτροπή που αναφέρεται στο άρθρο 54 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010,

63) «μικρή επιχείρηση»: χρηματοοικονομική οντότητα που απασχολεί 10 ή περισσότερα άτομα, αλλά λιγότερα από 50 άτομα, και της οποίας ο ετήσιος κύκλος εργασιών και/ή το σύνολο του ετήσιου ισολογισμού υπερβαίνει τα 2 εκατομμύρια EUR, αλλά δεν υπερβαίνει τα 10 εκατομμύρια EUR,

64) «μεσαία επιχείρηση»: χρηματοοικονομική οντότητα που δεν είναι μικρή επιχείρηση και απασχολεί λιγότερα από 250 άτομα και της οποίας ο ετήσιος κύκλος εργασιών δεν υπερβαίνει τα 50 εκατομμύρια EUR και/ή το σύνολο του ετήσιου ισολογισμού δεν υπερβαίνει τα 43 εκατομμύρια EUR,

65) «δημόσια αρχή»: κάθε κυβερνητικός ή άλλος φορέας δημόσιας διοίκησης, συμπεριλαμβανομένων των εθνικών κεντρικών τραπεζών.

([34]) Οδηγία (ΕΕ) 2016/97 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Ιανουαρίου 2016, σχετικά με τη διανομή ασφαλιστικών προϊόντων (ΕΕ L 26 της 2.2.2016, σ. 19).

([35]) Κανονισμός (ΕΕ) 2020/1503 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Οκτωβρίου 2020, σχετικά με τους Ευρωπαίους παρόχους υπηρεσιών συμμετοχικής χρηματοδότησης για επιχειρήσεις και την τροποποίηση του κανονισμού (ΕΕ) 2017/1129 και της οδηγίας (ΕΕ) 2019/1937 (ΕΕ L 347 της 20.10.2020, σ. 1).

([36]) Κανονισμός (ΕΕ) 2017/2402 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Δεκεμβρίου 2017, σχετικά με τη θέσπιση γενικού πλαισίου για την τιτλοποίηση και σχετικά με τη δημιουργία ειδικού πλαισίου για απλή, διαφανή και τυποποιημένη τιτλοποίηση και σχετικά με την τροποποίηση των οδηγιών 2009/65/ΕΚ, 2009/138/ΕΚ και 2011/61/ΕΕ και των κανονισμών (ΕΚ) αριθ. 1060/2009 και (ΕΕ) αριθ. 648/2012 (ΕΕ L 347 της 28.12.2017, σ. 35).

Άρθρο 4

Αρχή της αναλογικότητας

1. Οι χρηματοοικονομικές οντότητες εφαρμόζουν τους κανόνες που θεσπίζονται στο κεφάλαιο ΙΙ, σύμφωνα με την αρχή της αναλογικότητας, λαμβάνοντας υπόψη το μέγεθος, το συνολικό προφίλ κινδύνου, τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, δραστηριοτήτων και λειτουργιών τους.

2. Επιπλέον, η εφαρμογή από τις χρηματοοικονομικές οντότητες των κεφαλαίων ΙΙΙ και IV και του κεφαλαίου V τμήμα Ι είναι αναλογική προς το μέγεθός τους και το συνολικό προφίλ κινδύνου τους, καθώς και προς τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών τους, όπως προβλέπεται ειδικά στους σχετικούς κανόνες των εν λόγω κεφαλαίων.

3. Οι αρμόδιες αρχές εξετάζουν το ενδεχόμενο εφαρμογής της αρχής της αναλογικότητας από τις χρηματοοικονομικές οντότητες κατά την επανεξέταση της συνέπειας του πλαισίου διαχείρισης κινδύνων ΤΠΕ βάσει των εκθέσεων που υποβάλλονται κατόπιν αιτήματος των αρμόδιων αρχών σύμφωνα με το άρθρο 6 παράγραφος 5 και το άρθρο 16 παράγραφος 2.

ΚΕΦΑΛΑΙΟ ΙΙ

Διαχείριση κινδύνων ΤΠΕ

Τμήμα Ι

Άρθρο 5

Διακυβέρνηση και οργάνωση

1. Οι χρηματοοικονομικές οντότητες εφαρμόζουν πλαίσιο εσωτερικής διακυβέρνησης και ελέγχου το οποίο διασφαλίζει την αποτελεσματική και συνετή διαχείριση των κινδύνων ΤΠΕ, σύμφωνα με το άρθρο 6 παράγραφος 4, με σκοπό την επίτευξη υψηλού επιπέδου ψηφιακής επιχειρησιακής ανθεκτικότητας.

2. Το διοικητικό όργανο της χρηματοοικονομικής οντότητας καθορίζει, εγκρίνει, εποπτεύει και είναι υπεύθυνο για την εφαρμογή όλων των ρυθμίσεων σχετικά με το πλαίσιο διαχείρισης κινδύνων ΤΠΕ που προβλέπεται στο άρθρο 6 παράγραφος 1.

Για τους σκοπούς του πρώτου εδαφίου, το διοικητικό όργανο:

α) φέρει την τελική ευθύνη για τη διαχείριση κινδύνων ΤΠΕ της χρηματοοικονομικής οντότητας,

β) εφαρμόζει πολιτικές που στοχεύουν στη διασφάλιση της διατήρησης υψηλών προτύπων διαθεσιμότητας, γνησιότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων,

γ) καθορίζει σαφείς ρόλους και αρμοδιότητες για όλες τις λειτουργίες που σχετίζονται με τις ΤΠΕ και θεσπίζει κατάλληλες ρυθμίσεις διακυβέρνησης για τη διασφάλιση αποτελεσματικής και έγκαιρης επικοινωνίας, συνεργασίας και συντονισμού μεταξύ των εν λόγω λειτουργιών,

δ) φέρει τη συνολική ευθύνη για τον καθορισμό και την έγκριση της στρατηγικής ψηφιακής επιχειρησιακής ανθεκτικότητας, όπως αναφέρεται στο άρθρο 6 παράγραφος 8, συμπεριλαμβανομένου του καθορισμού του κατάλληλου επιπέδου ανοχής των κινδύνων ΤΠΕ της χρηματοοικονομικής οντότητας, όπως αναφέρεται στο άρθρο 6 παράγραφος 8 στοιχείο β),

ε) εγκρίνει, εποπτεύει και επανεξετάζει περιοδικά την εφαρμογή της πολιτικής επιχειρησιακής συνέχειας των ΤΠΕ και των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ, που αναφέρονται, αντίστοιχα, στο άρθρο 11 παράγραφοι 1 και 3, τα οποία μπορούν να εγκριθούν ως ειδική συγκεκριμένη πολιτική που αποτελεί αναπόσπαστο μέρος της συνολικής πολιτικής επιχειρησιακής συνέχειας και του σχεδίου αντιμετώπισης και ανάκαμψης της λειτουργίας της χρηματοοικονομικής οντότητας,

στ) εγκρίνει και επανεξετάζει περιοδικά τα προγράμματα εσωτερικού ελέγχου ΤΠΕ και τους ελέγχους ΤΠΕ της χρηματοοικονομικής οντότητας, καθώς και τις σημαντικές μεταβολές τους,

ζ) διαθέτει τον κατάλληλο προϋπολογισμό και τον επανεξετάζει τακτικά, ώστε να καλύπτονται οι ανάγκες ψηφιακής επιχειρησιακής ανθεκτικότητας της χρηματοοικονομικής οντότητας όσον αφορά όλα τα είδη πόρων, μεταξύ των οποίων τα σχετικά προγράμματα ευαισθητοποίησης σε θέματα ασφάλειας των ΤΠΕ και η κατάρτιση για την ψηφιακή επιχειρησιακή ανθεκτικότητα που αναφέρονται στο άρθρο 13 παράγραφος 6, και τις δεξιότητες ΤΠΕ για όλους,

η) εγκρίνει και επανεξετάζει τακτικά την πολιτική της χρηματοοικονομικής οντότητας σχετικά με τις ρυθμίσεις που αφορούν τη χρήση των υπηρεσιών ΤΠΕ οι οποίες παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ,

θ) θέτει σε εφαρμογή σε εταιρικό επίπεδο διαύλους αναφοράς που θα του επιτρέπουν να ενημερώνεται δεόντως σχετικά με τα ακόλουθα:

i) ρυθμίσεις που συνάπτονται με τρίτους παρόχους υπηρεσιών ΤΠΕ σχετικά με τη χρήση υπηρεσιών ΤΠΕ,

ii) οποιεσδήποτε σχετικές προγραμματισμένες ουσιώδεις αλλαγές όσον αφορά τους τρίτους παρόχους υπηρεσιών ΤΠΕ,

iii) τον δυνητικό αντίκτυπο των εν λόγω αλλαγών στις κρίσιμες ή σημαντικές λειτουργίες που υπόκεινται στις εν λόγω ρυθμίσεις, συμπεριλαμβανομένης σύνοψης ανάλυσης κινδύνου για την αξιολόγηση των επιπτώσεων των εν λόγω αλλαγών, και τουλάχιστον τα μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ και τις επιπτώσεις τους, καθώς και σχετικά με τα μέτρα αντιμετώπισης και ανάκαμψης και τα διορθωτικά μέτρα.

3. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, καθορίζουν ρόλο για την παρακολούθηση των ρυθμίσεων που συνάπτονται με τρίτους παρόχους υπηρεσιών ΤΠΕ όσον αφορά τη χρήση των υπηρεσιών ΤΠΕ ή ορίζουν ένα ανώτερο διοικητικό στέλεχος ως αρμόδιο για την εποπτεία της έκθεσης σε σχετικό κίνδυνο και της συναφούς τεκμηρίωσης.

4. Τα μέλη του διοικητικού οργάνου της χρηματοοικονομικής οντότητας εξελίσσουν ενεργά και επαρκώς τις γνώσεις και τις δεξιότητές τους, ώστε να κατανοούν και να αξιολογούν τους κινδύνους ΤΠΕ και τις επιπτώσεις τους στις δραστηριότητες της χρηματοοικονομικής οντότητας, μεταξύ άλλων παρακολουθώντας ειδική κατάρτιση σε τακτική βάση, ανάλογη προς τους κινδύνους ΤΠΕ που τελούν υπό διαχείριση.

ΤΜΗΜΑ ΙΙ

Άρθρο 6

Πλαίσιο διαχείρισης κινδύνων ΤΠΕ

1. Οι χρηματοοικονομικές οντότητες διαθέτουν ισχυρό, ολοκληρωμένο και άρτια τεκμηριωμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ στο πλαίσιο του συνολικού τους συστήματος διαχείρισης κινδύνων, που τους επιτρέπει να αντιμετωπίζουν τους κινδύνους ΤΠΕ με γρήγορο, αποτελεσματικό και εμπεριστατωμένο τρόπο και να διασφαλίζουν υψηλό επίπεδο ψηφιακής επιχειρησιακής ανθεκτικότητας.

2. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ περιλαμβάνει τουλάχιστον στρατηγικές, πολιτικές, διαδικασίες, πρωτόκολλα και εργαλεία ΤΠΕ που απαιτούνται για τη δέουσα και επαρκή προστασία όλων των πληροφοριακών πόρων και πόρων ΤΠΕ, συμπεριλαμβανομένου του λογισμικού, του υλισμικού, των διακομιστών, καθώς και για την προστασία όλων των σχετικών υλικών συνιστωσών και υποδομών, όπως εγκαταστάσεων, κέντρων δεδομένων και ευαίσθητων οριοθετημένων χώρων, ώστε να διασφαλίζεται ότι όλοι αυτοί οι πληροφοριακοί πόροι και πόροι ΤΠΕ προστατεύονται επαρκώς από κινδύνους, συμπεριλαμβανομένων τυχόν βλάβης και μη εξουσιοδοτημένης πρόσβασης ή χρήσης.

3. Σύμφωνα με το πλαίσιο διαχείρισης κινδύνων ΤΠΕ, οι χρηματοοικονομικές οντότητες ελαχιστοποιούν τις επιπτώσεις των κινδύνων ΤΠΕ με την ανάπτυξη κατάλληλων στρατηγικών, πολιτικών, διαδικασιών, πρωτοκόλλων ΤΠΕ και εργαλείων. Παρέχουν πλήρεις και επικαιροποιημένες πληροφορίες σχετικά με τους κινδύνους ΤΠΕ και σχετικά με το πλαίσιό τους για τη διαχείριση κινδύνων ΤΠΕ στις αρμόδιες αρχές κατόπιν αιτήματός τους.

4. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, εκχωρούν την ευθύνη για τη διαχείριση και την εποπτεία των κινδύνων ΤΠΕ σε μια λειτουργία ελέγχου και διασφαλίζουν σε επαρκές επίπεδο την ανεξαρτησία της εν λόγω λειτουργίας ελέγχου, προκειμένου να αποφεύγεται η σύγκρουση συμφερόντων. Οι χρηματοοικονομικές οντότητες διασφαλίζουν τον κατάλληλο διαχωρισμό και την κατάλληλη ανεξαρτησία των λειτουργιών διαχείρισης κινδύνων ΤΠΕ, των λειτουργιών ελέγχου και των λειτουργιών εσωτερικής επιθεώρησης, σύμφωνα με το μοντέλο των τριών γραμμών άμυνας ή ένα εσωτερικό μοντέλο διαχείρισης κινδύνων και ελέγχου.

5. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ τεκμηριώνεται και επανεξετάζεται τουλάχιστον μία φορά ετησίως, ή περιοδικά όσον αφορά τις πολύ μικρές επιχειρήσεις, καθώς και κατά την επέλευση μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ, και σύμφωνα με εποπτικές οδηγίες ή συμπεράσματα που προκύπτουν από σχετικές δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας ή διαδικασίες ελέγχου. Το πλαίσιο βελτιώνεται διαρκώς με βάση τα διδάγματα που αντλούνται από την εφαρμογή και την παρακολούθηση. Έκθεση σχετικά με την επανεξέταση του πλαισίου διαχείρισης κινδύνων ΤΠΕ υποβάλλεται στην αρμόδια αρχή κατόπιν αιτήματός της.

6. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ των χρηματοοικονομικών οντοτήτων, πλην των πολύ μικρών επιχειρήσεων, υπόκειται σε εσωτερική επιθεώρηση από ελεγκτές σε τακτική βάση, σύμφωνα με το πρόγραμμα ελέγχου των χρηματοοικονομικών οντοτήτων. Οι εν λόγω ελεγκτές διαθέτουν επαρκείς γνώσεις, δεξιότητες και εμπειρογνωσία όσον αφορά τους κινδύνους ΤΠΕ, καθώς και κατάλληλη ανεξαρτησία. Η συχνότητα και η εστίαση των ελέγχων ΤΠΕ είναι ανάλογες προς τους κινδύνους ΤΠΕ που αντιμετωπίζει η χρηματοοικονομική οντότητα.

7. Με βάση τα συμπεράσματα της επανεξέτασης εσωτερικής επιθεώρησης, οι χρηματοοικονομικές οντότητες θεσπίζουν επίσημη διαδικασία παρακολούθησης, συμπεριλαμβανομένων κανόνων για την έγκαιρη επαλήθευση και αποκατάσταση κρίσιμων ευρημάτων ελέγχου ΤΠΕ.

8. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ περιλαμβάνει στρατηγική επιχειρησιακής ψηφιακής ανθεκτικότητας για τον καθορισμό του τρόπου εφαρμογής του πλαισίου. Για τον σκοπό αυτόν, η στρατηγική επιχειρησιακής ψηφιακής ανθεκτικότητας περιλαμβάνει τις μεθόδους αντιμετώπισης κινδύνων ΤΠΕ και επίτευξης συγκεκριμένων στόχων ΤΠΕ, ως εξής:

α) επεξηγώντας τον τρόπο με τον οποίο το πλαίσιο διαχείρισης κινδύνων ΤΠΕ υποστηρίζει την επιχειρηματική στρατηγική και τους στόχους της χρηματοοικονομικής οντότητας,

β) θεσπίζοντας το επίπεδο ανοχής κινδύνου για τους κινδύνους ΤΠΕ, σύμφωνα με τη διάθεση ανάληψης κινδύνων της χρηματοοικονομικής οντότητας, και αναλύοντας την ανοχή στις επιπτώσεις για τις διαταραχές των ΤΠΕ,

γ) καθορίζοντας σαφείς στόχους ασφάλειας των πληροφοριών, συμπεριλαμβανομένων των βασικών δεικτών επιδόσεων και των βασικών μετρήσεων κινδύνου,

δ) επεξηγώντας την αρχιτεκτονική αναφοράς των ΤΠΕ και τυχόν αλλαγές που απαιτούνται για την επίτευξη συγκεκριμένων επιχειρηματικών στόχων,

ε) περιγράφοντας τους διάφορους μηχανισμούς που εφαρμόζονται για τον εντοπισμό των συμβάντων που σχετίζονται με τις ΤΠΕ, την αποτροπή των επιπτώσεών τους και την παροχή προστασίας από αυτές,

στ) τεκμηριώνοντας την τρέχουσα κατάσταση όσον αφορά την ψηφιακή επιχειρησιακή ανθεκτικότητα με βάση τον αριθμό των αναφερόμενων μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ και την αποτελεσματικότητα των προληπτικών μέτρων,

ζ) εφαρμόζοντας δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας, σύμφωνα με το κεφάλαιο IV του παρόντος κανονισμού,

η) περιγράφοντας μια στρατηγική επικοινωνίας σε περίπτωση συμβάντων που σχετίζονται με τις ΤΠΕ, η γνωστοποίηση των οποίων απαιτείται σύμφωνα με το άρθρο 14.

9. Οι χρηματοοικονομικές οντότητες μπορούν, στο πλαίσιο της στρατηγικής ψηφιακής επιχειρησιακής ανθεκτικότητας που αναφέρεται στην παράγραφο 8, να καθορίσουν μια ολιστική στρατηγική πολλαπλών προμηθευτών ΤΠΕ, σε επίπεδο ομίλου ή οντότητας, η οποία αναδεικνύει βασικές εξαρτήσεις από τρίτους παρόχους υπηρεσιών ΤΠΕ και επεξηγεί το σκεπτικό στο οποίο βασίζεται ο συνδυασμός προμηθειών από τρίτους παρόχους υπηρεσιών ΤΠΕ.

10. Οι χρηματοοικονομικές οντότητες δύνανται, σύμφωνα με το ενωσιακό και το εθνικό τομεακό δίκαιο, να αναθέσουν τα καθήκοντα επαλήθευσης της συμμόρφωσης με τις απαιτήσεις διαχείρισης κινδύνων ΤΠΕ σε ενδοομιλικές ή εξωτερικές επιχειρήσεις. Σε περίπτωση τέτοιας εξωτερικής ανάθεσης, η χρηματοοικονομική οντότητα παραμένει εξολοκλήρου υπεύθυνη για την επαλήθευση της συμμόρφωσης με τις απαιτήσεις διαχείρισης κινδύνων ΤΠΕ.

Άρθρο 7

Συστήματα, πρωτόκολλα και εργαλεία ΤΠΕ

Για την αντιμετώπιση και τη διαχείριση των κινδύνων ΤΠΕ, οι χρηματοοικονομικές οντότητες χρησιμοποιούν και διατηρούν επικαιροποιημένα συστήματα, πρωτόκολλα και εργαλεία ΤΠΕ, τα οποία:

α) είναι ανάλογα προς το μέγεθος των λειτουργιών που υποστηρίζουν τη διεξαγωγή των δραστηριοτήτων τους, σύμφωνα με την αρχή της αναλογικότητας που αναφέρεται στο άρθρο 4,

β) είναι αξιόπιστα,

γ) διαθέτουν επαρκή χωρητικότητα ώστε να επεξεργάζονται με ακρίβεια τα δεδομένα που είναι αναγκαία για την εκτέλεση δραστηριοτήτων και την έγκαιρη παροχή υπηρεσιών, και να εξυπηρετούν μεγάλο όγκο εντολών, μηνυμάτων ή συναλλαγών, όπως απαιτείται, μεταξύ άλλων σε περίπτωση υιοθέτησης νέας τεχνολογίας,

δ) είναι τεχνολογικά ανθεκτικά, ώστε να αντιμετωπίζουν επαρκώς τις πρόσθετες ανάγκες επεξεργασίας πληροφοριών, όπως απαιτείται υπό ακραίες συνθήκες της αγοράς ή άλλες αντίξοες καταστάσεις.

Άρθρο 8

Προσδιορισμός

1. Στο πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 6 παράγραφος 1, οι χρηματοοικονομικές οντότητες προσδιορίζουν, ταξινομούν και τεκμηριώνουν επαρκώς όλες τις επιχειρηματικές λειτουργίες, τους ρόλους και τις αρμοδιότητες που υποστηρίζονται από ΤΠΕ, τους πληροφοριακούς πόρους και τους πόρους ΤΠΕ που υποστηρίζουν τις εν λόγω λειτουργίες, καθώς και τους ρόλους και τις εξαρτήσεις τους σε σχέση με τους κινδύνους ΤΠΕ. Οι χρηματοοικονομικές οντότητες επανεξετάζουν, όταν κρίνεται αναγκαίο, και τουλάχιστον σε ετήσια βάση, την επάρκεια αυτής της ταξινόμησης και τυχόν συναφούς τεκμηρίωσης.

2. Οι χρηματοοικονομικές οντότητες προσδιορίζουν σε διαρκή βάση όλες τις πηγές κινδύνων ΤΠΕ, ιδίως την έκθεση σε κίνδυνο από και προς άλλες χρηματοοικονομικές οντότητες, και αξιολογούν τις κυβερνοαπειλές και τις ευπάθειες των ΤΠΕ που αφορούν τις οικείες επιχειρηματικές λειτουργίες που υποστηρίζονται από ΤΠΕ, τους πληροφοριακούς πόρους και τους πόρους ΤΠΕ. Οι χρηματοοικονομικές οντότητες επανεξετάζουν τακτικά, και τουλάχιστον σε ετήσια βάση, τα σενάρια κινδύνου που τις επηρεάζουν.

3. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, προβαίνουν σε αξιολόγηση κινδύνων έπειτα από κάθε σημαντική αλλαγή της υποδομής των συστημάτων δικτύου και πληροφοριών, των διαδικασιών ή των διεργασιών που επηρεάζουν τις οικείες επιχειρηματικές λειτουργίες που υποστηρίζονται από ΤΠΕ, τους πληροφοριακούς πόρους ή τους πόρους ΤΠΕ.

4. Οι χρηματοοικονομικές οντότητες προσδιορίζουν όλους τους πληροφοριακούς πόρους και τους πόρους ΤΠΕ, συμπεριλαμβανομένων εκείνων που βρίσκονται σε απομακρυσμένες τοποθεσίες, τους πόρους δικτύου και τον εξοπλισμό υλισμικού, και καταγράφουν όσους θεωρούνται κρίσιμοι. Καταγράφουν τις παραμέτρους των πληροφοριακών πόρων και των πόρων ΤΠΕ, καθώς και τις συνδέσεις και τις αλληλεξαρτήσεις μεταξύ των διαφόρων πληροφοριακών πόρων και πόρων ΤΠΕ.

5. Οι χρηματοοικονομικές οντότητες προσδιορίζουν και τεκμηριώνουν όλες τις διαδικασίες που εξαρτώνται από τρίτους παρόχους υπηρεσιών ΤΠΕ και προσδιορίζουν τις διασυνδέσεις με τρίτους παρόχους υπηρεσιών ΤΠΕ οι οποίοι παρέχουν υπηρεσίες που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες.

6. Για τους σκοπούς των παραγράφων 1, 4 και 5, οι χρηματοοικονομικές οντότητες τηρούν τους σχετικούς καταλόγους και τους ενημερώνουν περιοδικά και κάθε φορά που επέρχεται οποιαδήποτε σημαντική αλλαγή όπως αναφέρεται στην παράγραφο 3.

7. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, διενεργούν τακτικά, και τουλάχιστον σε ετήσια βάση, ειδική αξιολόγηση κινδύνων ΤΠΕ σε όλα τα παρωχημένα συστήματα ΤΠΕ και οπωσδήποτε πριν και μετά τη σύνδεση τεχνολογιών, εφαρμογών ή συστημάτων.

Άρθρο 9

Προστασία και πρόληψη

1. Για τους σκοπούς της διασφάλισης επαρκούς επιπέδου προστασίας συστημάτων ΤΠΕ και με στόχο την οργάνωση μέτρων αντιμετώπισης, οι χρηματοοικονομικές οντότητες παρακολουθούν και ελέγχουν σε διαρκή βάση την ασφάλεια και τη λειτουργία των συστημάτων και εργαλείων ΤΠΕ και ελαχιστοποιούν τις επιπτώσεις των σχετικών κινδύνων ΤΠΕ στα συστήματα ΤΠΕ με την ανάπτυξη κατάλληλων εργαλείων, πολιτικών και διαδικασιών για την ασφάλεια των ΤΠΕ.

2. Οι χρηματοοικονομικές οντότητες σχεδιάζουν, αποκτούν και εφαρμόζουν πολιτικές, διαδικασίες, πρωτόκολλα και εργαλεία ασφάλειας ΤΠΕ που έχουν ως στόχο τη διασφάλιση της ανθεκτικότητας, της συνέχειας και της διαθεσιμότητας των συστημάτων ΤΠΕ, ιδίως όσων υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες, και τη διατήρηση υψηλών προτύπων διαθεσιμότητας, γνησιότητας, ακεραιότητας και εμπιστευτικότητας δεδομένων, ανεξάρτητα από το αν βρίσκονται σε κατάσταση αποθήκευσης, χρήσης ή διαβίβασης.

3. Για την επίτευξη των στόχων που αναφέρονται στην παράγραφο 2, οι χρηματοοικονομικές οντότητες χρησιμοποιούν λύσεις και διαδικασίες ΤΠΕ που είναι κατάλληλες σύμφωνα με το άρθρο 4. Οι εν λόγω λύσεις και διαδικασίες ΤΠΕ:

α) εγγυώνται την ασφάλεια των μέσων διαβίβασης δεδομένων,

β) ελαχιστοποιούν τον κίνδυνο αλλοίωσης ή απώλειας δεδομένων, μη εξουσιοδοτημένης πρόσβασης και τεχνικών σφαλμάτων που ενδέχεται να παρεμποδίσουν την επιχειρηματική δραστηριότητα,

γ) προλαμβάνουν την έλλειψη διαθεσιμότητας, την υποβάθμιση της γνησιότητας και της ακεραιότητας, τις παραβιάσεις της εμπιστευτικότητας και την απώλεια δεδομένων,

δ) διασφαλίζουν ότι τα δεδομένα προστατεύονται από κινδύνους που προκύπτουν από τη διαχείριση των δεδομένων, συμπεριλαμβανομένων της πλημμελούς διοίκησης, των κινδύνων που σχετίζονται με την επεξεργασία και του ανθρώπινου σφάλματος.

4. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 6 παράγραφος 1, οι χρηματοοικονομικές οντότητες:

α) καταρτίζουν και τεκμηριώνουν πολιτική ασφάλειας των πληροφοριών που καθορίζει κανόνες για την προστασία της διαθεσιμότητας, της γνησιότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων, των πληροφοριακών πόρων και των πόρων ΤΠΕ, συμπεριλαμβανομένων εκείνων των πελατών τους, κατά περίπτωση,

β) ακολουθώντας μια προσέγγιση βάσει κινδύνων, θεσπίζουν δομή ορθής διαχείρισης δικτύων και υποδομών, χρησιμοποιώντας κατάλληλες τεχνικές, μεθόδους και πρωτόκολλα, που μπορούν να περιλαμβάνουν την εφαρμογή αυτοματοποιημένων μηχανισμών για την απομόνωση των πληροφοριακών πόρων που επηρεάζονται σε περίπτωση κυβερνοεπιθέσεων,

γ) εφαρμόζουν πολιτικές που περιορίζουν την υλική ή λογική πρόσβαση σε πληροφοριακούς πόρους και πόρους ΤΠΕ στην πρόσβαση που είναι απολύτως αναγκαία για τις νόμιμες και εγκεκριμένες λειτουργίες και δραστηριότητες και θεσπίζουν, για τον σκοπό αυτόν, ένα σύνολο πολιτικών, διαδικασιών και δικλείδων ασφάλειας που αφορούν τα δικαιώματα πρόσβασης και διασφαλίζουν την ορθή διαχείρισή τους,

δ) εφαρμόζουν πολιτικές και πρωτόκολλα για ισχυρούς μηχανισμούς αυθεντικοποίησης, με βάση σχετικά πρότυπα και ειδικά συστήματα ελέγχου, και προστατευτικά μέτρα κρυπτογραφικών κλειδιών με τα οποία κρυπτογραφούνται δεδομένα, βάσει αποτελεσμάτων εγκεκριμένων διαδικασιών κατηγοριοποίησης δεδομένων και αξιολόγησης κινδύνων ΤΠΕ,

ε) εφαρμόζουν τεκμηριωμένες πολιτικές, διαδικασίες και δικλείδες ασφάλειας για τη διαχείριση αλλαγών στις ΤΠΕ, συμπεριλαμβανομένων αλλαγών σε λογισμικό, υλισμικό, στοιχεία, συστήματα ή παράμετροι ασφάλειας υλικολογισμικού, που βασίζονται σε μια προσέγγιση αξιολόγησης κινδύνου και αποτελούν αναπόσπαστο μέρος της συνολικής διαδικασίας διαχείρισης αλλαγών της χρηματοοικονομικής οντότητας, ώστε να διασφαλιστεί ότι όλες οι αλλαγές στα συστήματα ΤΠΕ καταγράφονται, δοκιμάζονται, αξιολογούνται, εγκρίνονται, εφαρμόζονται και επαληθεύονται με ελεγχόμενο τρόπο,

στ) διαθέτουν κατάλληλες και ολοκληρωμένες τεκμηριωμένες πολιτικές σχετικά με τις ενημερώσεις κώδικα και τις επικαιροποιήσεις.

Για τους σκοπούς του πρώτου εδαφίου στοιχείο β), οι χρηματοοικονομικές οντότητες σχεδιάζουν την υποδομή σύνδεσης δικτύου κατά τρόπο ώστε να μπορεί να διακοπεί ή να κατατμηθεί στιγμιαία, προκειμένου να ελαχιστοποιείται και να αποτρέπεται η μετάδοση, ιδίως όσον αφορά τις διασυνδεδεμένες χρηματοοικονομικές διαδικασίες.

Για τους σκοπούς του πρώτου εδαφίου στοιχείο ε), η διαδικασία διαχείρισης αλλαγών ΤΠΕ εγκρίνεται από κατάλληλες ιεραρχικές δομές και διαθέτει ειδικά πρωτόκολλα.

Άρθρο 10

Εντοπισμός

1. Οι χρηματοοικονομικές οντότητες διαθέτουν μηχανισμούς για τον άμεσο εντοπισμό ασυνήθιστων δραστηριοτήτων, σύμφωνα με το άρθρο 17, συμπεριλαμβανομένων ζητημάτων που αφορούν τις επιδόσεις του δικτύου ΤΠΕ και συμβάντων που σχετίζονται με τις ΤΠΕ, καθώς και για τον προσδιορισμό των δυνητικά σημαντικών μοναδικών σημείων αποτυχίας.

Όλοι οι μηχανισμοί εντοπισμού που αναφέρονται στο πρώτο εδάφιο υποβάλλονται τακτικά σε δοκιμές σύμφωνα με το άρθρο 25.

2. Οι μηχανισμοί εντοπισμού που αναφέρονται στην παράγραφο 1 επιτρέπουν την ενεργοποίηση πολυεπίπεδων δικλείδων ασφάλειας, καθορίζουν όρια προειδοποίησης και κριτήρια για την ενεργοποίηση και έναρξη διαδικασιών αντιμετώπισης συμβάντων που σχετίζονται με τις ΤΠΕ, συμπεριλαμβανομένων αυτόματων μηχανισμών προειδοποίησης για το προσωπικό που είναι αρμόδιο για την αντιμετώπιση συμβάντων που σχετίζονται με τις ΤΠΕ.

3. Οι χρηματοοικονομικές οντότητες διαθέτουν επαρκείς πόρους και ικανότητες, ώστε να παρακολουθούν τη δραστηριότητα των χρηστών, την εμφάνιση ασυνήθιστων δραστηριοτήτων ΤΠΕ και συμβάντων που σχετίζονται με τις ΤΠΕ, ιδίως όσον αφορά κυβερνοεπιθέσεις.

4. Οι πάροχοι υπηρεσιών αναφοράς δεδομένων διαθέτουν, επιπλέον, συστήματα τα οποία μπορούν να ελέγχουν αποτελεσματικά αν οι αναφορές συναλλαγών είναι πλήρεις, να εντοπίζουν παραλείψεις και εμφανή σφάλματα και να ζητούν την εκ νέου διαβίβαση των εν λόγω αναφορών.

Άρθρο 11

Αντιμετώπιση και ανάκαμψη

1. Στο πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 6 παράγραφος 1 και βάσει των απαιτήσεων προσδιορισμού που προβλέπονται στο άρθρο 8, οι χρηματοοικονομικές οντότητες θέτουν σε εφαρμογή ολοκληρωμένη πολιτική επιχειρησιακής συνέχειας των ΤΠΕ, η οποία μπορεί να εγκριθεί ως ειδική και συγκεκριμένη πολιτική, που συνιστά αναπόσπαστο μέρος της συνολικής πολιτικής επιχειρησιακής συνέχειας της χρηματοοικονομικής οντότητας.

2. Οι χρηματοοικονομικές οντότητες εφαρμόζουν την πολιτική επιχειρησιακής συνέχειας των ΤΠΕ μέσω ειδικών, κατάλληλων και τεκμηριωμένων ρυθμίσεων, σχεδίων, διαδικασιών και μηχανισμών, με στόχο:

α) τη διασφάλιση της συνέχειας των κρίσιμων ή σημαντικών λειτουργιών της χρηματοοικονομικής οντότητας,

β) την ταχεία, κατάλληλη και αποτελεσματική αντιμετώπιση και επίλυση όλων των συμβάντων που σχετίζονται με τις ΤΠΕ, κατά τρόπο ώστε να περιορίζεται η βλάβη και να δίνεται προτεραιότητα στην επανεκκίνηση των δραστηριοτήτων και στις ενέργειες αποκατάστασης,

γ) την ενεργοποίηση, χωρίς καθυστέρηση, ειδικών σχεδίων που παρέχουν τη δυνατότητα εφαρμογής μέτρων, διαδικασιών και τεχνολογιών περιορισμού που αρμόζουν σε κάθε τύπο συμβάντος που σχετίζεται με τις ΤΠΕ και αποτρέπουν περαιτέρω βλάβες, καθώς και ειδικά προσαρμοσμένων διαδικασιών αντιμετώπισης και ανάκαμψης, οι οποίες θεσπίζονται σύμφωνα με το άρθρο 12,

δ) την προκαταρκτική εκτίμηση επιπτώσεων, βλαβών και ζημιών,

ε) τον καθορισμό δράσεων επικοινωνίας και διαχείρισης κρίσεων, οι οποίες διασφαλίζουν τη διαβίβαση επικαιροποιημένων πληροφοριών σε όλα τα μέλη του αρμόδιου εσωτερικού προσωπικού και τους εξωτερικούς συμφεροντούχους, σύμφωνα με το άρθρο 14, και αναφέρονται στις αρμόδιες αρχές σύμφωνα με το άρθρο 19.

3. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 6 παράγραφος 1, οι χρηματοοικονομικές οντότητες εφαρμόζουν σχετικά σχέδια αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ, τα οποία υπόκεινται, στην περίπτωση των χρηματοοικονομικών οντοτήτων πλην των πολύ μικρών επιχειρήσεων, σε ανεξάρτητη επανεξέταση εσωτερικής επιθεώρησης.

4. Οι χρηματοοικονομικές οντότητες θεσπίζουν, διατηρούν και υποβάλλουν περιοδικά σε δοκιμή κατάλληλα σχέδια επιχειρησιακής συνέχειας των ΤΠΕ, ιδίως όσον αφορά κρίσιμες ή σημαντικές λειτουργίες που αποτελούν αντικείμενο εξωτερικής ανάθεσης ή υπεργολαβίας μέσω ρυθμίσεων με τρίτους παρόχους υπηρεσιών ΤΠΕ.

5. Στο πλαίσιο της συνολικής πολιτικής επιχειρησιακής συνέχειας, οι χρηματοοικονομικές οντότητες διενεργούν ανάλυση επιχειρηματικών επιπτώσεων (ΑΕΕ) της έκθεσής τους σε σοβαρές διαταραχές της επιχειρηματικής δραστηριότητας. Στο πλαίσιο της ΑΕΕ, οι χρηματοοικονομικές οντότητες αξιολογούν τις πιθανές επιπτώσεις σοβαρών διαταραχών της επιχειρηματικής δραστηριότητας μέσω ποσοτικών και ποιοτικών κριτηρίων, χρησιμοποιώντας εσωτερικά και εξωτερικά δεδομένα και ανάλυση σεναρίων, κατά περίπτωση. Η ΑΕΕ εξετάζει την κρισιμότητα των προσδιορισμένων και χαρτογραφημένων επιχειρηματικών λειτουργιών, των διαδικασιών υποστήριξης, των εξαρτήσεων από τρίτους και των πληροφοριακών πόρων, καθώς και των αλληλεξαρτήσεών τους. Οι χρηματοοικονομικές οντότητες διασφαλίζουν ότι οι πόροι ΤΠΕ και οι υπηρεσίες ΤΠΕ σχεδιάζονται και χρησιμοποιούνται σε πλήρη ευθυγράμμιση με την ΑΕΕ, ιδίως όσον αφορά την επαρκή διασφάλιση της εφεδρείας όλων των κρίσιμων στοιχείων.

6. Στο πλαίσιο της ολοκληρωμένης διαχείρισης κινδύνων ΤΠΕ, οι χρηματοοικονομικές οντότητες:

α) δοκιμάζουν τα σχέδια επιχειρησιακής συνέχειας των ΤΠΕ και τα σχέδια αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ σε σχέση με τα συστήματα ΤΠΕ που υποστηρίζουν όλες τις λειτουργίες τουλάχιστον σε ετήσια βάση, καθώς και σε περίπτωση τυχόν ουσιαστικών αλλαγών στα συστήματα ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες,

β) υποβάλλουν σε δοκιμή τα σχέδια επικοινωνίας σε καταστάσεις κρίσης που καταρτίζονται σύμφωνα με το άρθρο 14.

Για τους σκοπούς του πρώτου εδαφίου στοιχείο α), οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, περιλαμβάνουν στα σχέδια δοκιμών σενάρια κυβερνοεπιθέσεων και μετάβασης μεταξύ της κύριας υποδομής ΤΠΕ και της εφεδρικής χωρητικότητας, αντίγραφα ασφαλείας και εφεδρικές εγκαταστάσεις που απαιτούνται για την εκπλήρωση των υποχρεώσεων που προβλέπονται στο άρθρο 12.

Οι χρηματοοικονομικές οντότητες επανεξετάζουν ανά τακτά χρονικά διαστήματα τα σχέδια επιχειρησιακής συνέχειας των ΤΠΕ και αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ, λαμβάνοντας υπόψη τα αποτελέσματα των δοκιμών που διενεργούνται σύμφωνα με το πρώτο εδάφιο και τις συστάσεις που προκύπτουν από ελέγχους ή εποπτικές αξιολογήσεις.

7. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, διαθέτουν λειτουργία διαχείρισης κρίσεων, η οποία, σε περίπτωση ενεργοποίησης των σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ ή των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ, καθορίζει, μεταξύ άλλων, σαφείς διαδικασίες για τη διαχείριση της εσωτερικής και εξωτερικής επικοινωνίας σε καταστάσεις κρίσης σύμφωνα με το άρθρο 14.

8. Οι χρηματοοικονομικές οντότητες τηρούν εύκολα προσβάσιμα αρχεία δραστηριοτήτων προ και κατά τη διάρκεια γεγονότων διαταραχής, όταν ενεργοποιούνται τα σχέδια επιχειρησιακής συνέχειας των ΤΠΕ και τα σχέδια αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ.

9. Τα κεντρικά αποθετήρια τίτλων παρέχουν στις αρμόδιες αρχές αντίγραφα των αποτελεσμάτων των δοκιμών επιχειρησιακής συνέχειας των ΤΠΕ ή παρόμοιων δραστηριοτήτων.

10. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, υποβάλλουν στις αρμόδιες αρχές, κατόπιν αιτήματός τους, εκτίμηση των συγκεντρωτικών ετήσιων δαπανών και ζημιών, οι οποίες προκαλούνται από μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ.

11. Σύμφωνα με το άρθρο 16 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010, οι ΕΕΑ, μέσω της μεικτής επιτροπής, καταρτίζουν έως τις 17 Ιουλίου 2024 κοινές κατευθυντήριες γραμμές για την εκτίμηση των συγκεντρωτικών ετήσιων δαπανών και ζημιών που αναφέρονται στην παράγραφο 10.

Άρθρο 12

Πολιτικές και διαδικασίες δημιουργίας εφεδρικών συστημάτων, διαδικασίες και μέθοδοι αποκατάστασης και ανάκτησης

1. Για τους σκοπούς της διασφάλισης της αποκατάστασης των συστημάτων και δεδομένων ΤΠΕ με ελάχιστο χρόνο διακοπής, με περιορισμό της διαταραχής και της ζημίας, στο πλαίσιο της οικείας διαχείρισης κινδύνων ΤΠΕ, οι χρηματοοικονομικές οντότητες καταρτίζουν και τεκμηριώνουν:

α) πολιτικές και διαδικασίες δημιουργίας εφεδρικών συστημάτων στις οποίες προσδιορίζεται το εύρος των δεδομένων που υπόκεινται σε εφεδρικά συστήματα και η ελάχιστη συχνότητα δημιουργίας αντιγράφων ασφαλείας, βάσει της κρισιμότητας των πληροφοριών ή του επιπέδου εμπιστευτικότητας των δεδομένων,

β) διαδικασίες και μεθόδους αποκατάστασης και ανάκτησης.

2. Οι χρηματοοικονομικές οντότητες δημιουργούν εφεδρικά συστήματα που μπορούν να ενεργοποιηθούν σύμφωνα με τις πολιτικές και τις διαδικασίες δημιουργίας εφεδρικών συστημάτων, καθώς και τις διαδικασίες και τις μεθόδους αποκατάστασης και ανάκτησης. Η ενεργοποίηση εφεδρικών συστημάτων δεν θέτει σε κίνδυνο την ασφάλεια των συστημάτων δικτύου και πληροφοριών ή τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων. Διενεργούνται περιοδικά δοκιμές των διαδικασιών δημιουργίας εφεδρικών συστημάτων και των διαδικασιών και μεθόδων αποκατάστασης και ανάκτησης.

3. Κατά την αποκατάσταση εφεδρικών δεδομένων με τη χρήση ιδίων συστημάτων, οι χρηματοοικονομικές οντότητες χρησιμοποιούν συστήματα ΤΠΕ που διαχωρίζονται φυσικά και λογικά από το σύστημα ΤΠΕ πηγής. Τα συστήματα ΤΠΕ προστατεύονται με ασφάλεια από κάθε μη εξουσιοδοτημένη πρόσβαση ή διαφθορά ΤΠΕ και επιτρέπουν την έγκαιρη αποκατάσταση των υπηρεσιών που χρησιμοποιούν τα εφεδρικά δεδομένα και συστήματα, ανάλογα με τις ανάγκες.

Για τους κεντρικούς αντισυμβαλλομένους, τα σχέδια αποκατάστασης επιτρέπουν την αποκατάσταση όλων των συναλλαγών κατά τον χρόνο της διαταραχής, ώστε ο κεντρικός αντισυμβαλλόμενος να είναι σε θέση να εξακολουθήσει να λειτουργεί με ασφάλεια και να ολοκληρώσει τον διακανονισμό κατά την προγραμματισμένη ημερομηνία.

Οι πάροχοι υπηρεσιών αναφοράς δεδομένων διατηρούν, επιπλέον, επαρκείς πόρους και διαθέτουν εφεδρικές εγκαταστάσεις και εγκαταστάσεις αποκατάστασης, προκειμένου να προσφέρουν και να διατηρούν τις υπηρεσίες τους ανά πάσα στιγμή.

4. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, διατηρούν εφεδρικές χωρητικότητες ΤΠΕ εξοπλισμένες με επαρκείς πόρους, ικανότητες και λειτουργίες για την κάλυψη των επιχειρηματικών αναγκών. Οι πολύ μικρές επιχειρήσεις αξιολογούν την ανάγκη διατήρησης αυτών των εφεδρικών χωρητικοτήτων ΤΠΕ με βάση το προφίλ κινδύνου τους.

5. Τα κεντρικά αποθετήρια τίτλων διατηρούν τουλάχιστον έναν δευτερεύοντα τόπο επεξεργασίας με επαρκείς πόρους, ικανότητες, λειτουργίες και στελέχωση για την κάλυψη των επιχειρηματικών αναγκών.

Ο δευτερεύων τόπος επεξεργασίας:

α) βρίσκεται σε γεωγραφική απόσταση από τον κύριο τόπο επεξεργασίας, ώστε να διασφαλίζεται ότι έχει διαφορετικό προφίλ κινδύνου και ώστε να μην είναι εφικτό να πληγεί από το ίδιο γεγονός που έχει επηρεάσει τον κύριο τόπο,

β) έχει την ικανότητα να διασφαλίζει την αδιάλειπτη λειτουργία κρίσιμων ή σημαντικών υπηρεσιών κατά πανομοιότυπο τρόπο με τον κύριο τόπο ή να παρέχει το απαιτούμενο επίπεδο υπηρεσιών ώστε να διασφαλίζεται ότι η χρηματοοικονομική οντότητα εκτελεί τις κρίσιμες δραστηριότητές της στο πλαίσιο των στόχων αποκατάστασης,

γ) είναι άμεσα προσβάσιμος από το προσωπικό της χρηματοοικονομικής οντότητας, ώστε να διασφαλίζεται η αδιάλειπτη λειτουργία κρίσιμων ή σημαντικών λειτουργιών σε περίπτωση που ο κύριος τόπος επεξεργασίας δεν είναι διαθέσιμος.

6. Κατά τον καθορισμό των στόχων ως προς τον χρόνο και το σημείο αποκατάστασης για κάθε λειτουργία, οι χρηματοοικονομικές οντότητες λαμβάνουν υπόψη αν πρόκειται για κρίσιμη ή σημαντική λειτουργία και τον δυνητικό συνολικό αντίκτυπο στην αποδοτικότητα της αγοράς. Οι εν λόγω στόχοι ως προς τον χρόνο διασφαλίζουν ότι, σε ακραία σενάρια, πληρούνται τα συμφωνημένα επίπεδα εξυπηρέτησης.

7. Κατά την αποκατάσταση λειτουργίας μετά από συμβάν που σχετίζεται με τις ΤΠΕ, οι χρηματοοικονομικές οντότητες διενεργούν τους απαραίτητους ελέγχους, συμπεριλαμβανομένων οποιωνδήποτε πολλαπλών ελέγχων και συμφωνιών, προκειμένου να διασφαλίσουν ότι η ακεραιότητα των δεδομένων διατηρείται στο ανώτατο επίπεδο. Οι έλεγχοι αυτοί διενεργούνται επίσης κατά την ανακατασκευή δεδομένων από εξωτερικούς συμφεροντούχους, ώστε να διασφαλίζεται η συνεκτικότητα όλων των δεδομένων μεταξύ των συστημάτων.

Άρθρο 13

Εκπαίδευση και εξέλιξη

1. Οι χρηματοοικονομικές οντότητες διαθέτουν ικανότητες και προσωπικό για τη συλλογή πληροφοριών σχετικά με τις ευπάθειες και τις κυβερνοαπειλές, τα συμβάντα που σχετίζονται με τις ΤΠΕ, ιδίως όσον αφορά τις κυβερνοεπιθέσεις, και για την ανάλυση των πιθανών επιπτώσεών τους στην ψηφιακή επιχειρησιακή τους ανθεκτικότητα.

2. Οι χρηματοοικονομικές οντότητες προβαίνουν σε επανεξετάσεις κατόπιν συμβάντων που σχετίζονται με τις ΤΠΕ, αφότου μείζον συμβάν που σχετίζεται με τις ΤΠΕ διαταράσσει τις βασικές τους δραστηριότητες, αναλύοντας τα αίτια της διαταραχής και προσδιορίζοντας τις βελτιώσεις που απαιτούνται στις λειτουργίες των ΤΠΕ ή στο πλαίσιο της πολιτικής επιχειρησιακής συνέχειας των ΤΠΕ, όπως αναφέρεται στο άρθρο 11.

Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, κοινοποιούν στις αρμόδιες αρχές, κατόπιν αιτήματος, τις αλλαγές που εφαρμόστηκαν μετά τις επανεξετάσεις κατόπιν συμβάντων που σχετίζονται με τις ΤΠΕ, όπως αναφέρεται στο πρώτο εδάφιο.

Οι επανεξετάσεις κατόπιν συμβάντων που σχετίζονται με τις ΤΠΕ, που αναφέρονται στο πρώτο εδάφιο, εξακριβώνουν αν τηρήθηκαν οι καθιερωμένες διαδικασίες και αν τα μέτρα που έχουν ληφθεί ήταν αποτελεσματικά, μεταξύ άλλων σε σχέση με τα εξής:

α) την ταχύτητα αντίδρασης σε ειδοποιήσεις ασφάλειας και προσδιορισμού των επιπτώσεων και της σοβαρότητας των συμβάντων που σχετίζονται με τις ΤΠΕ,

β) την ποιότητα και την ταχύτητα διενέργειας εγκληματολογικής ανάλυσης, εφόσον κρίνεται σκόπιμο,

γ) την αποτελεσματικότητα της παραπομπής του συμβάντος στο κατάλληλο επίπεδο εντός της χρηματοοικονομικής οντότητας,

δ) την αποτελεσματικότητα της εσωτερικής και εξωτερικής επικοινωνίας.

3. Τα διδάγματα που αντλούνται τόσο από τις δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας που πραγματοποιούνται σύμφωνα με τα άρθρα 26 και 27 όσο και από πραγματικά συμβάντα που σχετίζονται με τις ΤΠΕ, ιδίως κυβερνοεπιθέσεις, μαζί με τις προκλήσεις που αντιμετωπίστηκαν κατά την ενεργοποίηση σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ και σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ, σε συνδυασμό με τις σχετικές πληροφορίες που ανταλλάσσονται με αντισυμβαλλομένους και αξιολογούνται κατά τη διάρκεια εποπτικών ελέγχων, ενσωματώνονται δεόντως, σε διαρκή βάση, στη διαδικασία αξιολόγησης κινδύνων ΤΠΕ. Τα εν λόγω ευρήματα αποτελούν τη βάση για τη δέουσα επανεξέταση των συναφών συνιστωσών του πλαισίου διαχείρισης κινδύνων ΤΠΕ, όπως αναφέρεται στο άρθρο 6 παράγραφος 1.

4. Οι χρηματοοικονομικές οντότητες παρακολουθούν την αποτελεσματικότητα της εφαρμογής της στρατηγικής τους για την ψηφιακή επιχειρησιακή ανθεκτικότητα που καθορίζεται στο άρθρο 6 παράγραφος 8. Χαρτογραφούν την εξέλιξη των κινδύνων ΤΠΕ με την πάροδο του χρόνου, αναλύουν τη συχνότητα, τα είδη, το μέγεθος και την εξέλιξη των συμβάντων που σχετίζονται με τις ΤΠΕ, ιδίως όσον αφορά τις κυβερνοεπιθέσεις και τις πρακτικές που ακολουθούν, με σκοπό να κατανοήσουν το επίπεδο έκθεσης σε κινδύνους ΤΠΕ, ιδίως όσον αφορά κρίσιμες ή σημαντικές λειτουργίες, και να ενισχύσουν τα επίπεδα ωριμότητας και ετοιμότητας της χρηματοοικονομικής οντότητας στον κυβερνοχώρο.

5. Τα ανώτερα στελέχη ΤΠΕ υποβάλλουν στο διοικητικό όργανο έκθεση, τουλάχιστον σε ετήσια βάση, σχετικά με τα ευρήματα που αναφέρονται στην παράγραφο 3 και διατυπώνουν συστάσεις.

6. Οι χρηματοοικονομικές οντότητες αναπτύσσουν προγράμματα ευαισθητοποίησης σε θέματα ασφάλειας των ΤΠΕ και προγράμματα κατάρτισης για την ψηφιακή επιχειρησιακή ανθεκτικότητα ως υποχρεωτικές ενότητες των προγραμμάτων κατάρτισης του προσωπικού τους. Τα εν λόγω προγράμματα και καταρτίσεις ισχύουν για όλους τους υπαλλήλους και τα ανώτερα διοικητικά στελέχη και έχουν επίπεδο πολυπλοκότητας ανάλογο προς το αντικείμενο των καθηκόντων τους. Κατά περίπτωση, οι χρηματοοικονομικές οντότητες περιλαμβάνουν επίσης τρίτους παρόχους υπηρεσιών ΤΠΕ στα σχετικά προγράμματα κατάρτισής τους σύμφωνα με το άρθρο 30 παράγραφος 2 στοιχείο θ).

7. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, παρακολουθούν τις σχετικές τεχνολογικές εξελίξεις σε διαρκή βάση, με σκοπό επίσης την κατανόηση των πιθανών επιπτώσεων της ανάπτυξης νέων τεχνολογιών αυτού του είδους στις απαιτήσεις ασφάλειας των ΤΠΕ και στην ψηφιακή επιχειρησιακή ανθεκτικότητα. Ενημερώνονται για τις πρόσφατες διαδικασίες διαχείρισης κινδύνων ΤΠΕ, ώστε να καταπολεμούνται αποτελεσματικά οι τρέχουσες ή νέες μορφές κυβερνοεπιθέσεων.

Άρθρο 14

Επικοινωνία

1. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 6 παράγραφος 1, οι χρηματοοικονομικές οντότητες διαθέτουν σχέδια επικοινωνίας σε καταστάσεις κρίσης που καθιστούν δυνατή την υπεύθυνη γνωστοποίηση, τουλάχιστον, μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ ή ευπαθειών σε πελάτες και αντισυμβαλλομένους, καθώς και στο κοινό, ανάλογα με την περίπτωση.

2. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ, οι χρηματοοικονομικές οντότητες εφαρμόζουν πολιτικές επικοινωνίας που απευθύνονται στο εσωτερικό προσωπικό και σε εξωτερικούς συμφεροντούχους. Στις πολιτικές επικοινωνίας για το προσωπικό λαμβάνεται υπόψη η ανάγκη διαχωρισμού μεταξύ, αφενός, του προσωπικού που συμμετέχει στη διαχείριση κινδύνων ΤΠΕ, ιδίως του προσωπικού που είναι υπεύθυνο για την αντιμετώπιση και την ανάκαμψη, και, αφετέρου, του προσωπικού που πρέπει να ενημερωθεί.

3. Η αρμοδιότητα της εφαρμογής της στρατηγικής επικοινωνίας για συμβάντα που σχετίζονται με τις ΤΠΕ και της εκτέλεσης των καθηκόντων προς το κοινό και τα μέσα ενημέρωσης ανατίθεται τουλάχιστον σε ένα πρόσωπο της χρηματοοικονομικής οντότητας.

Άρθρο 15

Περαιτέρω εναρμόνιση των εργαλείων, μεθόδων, διαδικασιών και πολιτικών διαχείρισης κινδύνων ΤΠΕ

Οι ΕΕΑ, μέσω της μεικτής επιτροπής, σε συνεννόηση με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), καταρτίζουν κοινά σχέδια ρυθμιστικών τεχνικών προτύπων, προκειμένου:

α) να προσδιορίσουν περαιτέρω στοιχεία που πρέπει να συμπεριλαμβάνονται στις πολιτικές, τις διαδικασίες, τα πρωτόκολλα και τα εργαλεία ασφάλειας των ΤΠΕ που αναφέρονται στο άρθρο 9 παράγραφος 2, ώστε να διασφαλίζεται η ασφάλεια των δικτύων, να παρέχεται η δυνατότητα επαρκών διασφαλίσεων έναντι εισβολών και κατάχρησης δεδομένων, να διατηρούνται η διαθεσιμότητα, η γνησιότητα, η ακεραιότητα και η εμπιστευτικότητα των δεδομένων, συμπεριλαμβανομένων των τεχνικών κρυπτογράφησης, και να εξασφαλίζεται η ακριβής και έγκαιρη διαβίβαση δεδομένων χωρίς σημαντικές διαταραχές και αδικαιολόγητες καθυστερήσεις,

β) να αναπτύξουν περαιτέρω συνιστώσες των δικλείδων ασφάλειας για τη διαχείριση δικαιωμάτων πρόσβασης, που αναφέρονται στο άρθρο 9 παράγραφος 4 στοιχείο γ), και της σχετικής πολιτικής ανθρώπινων πόρων που ορίζει τα δικαιώματα πρόσβασης, τις διαδικασίες για τη χορήγηση και την ανάκληση δικαιωμάτων, την παρακολούθηση ασυνήθιστων δραστηριοτήτων σε σχέση με τους κινδύνους ΤΠΕ μέσω κατάλληλων δεικτών, συμπεριλαμβανομένων των πρακτικών χρήσης του δικτύου, των ωρών, της δραστηριότητας ΤΠ και των μη αναγνωρίσιμων συσκευών,

γ) να αναπτύξουν περαιτέρω τους μηχανισμούς που προσδιορίζονται στο άρθρο 10 παράγραφος 1, παρέχοντας τη δυνατότητα έγκαιρου εντοπισμού ασυνήθιστων δραστηριοτήτων, και τα κριτήρια που καθορίζονται στο άρθρο 10 παράγραφος 2 ενεργοποιώντας διαδικασίες εντοπισμού και αντιμετώπισης συμβάντων που σχετίζονται με τις ΤΠΕ,

δ) να προσδιορίσουν περαιτέρω τις συνιστώσες της πολιτικής επιχειρησιακής συνέχειας των ΤΠΕ που αναφέρεται στο άρθρο 11 παράγραφος 1,

ε) να προσδιορίσουν περαιτέρω τις δοκιμές των σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ που αναφέρονται στο άρθρο 11 παράγραφος 6, με σκοπό να διασφαλίζεται ότι κατά τις εν λόγω δοκιμές λαμβάνονται δεόντως υπόψη σενάρια στα οποία η ποιότητα της παροχής κρίσιμης ή σημαντικής λειτουργίας επιδεινώνεται σε μη αποδεκτό επίπεδο ή αποτυγχάνει, καθώς και ότι εξετάζονται δεόντως οι πιθανές επιπτώσεις της αφερεγγυότητας ή άλλης αθέτησης υποχρεώσεων οποιουδήποτε σχετικού τρίτου παρόχου υπηρεσιών ΤΠΕ και, κατά περίπτωση, οι πολιτικοί κίνδυνοι στις αντίστοιχες δικαιοδοσίες των παρόχων,

στ) να προσδιορίσουν περαιτέρω τις συνιστώσες των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ που αναφέρονται στο άρθρο 11 παράγραφος 3,

ζ) να προσδιορίσουν περαιτέρω το περιεχόμενο και τη μορφή της έκθεσης σχετικά με την επανεξέταση του πλαισίου διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 6 παράγραφος 5.

Κατά την κατάρτιση των εν λόγω σχεδίων ρυθμιστικών τεχνικών προτύπων, οι ΕΕΑ λαμβάνουν υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου της χρηματοοικονομικής οντότητας, καθώς και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της, λαμβάνοντας δεόντως υπόψη τυχόν ειδικά χαρακτηριστικά που προκύπτουν από τη διακριτή φύση των δραστηριοτήτων σε διάφορους τομείς χρηματοοικονομικών υπηρεσιών.

Οι ΕΕΑ υποβάλλουν τα εν λόγω σχέδια ρυθμιστικών τεχνικών προτύπων στην Επιτροπή έως τις 17 Ιανουαρίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο, σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

Άρθρο 16

Απλουστευμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ

1. Τα άρθρα 5 έως 15 του παρόντος κανονισμού δεν εφαρμόζονται σε μικρές και μη διασυνδεδεμένες επιχειρήσεις επενδύσεων, ιδρύματα πληρωμών που εξαιρούνται δυνάμει της οδηγίας (ΕΕ) 2015/2366· ιδρύματα που εξαιρούνται δυνάμει της οδηγίας 2013/36/ΕΕ για τα οποία τα κράτη μέλη έχουν αποφασίσει να μην εφαρμόσουν την επιλογή που αναφέρεται στο άρθρο 2 παράγραφος 4 του παρόντος κανονισμού· ιδρύματα ηλεκτρονικού χρήματος που εξαιρούνται δυνάμει της οδηγίας 2009/110/ΕΚ· και μικρά ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών.

Με την επιφύλαξη του πρώτου εδαφίου, οι οντότητες που απαριθμούνται στο πρώτο εδάφιο:

α) θεσπίζουν και διατηρούν ένα άρτιο και τεκμηριωμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ, το οποίο περιγράφει λεπτομερώς τους μηχανισμούς και τα μέτρα που αποσκοπούν στην ταχεία, αποτελεσματική και ολοκληρωμένη διαχείριση των κινδύνων ΤΠΕ, μεταξύ άλλων για την προστασία των σχετικών υλικών συνιστωσών και υποδομών,

β) παρακολουθούν συνεχώς την ασφάλεια και τη λειτουργία όλων των συστημάτων ΤΠΕ,

γ) ελαχιστοποιούν τον αντίκτυπο των κινδύνων ΤΠΕ μέσω της χρήσης ορθών, ανθεκτικών και επικαιροποιημένων συστημάτων, πρωτοκόλλων και εργαλείων ΤΠΕ, τα οποία είναι κατάλληλα για την υποστήριξη της εκτέλεσης των δραστηριοτήτων τους και της παροχής υπηρεσιών και προστατεύουν επαρκώς τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων στα συστήματα δικτύου και πληροφοριών,

δ) επιτρέπουν τον άμεσο εντοπισμό και την ανίχνευση πηγών κινδύνων και ανωμαλιών ΤΠΕ στα δικτυακά και πληροφοριακά συστήματα και τον άμεσο χειρισμό συμβάντων ΤΠΕ,

ε) εντοπίζουν βασικές εξαρτήσεις από τρίτους παρόχους υπηρεσιών ΤΠΕ,

στ) διασφαλίζουν τη συνέχεια κρίσιμων ή σημαντικών λειτουργιών, μέσω σχεδίων επιχειρησιακής συνέχειας και μέτρων αντιμετώπισης και ανάκαμψης, τα οποία περιλαμβάνουν, τουλάχιστον, μέτρα υποστήριξης και αποκατάστασης,

ζ) δοκιμάζουν, σε τακτική βάση, τα σχέδια και τα μέτρα που αναφέρονται στο στοιχείο στ), καθώς και την αποτελεσματικότητα των ελέγχων που υλοποιούνται σύμφωνα με τα στοιχεία α) και γ),

η) εφαρμόζουν, κατά περίπτωση, τα σχετικά επιχειρησιακά συμπεράσματα που προκύπτουν από τις δοκιμές οι οποίες αναφέρονται στο στοιχείο ζ) και από την ανάλυση κατόπιν συμβάντος στη διαδικασία αξιολόγησης κινδύνων ΤΠΕ και καταρτίζουν, σύμφωνα με τις ανάγκες και το προφίλ κινδύνου ΤΠΕ, προγράμματα ευαισθητοποίησης σε θέματα ασφάλειας των ΤΠΕ και προγράμματα κατάρτισης για την ψηφιακή επιχειρησιακή ανθεκτικότητα για το προσωπικό και τη διοίκηση στον τομέα της ασφάλειας ΤΠΕ.

2. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στην παράγραφο 1 δεύτερο εδάφιο στοιχείο α) τεκμηριώνεται και επανεξετάζεται περιοδικά και σε περίπτωση εκδήλωσης μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ σύμφωνα με τις εποπτικές οδηγίες. Το πλαίσιο βελτιώνεται διαρκώς με βάση τα διδάγματα που αντλούνται από την εφαρμογή και την παρακολούθηση. Έκθεση σχετικά με την επανεξέταση του πλαισίου διαχείρισης κινδύνων ΤΠΕ υποβάλλεται στην αρμόδια αρχή κατόπιν αιτήματός της.

3. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, σε συνεννόηση με τον ENISA, καταρτίζουν κοινά σχέδια ρυθμιστικών τεχνικών προτύπων προκειμένου:

α) να προσδιορίσουν περαιτέρω τα στοιχεία που πρέπει να περιλαμβάνονται στο πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στην παράγραφο 1 δεύτερο εδάφιο στοιχείο α),

β) να προσδιορίσουν περαιτέρω τα στοιχεία σε σχέση με τα συστήματα, τα πρωτόκολλα και τα εργαλεία για την ελαχιστοποίηση του αντικτύπου των κινδύνων ΤΠΕ που αναφέρεται στην παράγραφο 1 δεύτερο εδάφιο στοιχείο γ), με σκοπό τη διαφύλαξη της ασφάλειας των δικτύων, την παροχή επαρκών διασφαλίσεων έναντι εισβολών και κατάχρησης δεδομένων και τη διατήρηση της διαθεσιμότητας, της γνησιότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων,

γ) να προσδιορίσουν περαιτέρω τις συνιστώσες των σχεδίων επιχειρησιακής συνέχειας των ΤΠΕ που αναφέρονται στο άρθρο 1 δεύτερο εδάφιο στοιχείο στ),

δ) να προσδιορίσουν περαιτέρω τους κανόνες σχετικά με τη δοκιμή των σχεδίων επιχειρησιακής συνέχειας και να διασφαλίσουν την αποτελεσματικότητα των ελέγχων που αναφέρονται στην παράγραφο 1 δεύτερο εδάφιο στοιχείο ζ) και να διασφαλιστεί ότι οι εν λόγω δοκιμές λαμβάνουν δεόντως υπόψη σενάρια στα οποία η ποιότητα της παροχής μιας κρίσιμης ή σημαντικής λειτουργίας επιδεινώνεται σε μη αποδεκτό επίπεδο ή αποτυγχάνει,

ε) να προσδιορίσουν περαιτέρω το περιεχόμενο και τη μορφή της ετήσιας έκθεσης σχετικά με την επανεξέταση του πλαισίου διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στην παράγραφο 2.

Κατά την κατάρτιση των εν λόγω σχεδίων ρυθμιστικών τεχνικών προτύπων, οι ΕΕΑ λαμβάνουν υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου της χρηματοοικονομικής οντότητας και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της.

Οι ΕΕΑ υποβάλλουν τα εν λόγω σχέδια ρυθμιστικών τεχνικών προτύπων στην Επιτροπή έως τις 17 Ιανουαρίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο, σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

ΚΕΦΑΛΑΙΟ III

Διαχείριση, ταξινόμηση και αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ

Άρθρο 17

Διαδικασία διαχείρισης συμβάντων που σχετίζονται με τις ΤΠΕ

1. Οι χρηματοοικονομικές οντότητες ορίζουν, θεσπίζουν και εφαρμόζουν διαδικασία διαχείρισης συμβάντων που σχετίζονται με τις ΤΠΕ, με σκοπό τον εντοπισμό, τη διαχείριση και την κοινοποίηση συμβάντων που σχετίζονται με τις ΤΠΕ.

2. Οι χρηματοοικονομικές οντότητες καταγράφουν όλα τα συμβάντα που σχετίζονται με τις ΤΠΕ και τις σημαντικές κυβερνοαπειλές. Οι χρηματοοικονομικές οντότητες θεσπίζουν κατάλληλες διεργασίες και διαδικασίες για τη διασφάλιση συνεπούς και ολοκληρωμένου ελέγχου, χειρισμού και παρακολούθησης συμβάντων που σχετίζονται με τις ΤΠΕ, ώστε να εξασφαλιστεί ότι τα βαθύτερα αίτια προσδιορίζονται, τεκμηριώνονται και αντιμετωπίζονται προκειμένου να προληφθεί η εκδήλωση τέτοιων συμβάντων.

3. Η διαδικασία διαχείρισης συμβάντων που σχετίζονται με τις ΤΠΕ που αναφέρεται στην παράγραφο 1:

α) θέτει σε εφαρμογή δείκτες έγκαιρης προειδοποίησης,

β) καθιερώνει διαδικασίες για τον προσδιορισμό, την ανίχνευση, την καταγραφή, την κατηγοριοποίηση και την ταξινόμηση συμβάντων που σχετίζονται με τις ΤΠΕ ανάλογα με την προτεραιότητα και τη σοβαρότητά τους, και την κρισιμότητα των υπηρεσιών που επηρεάζονται, σύμφωνα με τα κριτήρια που καθορίζονται στο άρθρο 18 παράγραφος 1,

γ) αναθέτει ρόλους και αρμοδιότητες που πρέπει να ενεργοποιηθούν για διάφορα είδη και σενάρια συμβάντων που σχετίζονται με τις ΤΠΕ,

δ) καθορίζει σχέδια για την επικοινωνία με το προσωπικό, τους εκτός οντότητας συμφεροντούχους και τα μέσα ενημέρωσης, σύμφωνα με το άρθρο 14, και για την κοινοποίηση σε πελάτες, για εσωτερικές διαδικασίες παραπομπής συμβάντων στο κατάλληλο επίπεδο, συμπεριλαμβανομένων καταγγελιών πελατών που αφορούν τις ΤΠΕ, καθώς και για την παροχή πληροφοριών σε χρηματοοικονομικές οντότητες που ενεργούν ως αντισυμβαλλόμενοι, ανάλογα με την περίπτωση,

ε) διασφαλίζει ότι τουλάχιστον τα μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ αναφέρονται στα αρμόδια ανώτερα διοικητικά στελέχη και ότι το διοικητικό όργανο τηρείται ενήμερο τουλάχιστον για τα μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ, επεξηγώντας τις επιπτώσεις, την αντιμετώπιση και τις πρόσθετες δικλείδες ασφάλειας που πρέπει να καθοριστούν ως αποτέλεσμα τέτοιων συμβάντων που σχετίζονται με τις ΤΠΕ,

στ) καθιερώνει διαδικασίες αντιμετώπισης συμβάντων που σχετίζονται με τις ΤΠΕ για να μετριαστούν οι επιπτώσεις και να διασφαλιστεί ότι οι υπηρεσίες καθίστανται εγκαίρως λειτουργικές και ασφαλείς.

Άρθρο 18

Ταξινόμηση συμβάντων που σχετίζονται με τις ΤΠΕ και κυβερνοαπειλών

1. Οι χρηματοοικονομικές οντότητες ταξινομούν τα συμβάντα που σχετίζονται με τις ΤΠΕ και προσδιορίζουν τις επιπτώσεις τους με βάση τα ακόλουθα κριτήρια:

α) τον αριθμό και/ή τη συνάφεια των επηρεαζόμενων πελατών ή χρηματοοικονομικών αντισυμβαλλομένων και, κατά περίπτωση, το ύψος ή τον αριθμό των συναλλαγών που επηρεάζονται από τη διαταραχή που προκλήθηκε από το συμβάν που σχετίζεται με τις ΤΠΕ, και κατά πόσο το εν λόγω συμβάν έχει επιπτώσεις στη φήμη,

β) τη διάρκεια του συμβάντος που σχετίζεται με τις ΤΠΕ, συμπεριλαμβανομένου του χρόνου διακοπής της υπηρεσίας,

γ) τη γεωγραφική εξάπλωση των περιοχών που επηρεάζονται από το συμβάν που σχετίζεται με τις ΤΠΕ, ιδίως εάν επηρεάζει περισσότερα από δύο κράτη μέλη,

δ) τις απώλειες δεδομένων που συνεπάγεται το συμβάν που σχετίζεται με τις ΤΠΕ, όσον αφορά τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων,

ε) την κρισιμότητα των επηρεαζόμενων υπηρεσιών, συμπεριλαμβανομένων των συναλλαγών και των δραστηριοτήτων της χρηματοοικονομικής οντότητας,

στ) τις οικονομικές επιπτώσεις, ιδίως τις άμεσες και έμμεσες δαπάνες και απώλειες, του συμβάντος που σχετίζεται με τις ΤΠΕ σε απόλυτους και σχετικούς όρους.

2. Οι χρηματοοικονομικές οντότητες ταξινομούν τις κυβερνοαπειλές ως σημαντικές με βάση την κρισιμότητα των υπηρεσιών που διατρέχουν κίνδυνο, συμπεριλαμβανομένων των συναλλαγών και των δραστηριοτήτων της χρηματοοικονομικής οντότητας, του αριθμού και/ή της συνάφειας των στοχευόμενων πελατών ή χρηματοοικονομικών αντισυμβαλλομένων και της γεωγραφικής εξάπλωσης των περιοχών που διατρέχουν κίνδυνο.

3. Οι ΕΕΑ, μέσω της μεικτής επιτροπής των ΕΕΑ και σε συνεννόηση με την ΕΚΤ και τον ENISA, καταρτίζουν κοινά σχέδια ρυθμιστικών τεχνικών προτύπων, προκειμένου να προσδιορίσουν περαιτέρω τα εξής:

α) τα κριτήρια που καθορίζονται στην παράγραφο 1, συμπεριλαμβανομένων κατώτατων ορίων σημαντικότητας για τον προσδιορισμό μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ ή, κατά περίπτωση, μειζόνων λειτουργικών συμβάντων ή συμβάντων ασφάλειας που σχετίζονται με πληρωμές, τα οποία υπόκεινται στην υποχρέωση αναφοράς που προβλέπεται στο άρθρο 19 παράγραφος 1,

β) τα κριτήρια που πρέπει να εφαρμόζουν οι αρμόδιες αρχές για την αξιολόγηση της συνάφειας μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ ή, κατά περίπτωση, μειζόνων λειτουργικών συμβάντων ή συμβάντων ασφάλειας που σχετίζονται με πληρωμές στις σχετικές αρμόδιες αρχές σε άλλα κράτη μέλη, καθώς και τα στοιχεία των αναφορών μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ ή, κατά περίπτωση, μειζόνων λειτουργικών συμβάντων ή συμβάντων ασφάλειας που σχετίζονται με πληρωμές, τα οποία πρέπει να κοινοποιούνται σε άλλες αρμόδιες αρχές σύμφωνα με το άρθρο 19 παράγραφοι 6 και 7,

γ) τα κριτήρια που καθορίζονται στην παράγραφο 2 του παρόντος άρθρου, συμπεριλαμβανομένων των κατώτατων ορίων υψηλής σημαντικότητας για τον προσδιορισμό σημαντικών κυβερνοαπειλών.

4. Κατά την κατάρτιση των κοινών σχεδίων ρυθμιστικών τεχνικών προτύπων που αναφέρονται στην παράγραφο 3 του παρόντος άρθρου, οι ΕΕΑ λαμβάνουν υπόψη τα κριτήρια που καθορίζονται στο άρθρο 4 παράγραφος 2 καθώς και τα διεθνή πρότυπα, τις κατευθυντήριες γραμμές και τις προδιαγραφές που αναπτύσσει και δημοσιεύει ο ENISA, συμπεριλαμβανομένων, κατά περίπτωση, των προδιαγραφών που ισχύουν για άλλους οικονομικούς τομείς. Για τους σκοπούς της εφαρμογής των κριτηρίων που καθορίζονται στο άρθρο 4 παράγραφος 2, οι ΕΕΑ λαμβάνουν δεόντως υπόψη την ανάγκη οι πολύ μικρές και οι μικρές και μεσαίες επιχειρήσεις να κινητοποιήσουν επαρκείς πόρους και ικανότητες για να διασφαλίσουν την ταχεία διαχείριση συμβάντων που σχετίζονται με τις ΤΠΕ.

Οι ΕΕΑ υποβάλλουν τα εν λόγω κοινά σχέδια ρυθμιστικών τεχνικών προτύπων στην Επιτροπή έως τις 17 Ιανουαρίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στην παράγραφο 3, σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

Άρθρο 19

Αναφορά μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ και προαιρετική κοινοποίηση σημαντικών κυβερνοαπειλών

1. Οι χρηματοοικονομικές οντότητες αναφέρουν στην αρμόδια αρχή μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ, όπως ορίζεται στο άρθρο 46, σύμφωνα με την παράγραφο 4 του παρόντος άρθρου.

Όταν μια χρηματοοικονομική οντότητα υπόκειται σε εποπτεία από περισσότερες από μία εθνικές αρμόδιες αρχές, οι οποίες αναφέρονται στο άρθρο 46, τα κράτη μέλη ορίζουν ενιαία αρμόδια αρχή ως τη σχετική αρμόδια αρχή που είναι υπεύθυνη για την εκτέλεση των λειτουργιών και των καθηκόντων που προβλέπονται στο παρόν άρθρο.

Τα πιστωτικά ιδρύματα που ταξινομούνται ως σημαντικά, σύμφωνα με το άρθρο 6 παράγραφος 4 του κανονισμού (ΕΕ) αριθ. 1024/2013, αναφέρουν μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ στη σχετική εθνική αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 4 της οδηγίας 2013/36/ΕΕ, η οποία διαβιβάζει αμέσως την εν λόγω αναφορά στην ΕΚΤ.

Για τους σκοπούς του πρώτου εδαφίου, οι χρηματοοικονομικές οντότητες, αφού συλλέξουν και αναλύσουν όλες τις σχετικές πληροφορίες, καταρτίζουν την αρχική κοινοποίηση και τις αναφορές που προβλέπονται στην παράγραφο 4 του παρόντος άρθρου, χρησιμοποιώντας τα υποδείγματα που αναφέρονται στο άρθρο 20, και τις υποβάλλουν στην αρμόδια αρχή. Σε περίπτωση που μια τεχνική αδυναμία εμποδίζει την υποβολή της αρχικής κοινοποίησης με τη χρήση του υποδείγματος, οι χρηματοοικονομικές οντότητες ενημερώνουν σχετικά την αρμόδια αρχή με εναλλακτικά μέσα.

Η αρχική κοινοποίηση και οι αναφορές που προβλέπονται στην παράγραφο 4 περιλαμβάνουν όλες τις απαραίτητες πληροφορίες προκειμένου η αρμόδια αρχή να είναι σε θέση να προσδιορίσει τη σημασία του μείζονος συμβάντος που σχετίζεται με τις ΤΠΕ και να προβεί σε εκτίμηση των πιθανών διασυνοριακών επιπτώσεων.

Με την επιφύλαξη των αναφορών σύμφωνα με το πρώτο εδάφιο από τη χρηματοοικονομική οντότητα στη σχετική αρμόδια αρχή, τα κράτη μέλη μπορούν επιπλέον να ορίζουν ότι ορισμένες ή όλες οι χρηματοοικονομικές οντότητες παρέχουν επίσης την αρχική κοινοποίηση και κάθε αναφορά που προβλέπεται στην παράγραφο 4 του παρόντος άρθρου, χρησιμοποιώντας τα υποδείγματα που αναφέρονται στο άρθρο 20, στις αρμόδιες αρχές ή στις ομάδες αντιμετώπισης συμβάντων ασφάλειας σε υπολογιστές (CSIRT) που έχουν οριστεί ή συσταθεί σύμφωνα με την οδηγία (ΕΕ) 2022/2555

2. Οι χρηματοοικονομικές οντότητες μπορούν, σε προαιρετική βάση, να κοινοποιούν σημαντικές κυβερνοαπειλές στη σχετική αρμόδια αρχή όταν θεωρούν ότι η απειλή είναι σημαντική για το χρηματοοικονομικό σύστημα, τους χρήστες υπηρεσιών ή τους πελάτες. Η σχετική αρμόδια αρχή μπορεί να παρέχει τις πληροφορίες αυτές σε άλλες σχετικές αρχές που αναφέρονται στην παράγραφο 6.

Τα πιστωτικά ιδρύματα που ταξινομούνται ως σημαντικά, σύμφωνα με το άρθρο 6 παράγραφος 4 του κανονισμού (ΕΕ) αριθ. 1024/2013, μπορούν, σε προαιρετική βάση, να κοινοποιούν σημαντικές κυβερνοαπειλές στη σχετική εθνική αρμόδια αρχή, η οποία έχει οριστεί σύμφωνα με το άρθρο 4 της οδηγίας 2013/36/ΕΕ, και η οποία διαβιβάζει αμέσως την κοινοποίηση στην ΕΚΤ.

Τα κράτη μέλη μπορούν να ορίζουν ότι οι χρηματοοικονομικές οντότητες που κοινοποιούν σε προαιρετική βάση σύμφωνα με το πρώτο εδάφιο μπορούν επίσης να διαβιβάζουν την εν λόγω κοινοποίηση στις CSIRT που ορίζονται ή συστήνονται σύμφωνα με ην οδηγία (ΕΕ) 2022/2555

3. Κατά την εκδήλωση μείζονος συμβάντος, το οποίο σχετίζεται με τις ΤΠΕ και έχει επιπτώσεις στα οικονομικά συμφέροντα των πελατών, οι χρηματοοικονομικές οντότητες ενημερώνουν, χωρίς αδικαιολόγητη καθυστέρηση, αφού λάβουν γνώση του συμβάντος, τους πελάτες όσον αφορά το μείζον συμβάν που σχετίζεται με τις ΤΠΕ και σχετικά με τα μέτρα που έχουν ληφθεί για τον περιορισμό των δυσμενών επιπτώσεων του εν λόγω συμβάντος.

Σε περίπτωση σημαντικής κυβερνοαπειλής, οι χρηματοοικονομικές οντότητες ενημερώνουν, κατά περίπτωση, τους πελάτες τους που ενδέχεται να επηρεαστούν σχετικά με τυχόν κατάλληλα μέτρα προστασίας τα οποία ενδέχεται να εξετάσουν οι τελευταίοι.

4. Οι χρηματοοικονομικές οντότητες, εντός των προθεσμιών που καθορίζονται σύμφωνα με το άρθρο 20 πρώτο εδάφιο στοιχείο α) σημείο ii), υποβάλλουν τα ακόλουθα στη σχετική αρμόδια αρχή:

α) αρχική κοινοποίηση,

β) ενδιάμεση αναφορά μετά την αρχική κοινοποίηση που αναφέρεται στο στοιχείο α), αμέσως μόλις μεταβληθεί σημαντικά η κατάσταση του αρχικού συμβάντος ή μεταβληθεί ο χειρισμός του μείζονος συμβάντος που σχετίζεται με τις ΤΠΕ βάσει νέων διαθέσιμων πληροφοριών, ακολουθούμενη, κατά περίπτωση, από επικαιροποιημένες κοινοποιήσεις κάθε φορά που είναι διαθέσιμη σχετική επικαιροποίηση της κατάστασης, καθώς και κατόπιν συγκεκριμένου αιτήματος της αρμόδιας αρχής,

γ) τελική αναφορά, όταν ολοκληρωθεί η ανάλυση των βαθύτερων αιτίων, ανεξάρτητα από το αν έχουν ήδη εφαρμοστεί μέτρα μετριασμού, και όταν είναι διαθέσιμα τα στοιχεία των πραγματικών επιπτώσεων προς αντικατάσταση των εκτιμήσεων.

5. Οι χρηματοοικονομικές οντότητες μπορούν να αναθέτουν, σύμφωνα με το ενωσιακό και εθνικό τομεακό δίκαιο, τις υποχρεώσεις αναφοράς που προβλέπονται στο παρόν άρθρο σε τρίτο πάροχο υπηρεσιών. Σε περίπτωση τέτοιας εξωτερικής ανάθεσης, η χρηματοοικονομική οντότητα παραμένει εξολοκλήρου υπεύθυνη για την εκπλήρωση των απαιτήσεων αναφοράς συμβάντων.

6. Μετά την παραλαβή της αρχικής κοινοποίησης και κάθε αναφοράς που προβλέπεται στην παράγραφο 4, η αρμόδια αρχή παρέχει εγκαίρως λεπτομερή στοιχεία για το μείζον συμβάν που σχετίζεται με τις ΤΠΕ στους ακόλουθους αποδέκτες με βάση, κατά περίπτωση, τις αντίστοιχες αρμοδιότητές τους:

α) στην ΕΑΤ, στην ΕΑΚΑΑ ή στην ΕΑΑΕΣ,

β) στην ΕΚΤ, στην περίπτωση των χρηματοοικονομικών οντοτήτων που αναφέρονται στο άρθρο 2 παράγραφος 1 στοιχεία α), β) και δ),

γ) στις αρμόδιες αρχές, στα ενιαία σημεία επαφής ή στις CSIRT που έχουν οριστεί ή συσταθεί, σύμφωνα με την οδηγία (ΕΕ) 2022/2555

δ) στις αρχές εξυγίανσης, όπως αναφέρονται στο άρθρο 3 της οδηγίας 2014/59/ΕΕ, και στο Ενιαίο Συμβούλιο Εξυγίανσης (ΕΣΕ) όσον αφορά τις οντότητες που αναφέρονται στο άρθρο 7 παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 806/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([37]), και όσον αφορά τις οντότητες και τους ομίλους που αναφέρονται στο άρθρο 7 παράγραφος 4 στοιχείο β) και στο άρθρο 7 παράγραφος 5 του κανονισμού (ΕΕ) αριθ. 806/2014, εάν οι λεπτομέρειες αυτές αφορούν συμβάντα που ενέχουν κίνδυνο για τη διασφάλιση κρίσιμων λειτουργιών κατά την έννοια του άρθρου 2 παράγραφος 1 σημείο 35) της οδηγίας 2014/59/ΕΕ, και

ε) σε άλλες αρμόδιες δημόσιες αρχές βάσει του εθνικού δικαίου.

7. Μετά την παραλαβή των πληροφοριών σύμφωνα με την παράγραφο 6, η ΕΑΤ, η ΕΑΚΑΑ ή η ΕΑΑΕΣ και η ΕΚΤ, σε συνεννόηση με τον ENISA και σε συνεργασία με τη σχετική αρμόδια αρχή, αξιολογούν αν το μείζον συμβάν που σχετίζεται με τις ΤΠΕ έχει ενδιαφέρον για τις αρμόδιες αρχές σε άλλα κράτη μέλη. Μετά την εν λόγω αξιολόγηση, η ΕΑΤ, η ΕΑΚΑΑ ή η ΕΑΑΕΣ ενημερώνουν σχετικά, το συντομότερο δυνατόν, τις σχετικές αρμόδιες αρχές άλλων κρατών μελών. Η ΕΚΤ ενημερώνει τα μέλη του Ευρωπαϊκού Συστήματος Κεντρικών Τραπεζών για θέματα που σχετίζονται με το σύστημα πληρωμών. Βάσει της εν λόγω ενημέρωσης, οι αρμόδιες αρχές λαμβάνουν, κατά περίπτωση, όλα τα αναγκαία μέτρα για την προστασία της άμεσης σταθερότητας του χρηματοοικονομικού συστήματος.

([37]) Κανονισμός (ΕΕ) αριθ. 806/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Ιουλίου 2014, περί θεσπίσεως ενιαίων κανόνων και διαδικασίας για την εξυγίανση πιστωτικών ιδρυμάτων και ορισμένων επιχειρήσεων επενδύσεων στο πλαίσιο ενός Ενιαίου Μηχανισμού Εξυγίανσης και ενός Ενιαίου Ταμείου Εξυγίανσης και τροποποιήσεως του κανονισμού (ΕΕ) αριθ. 1093/2010 (ΕΕ L 225 της 30.7.2014, σ. 1).

8. Η κοινοποίηση που πρέπει να γίνει από την ΕΑΚΑΑ σύμφωνα με την παράγραφο 7 του παρόντος άρθρου δεν θίγει την ευθύνη της αρμόδιας αρχής να διαβιβάζει επειγόντως τις λεπτομέρειες του μείζονος συμβάντος που σχετίζεται με τις ΤΠΕ στη σχετική αρχή του κράτους μέλους υποδοχής, όταν ένα κεντρικό αποθετήριο τίτλων ασκεί σημαντική διασυνοριακή δραστηριότητα στο κράτος μέλος υποδοχής, το μείζον συμβάν που σχετίζεται με τις ΤΠΕ είναι πιθανό να έχει σοβαρές επιπτώσεις στις χρηματοοικονομικές αγορές του κράτους μέλους υποδοχής και όταν υπάρχουν ρυθμίσεις συνεργασίας μεταξύ των αρμόδιων αρχών σχετικά με την εποπτεία των χρηματοοικονομικών οντοτήτων.

Άρθρο 20

Εναρμόνιση του περιεχομένου και των υποδειγμάτων των αναφορών

Οι ΕΕΑ, μέσω της μεικτής επιτροπής και σε συνεννόηση με τον ENISA και την ΕΚΤ, καταρτίζουν:

α) κοινά σχέδια ρυθμιστικών τεχνικών προτύπων προκειμένου:

i) καθορίζουν το περιεχόμενο των αναφορών για μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ, ώστε να αντικατοπτρίζει τα κριτήρια του άρθρου 18 παράγραφος 1 και να ενσωματώνει περαιτέρω στοιχεία, όπως λεπτομέρειες για τον προσδιορισμό της συνάφειας της υποβολής εκθέσεων για άλλα κράτη μέλη και του αν πρόκειται ή όχι για μείζον λειτουργικό συμβάν ή συμβάν ασφάλειας που σχετίζεται με πληρωμές,

ii) καθορίζουν τις προθεσμίες για την αρχική κοινοποίηση και για κάθε αναφορά που προβλέπεται στο άρθρο 19 παράγραφος 4,

iii) καθορίζουν το περιεχόμενο της κοινοποίησης για σημαντικές κυβερνοαπειλές.

Κατά την κατάρτιση των εν λόγω σχεδίων ρυθμιστικών τεχνικών προτύπων, οι ΕΕΑ λαμβάνουν υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου της χρηματοοικονομικής οντότητας, και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της, και ιδίως προκειμένου να διασφαλιστεί ότι, για τους σκοπούς του σημείου ii) του στοιχείου α) του παρόντος εδαφίου, διαφορετικές προθεσμίες μπορούν να αντικατοπτρίζουν, κατά περίπτωση, τις ιδιαιτερότητες των χρηματοοικονομικών τομέων, με την επιφύλαξη της διατήρησης συνεκτικής προσέγγισης για την αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ σύμφωνα με τον παρόντα κανονισμό και την οδηγία (ΕΕ) 2022/2555 Οι ΕΕΑ παρέχουν, κατά περίπτωση, αιτιολόγηση όταν αποκλίνουν από τις προσεγγίσεις που υιοθετούνται στο πλαίσιο της εν λόγω οδηγίας,

β) κοινά σχέδια εκτελεστικών τεχνικών προτύπων με σκοπό τη δημιουργία τυποποιημένων εντύπων, υποδειγμάτων και διαδικασιών για την αναφορά μείζονος συμβάντος που σχετίζεται με τις ΤΠΕ και την κοινοποίηση σημαντικής κυβερνοαπειλής από τις χρηματοοικονομικές οντότητες.

Οι ΕΕΑ υποβάλλουν στην Επιτροπή τα κοινά σχέδια ρυθμιστικών τεχνικών προτύπων που αναφέρονται στο πρώτο εδάφιο στοιχείο α) και τα κοινά σχέδια εκτελεστικών τεχνικών προτύπων που αναφέρονται στο πρώτο εδάφιο στοιχείο β) στην Επιτροπή έως τις 17 Ιουλίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα κοινά ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο στοιχείο α), σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

Ανατίθεται στην Επιτροπή η εξουσία να εγκρίνει τα κοινά εκτελεστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο στοιχείο β), σύμφωνα με το άρθρο 15 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

Άρθρο 21

Κεντρική διαχείριση της αναφοράς μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ

1. Οι ΕΕΑ, μέσω της μεικτής επιτροπής και σε συνεννόηση με την ΕΚΤ και τον ENISA, καταρτίζουν κοινή έκθεση στην οποία αξιολογείται η σκοπιμότητα περαιτέρω συγκέντρωσης της αναφοράς συμβάντων μέσω της δημιουργίας ενός ενιαίου κόμβου της ΕΕ για την αναφορά μείζονος συμβάντος που σχετίζεται με τις ΤΠΕ από τις χρηματοοικονομικές οντότητες. Στην κοινή έκθεση εξετάζονται πιθανοί τρόποι για τη διευκόλυνση της ροής των αναφορών συμβάντων που σχετίζονται με τις ΤΠΕ, τη μείωση των σχετικών δαπανών και τη στήριξη θεματικών αναλύσεων με στόχο την ενίσχυση της εποπτικής σύγκλισης.

2. Στην κοινή έκθεση που αναφέρεται στην παράγραφο 1 περιλαμβάνονται τουλάχιστον τα εξής στοιχεία:

α) προϋποθέσεις για τη δημιουργία ενιαίου κόμβου της ΕΕ,

β) οφέλη, περιορισμοί και κίνδυνοι, συμπεριλαμβανομένων των κινδύνων που συνδέονται με την υψηλή συγκέντρωση ευαίσθητων πληροφοριών,

γ) η αναγκαία ικανότητα για τη διασφάλιση της διαλειτουργικότητας όσον αφορά άλλα σχετικά συστήματα αναφοράς,

δ) στοιχεία λειτουργικής διαχείρισης,

ε) όροι συμμετοχής,

στ) τεχνικές ρυθμίσεις για την πρόσβαση των χρηματοοικονομικών οντοτήτων και των εθνικών αρμόδιων αρχών στον ενιαίο κόμβο της ΕΕ,

ζ) προκαταρκτική αξιολόγηση του οικονομικού κόστους που προκύπτει από τη σύσταση της επιχειρησιακής πλατφόρμας για την υποστήριξη του ενιαίου κόμβου της ΕΕ, συμπεριλαμβανομένης της απαιτούμενης εμπειρογνωσίας.

3. Οι ΕΕΑ υποβάλλουν στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο και στην Επιτροπή την έκθεση που αναφέρεται στην παράγραφο 1 έως τις 17 Ιανουαρίου 2025.

Άρθρο 22

Εποπτικές παρατηρήσεις

1. Με την επιφύλαξη της τεχνικής συμβολής, των συμβουλών ή των διορθωτικών μέτρων και της επακόλουθης συνέχειας που μπορεί να δοθεί, κατά περίπτωση, σύμφωνα με το εθνικό δίκαιο, από τις CSIRT δυνάμει της οδηγίας (ΕΕ) 2022/2555 η αρμόδια αρχή, μόλις λάβει την αρχική κοινοποίηση και κάθε αναφορά, όπως προβλέπεται στο άρθρο 19 παράγραφος 4, επιβεβαιώνει την παραλαβή και μπορεί, όπου είναι εφικτό, να παρέχει εγκαίρως σχετικές και αναλογικές παρατηρήσεις ή κατευθυντήριες γραμμές υψηλού επιπέδου στη χρηματοοικονομική οντότητα, ιδίως καθιστώντας διαθέσιμες τυχόν σχετικές ανωνυμοποιημένες πληροφορίες και στοιχεία σχετικά με παρόμοιες απειλές, και μπορεί να συζητά τα διορθωτικά μέτρα που εφαρμόζονται στο επίπεδο της χρηματοοικονομικής οντότητας και τους τρόπους ελαχιστοποίησης και μετριασμού των δυσμενών επιπτώσεων σε ολόκληρο τον χρηματοοικονομικό τομέα. Με την επιφύλαξη των εποπτικών παρατηρήσεων που λαμβάνονται, οι χρηματοοικονομικές οντότητες παραμένουν πλήρως υπεύθυνες για τον χειρισμό και για τις συνέπειες των συμβάντων που σχετίζονται με τις ΤΠΕ και αναφέρονται σύμφωνα με το άρθρο 19 παράγραφος 1.

2. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, αναφέρουν ετησίως σε ανωνυμοποιημένη και συγκεντρωτική βάση τα μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ, των οποίων τα λεπτομερή στοιχεία παρέχονται από τις αρμόδιες αρχές σύμφωνα με το άρθρο 19 παράγραφος 6, εκθέτοντας τουλάχιστον τον αριθμό των μειζόνων συμβάντων που σχετίζονται με τις ΤΠΕ, τη φύση τους, τις επιπτώσεις τους στις λειτουργίες των χρηματοοικονομικών οντοτήτων ή των πελατών, τα διορθωτικά μέτρα που λήφθηκαν και τις δαπάνες που πραγματοποιήθηκαν.

Οι ΕΕΑ εκδίδουν προειδοποιήσεις και παράγουν στατιστικά στοιχεία υψηλού επιπέδου προς υποστήριξη των αξιολογήσεων των απειλών και των ευπαθειών για τις ΤΠΕ.

Άρθρο 23

Λειτουργικά συμβάντα ή συμβάντα ασφάλειας που σχετίζονται με πληρωμές, τα οποία αφορούν πιστωτικά ιδρύματα, ιδρύματα πληρωμών, παρόχους υπηρεσιών πληροφοριών λογαριασμού και ιδρύματα ηλεκτρονικού χρήματος

Οι απαιτήσεις που ορίζονται στο παρόν κεφάλαιο ισχύουν επίσης για λειτουργικά συμβάντα ή συμβάντα ασφάλειας που σχετίζονται με πληρωμές και για μείζονα λειτουργικά συμβάντα ή συμβάντα ασφάλειας που σχετίζονται με πληρωμές, όταν αφορούν πιστωτικά ιδρύματα, ιδρύματα πληρωμών, παρόχους υπηρεσιών πληροφοριών λογαριασμού και ιδρύματα ηλεκτρονικού χρήματος.

ΚΕΦΑΛΑΙΟ IV

Δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας

Άρθρο 24

Γενικές απαιτήσεις για τη διενέργεια δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας

1. Για τους σκοπούς της αξιολόγησης της ετοιμότητας όσον αφορά τον χειρισμό συμβάντων που σχετίζονται με τις ΤΠΕ, του εντοπισμού αδυναμιών, ελλείψεων και κενών στην ψηφιακή επιχειρησιακή ανθεκτικότητα, καθώς και της άμεσης εφαρμογής διορθωτικών μέτρων, οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, λαμβάνοντας υπόψη τα κριτήρια του άρθρου 4 παράγραφος 2, θεσπίζουν, διατηρούν και επανεξετάζουν ένα άρτιο και ολοκληρωμένο πρόγραμμα δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας ως αναπόσπαστο μέρος του πλαισίου διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 6.

2. Το πρόγραμμα δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας περιλαμβάνει σειρά αξιολογήσεων, δοκιμών, μεθοδολογιών, πρακτικών και εργαλείων που πρέπει να εφαρμόζονται σύμφωνα με τα άρθρα 25 και 26.

3. Κατά τη διεξαγωγή του προγράμματος δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου, οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, ακολουθούν προσέγγιση βάσει κινδύνου, λαμβάνοντας υπόψη τα κριτήρια που ορίζονται στο άρθρο 4 παράγραφος 2, συνεκτιμώντας δεόντως το εξελισσόμενο τοπίο του κινδύνου ΤΠΕ, τυχόν ειδικούς κινδύνους στους οποίους εκτίθεται ή ενδέχεται να εκτεθεί η συγκεκριμένη χρηματοοικονομική οντότητα, την κρισιμότητα των πληροφοριακών πόρων και των παρεχόμενων υπηρεσιών, καθώς και κάθε άλλο παράγοντα τον οποίο κρίνει κατάλληλο η χρηματοοικονομική οντότητα.

4. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, διασφαλίζουν ότι οι δοκιμές πραγματοποιούνται από ανεξάρτητους φορείς, εσωτερικούς ή εξωτερικούς. Όταν διενεργούνται δοκιμές από εσωτερικό δοκιμαστή, οι χρηματοοικονομικές οντότητες διαθέτουν επαρκείς πόρους και διασφαλίζουν την αποφυγή συγκρούσεων συμφερόντων καθ' όλη τη διάρκεια των φάσεων σχεδιασμού και εκτέλεσης της δοκιμής.

5. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, θεσπίζουν διαδικασίες και πολιτικές για την ιεράρχηση, την ταξινόμηση και την επίλυση όλων των ζητημάτων που ανακύπτουν κατά τη διενέργεια των δοκιμών, και καθιερώνουν εσωτερικές μεθοδολογίες επικύρωσης, ώστε να εξακριβώνεται ότι αντιμετωπίζονται πλήρως όλες οι αδυναμίες, οι ελλείψεις ή τα κενά που έχουν διαπιστωθεί.

6. Οι χρηματοοικονομικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, διασφαλίζουν τουλάχιστον ετησίως ότι διενεργούνται κατάλληλες δοκιμές σε όλα τα συστήματα και εφαρμογές ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες.

Άρθρο 25

Δοκιμές των εργαλείων και συστημάτων ΤΠΕ

1. Το πρόγραμμα δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας που αναφέρεται στο άρθρο 24 προβλέπει**,** σύμφωνα με τα κριτήρια του άρθρου 4 παράγραφος 2, τη διενέργεια κατάλληλων δοκιμών, όπως αξιολογήσεις και έλεγχοι ευπαθειών, αναλύσεις ανοικτού κώδικα, αξιολογήσεις ασφάλειας δικτύου, αναλύσεις ελλείψεων, επισκοπήσεις υλικής ασφάλειας, ερωτηματολόγια και λύσεις λογισμικού σάρωσης, επανεξετάσεις πηγαίου κώδικα εφόσον είναι εφικτό, δοκιμές βάσει σεναρίων, δοκιμές συμβατότητας, δοκιμές επιδόσεων, διατερματικές δοκιμές και δοκιμές παρείσδυσης.

2. Τα κεντρικά αποθετήρια τίτλων και οι κεντρικοί αντισυμβαλλόμενοι διενεργούν αξιολογήσεις ευπαθειών πριν από την υλοποίηση ή αναδιάταξη νέων ή υφιστάμενων εφαρμογών και στοιχείων υποδομής και υπηρεσιών ΤΠΕ που υποστηρίζουν τις κρίσιμες ή σημαντικές λειτουργίες της χρηματοοικονομικής οντότητα.

3. Οι πολύ μικρές επιχειρήσεις διενεργούν τις δοκιμές που αναφέρονται στην παράγραφο 1 συνδυάζοντας μια προσέγγιση βάσει κινδύνου με στρατηγικό σχεδιασμό των δοκιμών ΤΠΕ, λαμβάνοντας δεόντως υπόψη την ανάγκη διατήρησης ισορροπημένης προσέγγισης μεταξύ της κλίμακας των πόρων και του χρόνου που πρέπει να διατεθεί στις δοκιμές ΤΠΕ σύμφωνα με το παρόν άρθρο, αφενός, και του επείγοντος χαρακτήρα, του είδους του κινδύνου, της κρισιμότητας των πληροφοριακών πόρων και των παρεχόμενων υπηρεσιών, καθώς και κάθε άλλο σχετικό παράγοντα, συμπεριλαμβανομένης της ικανότητας της χρηματοοικονομικής οντότητας να αναλαμβάνει υπολογιζόμενους κινδύνους, αφετέρου.

Άρθρο 26

Προηγμένες δοκιμές εργαλείων, συστημάτων και διαδικασιών ΤΠΕ με βάση τις δοκιμές διείσδυσης βάσει απειλών (TLPT)

1. Οι χρηματοοικονομικές οντότητες, πλην των οντοτήτων που αναφέρονται στο άρθρο 16 παράγραφος 1 πρώτο εδάφιο και των πολύ μικρών επιχειρήσεων, οι οποίες προσδιορίζονται σύμφωνα με την παράγραφο 8 τρίτο εδάφιο του παρόντος άρθρου, διενεργούν τουλάχιστον ανά τριετία προηγμένες δοκιμές μέσω TLPT. Με βάση το προφίλ κινδύνου της χρηματοοικονομικής οντότητας και λαμβάνοντας υπόψη τις επιχειρησιακές συνθήκες, η αρμόδια αρχή μπορεί, εφόσον απαιτείται, να ζητήσει από τη χρηματοοικονομική οντότητα να μειώσει ή να αυξήσει τη συχνότητα αυτή.

2. Κάθε δοκιμή παρείσδυσης βάσει απειλών καλύπτει μερικές ή όλες τις κρίσιμες ή σημαντικές λειτουργίες μιας χρηματοοικονομικής οντότητας και διενεργείται σε συστήματα παραγωγής που υποστηρίζουν τις εν λόγω λειτουργίες.

Οι χρηματοοικονομικές οντότητες προσδιορίζουν όλα τα σχετικά υποκείμενα συστήματα, διαδικασίες και τεχνολογίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες και υπηρεσίες ΤΠΕ, συμπεριλαμβανομένων όσων υποστηρίζουν τις κρίσιμες ή σημαντικές λειτουργίες που έχουν αποτελέσει αντικείμενο εξωτερικής ανάθεσης ή υπεργολαβίας σε τρίτους παρόχους υπηρεσιών ΤΠΕ.

Οι χρηματοοικονομικές οντότητες αξιολογούν ποιες κρίσιμες ή σημαντικές λειτουργίες είναι ανάγκη να καλύπτονται από τις TLPT. Το αποτέλεσμα της αξιολόγησης αυτής καθορίζει το ακριβές πεδίο των TLPT και επικυρώνεται από τις αρμόδιες αρχές.

3. Όταν στο πεδίο των TLPT περιλαμβάνονται τρίτοι πάροχοι υπηρεσιών ΤΠΕ, η χρηματοοικονομική οντότητα λαμβάνει τα αναγκαία μέτρα και διασφαλίσεις για να εξασφαλίσει τη συμμετοχή των εν λόγω τρίτων παρόχων υπηρεσιών ΤΠΕ στις TLPT και διατηρεί ανά πάσα στιγμή την πλήρη ευθύνη για τη διασφάλιση της συμμόρφωσης με τον παρόντα κανονισμό.

4. Με την επιφύλαξη της παραγράφου 2 πρώτο και δεύτερο εδάφιο, όταν η συμμετοχή τρίτου παρόχου υπηρεσιών ΤΠΕ στις TLPT, που αναφέρεται στην παράγραφο 3, αναμένεται ευλόγως να έχει αρνητικό αντίκτυπο στην ποιότητα ή στην ασφάλεια των υπηρεσιών που παρέχονται από τον τρίτο πάροχο υπηρεσιών ΤΠΕ σε πελάτες που είναι οντότητες μη εμπίπτουσες στο πεδίο εφαρμογής του παρόντος κανονισμού, ή στην εμπιστευτικότητα των δεδομένων που σχετίζονται με τις εν λόγω υπηρεσίες, η χρηματοοικονομική οντότητα και ο τρίτος πάροχος υπηρεσιών ΤΠΕ μπορούν να συμφωνήσουν εγγράφως ότι ο τρίτος πάροχος υπηρεσιών ΤΠΕ συνάπτει απευθείας συμβατικές ρυθμίσεις με εξωτερικό δοκιμαστή, για τον σκοπό της διεξαγωγής, υπό τη διεύθυνση μιας ορισθείσας χρηματοοικονομικής οντότητας, ομαδικών TLPT όπου συμμετέχουν διάφορες χρηματοοικονομικές οντότητες (ομαδικές δοκιμές) στις οποίες ο τρίτος πάροχος υπηρεσιών ΤΠΕ παρέχει υπηρεσίες ΤΠΕ.

Οι εν λόγω ομαδικές δοκιμές καλύπτουν το σχετικό φάσμα υπηρεσιών ΤΠΕ που υποστηρίζουν τις κρίσιμες ή σημαντικές λειτουργίες που ανατίθενται στον αντίστοιχο τρίτο πάροχο υπηρεσιών ΤΠΕ από τις χρηματοοικονομικές οντότητες. Οι ομαδικές δοκιμές θεωρούνται TLPT που διενεργούνται από τις χρηματοοικονομικές οντότητες που συμμετέχουν στις ομαδικές δοκιμές.

Ο αριθμός των χρηματοοικονομικών οντοτήτων που συμμετέχουν στις ομαδικές δοκιμές βαθμονομείται δεόντως, λαμβανομένων υπόψη της πολυπλοκότητας και των τύπων των σχετικών υπηρεσιών.

5. Οι χρηματοοικονομικές οντότητες, σε συνεργασία με τρίτους παρόχους υπηρεσιών ΤΠΕ και άλλα εμπλεκόμενα μέρη, συμπεριλαμβανομένων δοκιμαστών αλλά εξαιρουμένων των αρμόδιων αρχών, εφαρμόζουν αποτελεσματικούς ελέγχους διαχείρισης κινδύνων με σκοπό τη μείωση των κινδύνων όσον αφορά τις πιθανές επιπτώσεις στα δεδομένα, την πρόκληση ζημίας στα περιουσιακά στοιχεία και τη διαταραχή κρίσιμων ή σημαντικών λειτουργιών, υπηρεσιών ή δραστηριοτήτων της ίδιας της χρηματοοικονομικής οντότητας, των αντισυμβαλλομένων της ή του χρηματοοικονομικού τομέα.

6. Με την ολοκλήρωση της δοκιμής, αφού συμφωνηθούν οι εκθέσεις και τα σχέδια αποκατάστασης, η χρηματοοικονομική οντότητα και, κατά περίπτωση, οι εξωτερικοί δοκιμαστές παρέχουν, στην αρχή που έχει οριστεί σύμφωνα με την παράγραφο 9 ή 10, περίληψη των σχετικών ευρημάτων, των σχεδίων αποκατάστασης και της τεκμηρίωσης που αποδεικνύει ότι η TLPT διενεργήθηκε σύμφωνα με τις απαιτήσεις.

7. Οι αρχές παρέχουν σε χρηματοοικονομικές οντότητες βεβαίωση που επιβεβαιώνει ότι η δοκιμή διενεργήθηκε σύμφωνα με τις απαιτήσεις και τα στοιχεία της τεκμηρίωσης, προκειμένου να καταστεί δυνατή η αμοιβαία αναγνώριση των δοκιμών παρείσδυσης βάσει απειλών μεταξύ των αρμόδιων αρχών. Η χρηματοοικονομική οντότητα κοινοποιεί στη σχετική αρμόδια αρχή τη βεβαίωση, την περίληψη των σχετικών ευρημάτων και τα σχέδια αποκατάστασης.

Με την επιφύλαξη της βεβαίωσης αυτής, οι χρηματοοικονομικές οντότητες παραμένουν ανά πάσα στιγμή πλήρως υπεύθυνες για τις επιπτώσεις των δοκιμών που αναφέρονται στην παράγραφο 4.

8. Οι χρηματοοικονομικές οντότητες συνάπτουν συμβάσεις με δοκιμαστές για τους σκοπούς της ανάληψης TLPT σύμφωνα με το άρθρο 27. Όταν οι χρηματοοικονομικές οντότητες χρησιμοποιούν εσωτερικούς δοκιμαστές για τους σκοπούς της ανάληψης TLPT, συνάπτουν σύμβαση με εξωτερικούς δοκιμαστές ανά τρεις δοκιμές.

Τα πιστωτικά ιδρύματα τα οποία χαρακτηρίζονται ως σημαντικά σύμφωνα με το άρθρο 6 παράγραφος 4 του κανονισμού (ΕΕ) αριθ. 1024/2013 χρησιμοποιούν μόνο εξωτερικούς δοκιμαστές σύμφωνα με το άρθρο 27 παράγραφος 1 στοιχεία α) έως ε).

Οι αρμόδιες αρχές προσδιορίζουν τις χρηματοοικονομικές οντότητες που υποχρεούνται να διενεργούν TLPT, λαμβάνοντας υπόψη τα κριτήρια που ορίζονται στο άρθρο 4 παράγραφος 2, αξιολογώντας τα ακόλουθα:

α) παράγοντες που σχετίζονται με τις επιπτώσεις, ιδίως όσον αφορά τον βαθμό στον οποίο οι παρεχόμενες υπηρεσίες και δραστηριότητες που αναλαμβάνει η χρηματοοικονομική οντότητα επηρεάζουν τον χρηματοοικονομικό τομέα,

β) πιθανούς προβληματισμούς σχετικά με τη χρηματοοικονομική σταθερότητα, συμπεριλαμβανομένου του συστημικού χαρακτήρα της χρηματοοικονομικής οντότητας σε ενωσιακό ή εθνικό επίπεδο, κατά περίπτωση,

γ) το ειδικό προφίλ κινδύνου ΤΠΕ, το επίπεδο ωριμότητας ΤΠΕ της χρηματοοικονομικής οντότητας ή τα σχετικά τεχνολογικά χαρακτηριστικά.

9. Τα κράτη μέλη μπορούν να ορίσουν μία ενιαία δημόσια αρχή στον χρηματοοικονομικό τομέα ως υπεύθυνη για θέματα σχετικά με τις TLPT στον χρηματοοικονομικό τομέα σε εθνικό επίπεδο και της αναθέτουν όλες τις αρμοδιότητες και τα καθήκοντα για τον σκοπό αυτό.

10. Ελλείψει ορισμού σύμφωνα με την παράγραφο 9 του παρόντος άρθρου, και με την επιφύλαξη της εξουσίας προσδιορισμού των χρηματοοικονομικών οντοτήτων που απαιτούνται για την εκτέλεση TLPT, μια αρμόδια αρχή μπορεί να αναθέσει την άσκηση ορισμένων ή όλων των καθηκόντων που αναφέρονται στο παρόν άρθρο και στο άρθρο 27 σε άλλη εθνική αρχή του χρηματοοικονομικού τομέα.

11. Οι ΕΕΑ, σε συμφωνία με την ΕΚΤ, καταρτίζουν κοινά σχέδια ρυθμιστικών τεχνικών προτύπων σύμφωνα με το πλαίσιο TIBER-EU, προκειμένου να προσδιορίσουν περαιτέρω:

α) τα κριτήρια που χρησιμοποιούνται για την εφαρμογή της παραγράφου 8 δεύτερο εδάφιο,

β) τις απαιτήσεις και τα πρότυπα που διέπουν τη χρήση εσωτερικών δοκιμαστών,

γ) τις απαιτήσεις σχετικά με:

   i) το πεδίο των TLPT που αναφέρεται στην παράγραφο 2,

   ii) τη μεθοδολογία των δοκιμών και την προσέγγιση που πρέπει να ακολουθείται σε κάθε συγκεκριμένο στάδιο της διαδικασίας δοκιμής,

   iii) τα αποτελέσματα, τα στάδια ολοκλήρωσης και αποκατάστασης στο πλαίσιο της δοκιμής,

δ) το είδος της εποπτικής και άλλης σχετικής συνεργασίας που απαιτούνται για την εφαρμογή TLPT και για τη διευκόλυνση της αμοιβαίας αναγνώρισης των εν λόγω δοκιμών, στο πλαίσιο των χρηματοοικονομικών οντοτήτων που δραστηριοποιούνται σε περισσότερα από ένα κράτη μέλη, ώστε να παρέχεται η δυνατότητα κατάλληλου επιπέδου εποπτικής συμμετοχής, καθώς και η δυνατότητα ευέλικτης εφαρμογής για την κάλυψη των ιδιαίτερων χαρακτηριστικών επιμέρους χρηματοοικονομικών τομέων ή τοπικών χρηματοοικονομικών αγορών.

Κατά την κατάρτιση των εν λόγω σχεδίων ρυθμιστικών τεχνικών προτύπων, οι ΕΕΑ λαμβάνουν δεόντως υπόψη κάθε ειδικό χαρακτηριστικό που προκύπτει από τη διακριτή φύση των δραστηριοτήτων σε διάφορους τομείς χρηματοοικονομικών υπηρεσιών.

Οι ΕΕΑ υποβάλλουν τα εν λόγω σχέδια ρυθμιστικών τεχνικών προτύπων στην Επιτροπή έως τις 17 Ιουλίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο, σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

Άρθρο 27

Απαιτήσεις για δοκιμαστές για τη διενέργεια TLPT

1. Οι χρηματοοικονομικές οντότητες, για τη διενέργεια TLPT, χρησιμοποιούν μόνο δοκιμαστές οι οποίοι:

α) είναι απολύτως κατάλληλοι και έγκριτοι,

β) διαθέτουν τεχνικές και οργανωτικές ικανότητες και επιδεικνύουν ειδική εμπειρογνωσία σε θέματα πληροφοριών για απειλές, δοκιμών παρείσδυσης και δοκιμών κόκκινης ομάδας,

γ) έχουν πιστοποίηση από οργανισμό διαπίστευσης κράτους μέλους ή τηρούν επίσημους κώδικες ή πλαίσια δεοντολογίας,

δ) παρέχουν ανεξάρτητη διαβεβαίωση ή έκθεση ελέγχου όσον αφορά την ορθή διαχείριση των κινδύνων που σχετίζονται με τη διενέργεια TLPT, συμπεριλαμβανομένων της δέουσας προστασίας των εμπιστευτικών πληροφοριών της χρηματοοικονομικής οντότητας και της αντιμετώπισης των επιχειρηματικών κινδύνων της χρηματοοικονομικής οντότητας,

ε) καλύπτονται δεόντως και πλήρως από σχετική ασφάλιση επαγγελματικής ευθύνης, μεταξύ άλλων έναντι κινδύνων παραπτωμάτων και αμέλειας.

2. Όταν χρησιμοποιούν εσωτερικούς δοκιμαστές, οι χρηματοοικονομικές οντότητες διασφαλίζουν ότι, πέραν των απαιτήσεων στην παράγραφο 1, πληρούνται και οι ακόλουθες προϋποθέσεις:

α) η χρήση αυτή έχει εγκριθεί από τη σχετική αρμόδια αρχή ή από την ενιαία δημόσια αρχή που έχει οριστεί σύμφωνα με το άρθρο 26 παράγραφοι 9 και 10,

β) η σχετική αρμόδια αρχή έχει επαληθεύσει ότι η χρηματοοικονομική οντότητα διαθέτει επαρκείς ειδικούς πόρους και έχει διασφαλίσει την αποφυγή συγκρούσεων συμφερόντων καθ' όλη τη διάρκεια των φάσεων σχεδιασμού και εκτέλεσης της δοκιμής και

γ) ο πάροχος πληροφοριών για απειλές είναι εξωτερικός σε σχέση με τη χρηματοοικονομική οντότητα.

3. Οι χρηματοοικονομικές οντότητες διασφαλίζουν ότι οι συμβάσεις που συνάπτονται με εξωτερικούς δοκιμαστές προϋποθέτουν την ορθή διαχείριση των αποτελεσμάτων των TLPT και ότι οποιαδήποτε σχετική επεξεργασία δεδομένων, συμπεριλαμβανομένων τυχόν παραγωγής, αποθήκευσης, συγκέντρωσης, σχεδίου, αναφοράς, επικοινωνίας ή καταστροφής, δεν προκαλεί κινδύνους για τη χρηματοοικονομική οντότητα.

ΚΕΦΑΛΑΙΟ V

Διαχείριση κινδύνου τρίτων παρόχων ΤΠΕ

Τμήμα I

Βασικές αρχές για τη χρηστή διαχείριση κινδύνου τρίτων παρόχων ΤΠΕ

Άρθρο 28

Γενικές αρχές

1. Οι χρηματοοικονομικές οντότητες διαχειρίζονται τον κίνδυνο τρίτων παρόχων ΤΠΕ ως αναπόσπαστο στοιχείο των κινδύνων ΤΠΕ εντός του πλαισίου τους διαχείρισης κινδύνων ΤΠΕ όπως αναφέρεται στο άρθρο 6 παράγραφος 1 και σύμφωνα με τις ακόλουθες αρχές:

α) οι χρηματοοικονομικές οντότητες που έχουν θεσπίσει συμβατικές ρυθμίσεις για τη χρήση των υπηρεσιών ΤΠΕ με σκοπό τη διεξαγωγή των επιχειρηματικών τους δραστηριοτήτων εξακολουθούν σε κάθε περίπτωση να είναι πλήρως υπεύθυνες για την τήρηση και την εκπλήρωση όλων των υποχρεώσεων που απορρέουν από τον παρόντα κανονισμό και το ισχύον δίκαιο για τις χρηματοοικονομικές υπηρεσίες,

β) η διαχείριση κινδύνου τρίτων παρόχων ΤΠΕ από τις χρηματοοικονομικές οντότητες εφαρμόζεται βάσει της αρχής της αναλογικότητας, λαμβάνοντας υπόψη:

i) τη φύση, την κλίμακα, την πολυπλοκότητα και τη σημασία των εξαρτήσεων που σχετίζονται με τις ΤΠΕ,

ii) τους κινδύνους που απορρέουν από συμβατικές ρυθμίσεις για τη χρήση υπηρεσιών ΤΠΕ, οι οποίες έχουν συναφθεί με τρίτους παρόχους υπηρεσιών ΤΠΕ, λαμβάνοντας υπόψη την κρισιμότητα ή τη σημασία της αντίστοιχης υπηρεσίας, διαδικασίας ή λειτουργίας, και τις πιθανές επιπτώσεις στη συνέχεια και τη διαθεσιμότητα των χρηματοοικονομικών υπηρεσιών και δραστηριοτήτων, τόσο σε μεμονωμένο επίπεδο όσο και σε επίπεδο ομίλου.

2. Στο πλαίσιο της διαχείρισης κινδύνου ΤΠΕ, οι χρηματοοικονομικές οντότητες, εκτός των οντοτήτων που αναφέρονται στο άρθρο 16 παράγραφος 1 πρώτο εδάφιο και εκτός των πολύ μικρών επιχειρήσεων, εγκρίνουν και επανεξετάζουν τακτικά τη στρατηγική για τους κινδύνους τρίτων παρόχων ΤΠΕ, λαμβάνοντας υπόψη τη στρατηγική πολλαπλών προμηθευτών που αναφέρεται στο άρθρο 6 παράγραφος 9, κατά περίπτωση. Η στρατηγική για τη διαχείριση κινδύνου τρίτων παρόχων ΤΠΕ περιλαμβάνει πολιτική για τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κριτικές ή σημαντικές λειτουργίες, οι οποίες παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ και εφαρμόζεται σε μεμονωμένη βάση και, ανάλογα με την περίπτωση, σε υποενοποιημένη και ενοποιημένη βάση. Το διοικητικό όργανο, βάσει αξιολόγησης του συνολικού προφίλ κινδύνου της χρηματοοικονομικής οντότητας και της κλίμακας και της πολυπλοκότητας των επιχειρηματικών υπηρεσιών, επανεξετάζει τακτικά τους κινδύνους που εντοπίζονται σε σχέση με συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες.

3. Στο πλαίσιο της διαχείρισης κινδύνου ΤΠΕ, οι χρηματοοικονομικές οντότητες τηρούν και επικαιροποιούν σε επίπεδο οντότητας και σε υποενοποιημένο και ενοποιημένο επίπεδο, μητρώο πληροφοριών όσον αφορά το σύνολο των συμβατικών ρυθμίσεων σχετικά με τη χρήση υπηρεσιών ΤΠΕ που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ.

Οι συμβατικές ρυθμίσεις που αναφέρονται στο πρώτο εδάφιο τεκμηριώνονται κατάλληλα, με διαχωρισμό των ρυθμίσεων που καλύπτουν υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες από τις υπόλοιπες ρυθμίσεις.

Οι χρηματοοικονομικές οντότητες αναφέρουν στις αρμόδιες αρχές, τουλάχιστον ετησίως, τον αριθμό των νέων συμβατικών ρυθμίσεων για τη χρήση υπηρεσιών ΤΠΕ, τις κατηγορίες τρίτων παρόχων υπηρεσιών ΤΠΕ, το είδος των συμβατικών ρυθμίσεων και τις παρεχόμενες υπηρεσίες και λειτουργίες ΤΠΕ.

Οι χρηματοοικονομικές οντότητες θέτουν στη διάθεση της αρμόδιας αρχής, κατόπιν αιτήματός της, το πλήρες μητρώο πληροφοριών ή, εφόσον ζητείται, συγκεκριμένα τμήματα αυτού, καθώς και κάθε πληροφορία που κρίνεται απαραίτητη για την αποτελεσματική εποπτεία της χρηματοοικονομικής οντότητας.

Οι χρηματοοικονομικές οντότητες ενημερώνουν εγκαίρως την αρμόδια αρχή για οποιαδήποτε προγραμματισμένη συμβατική ρύθμιση σχετικά με τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες, καθώς και για τη χρονική στιγμή κατά την οποία καθίσταται κρίσιμη ή σημαντική μια λειτουργία.

4. Πριν από τη σύναψη συμβατικής ρύθμισης σχετικά με τη χρήση υπηρεσιών ΤΠΕ, οι χρηματοοικονομικές οντότητες:

α) αξιολογούν αν η συμβατική ρύθμιση καλύπτει τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμη ή σημαντική λειτουργία,

β) αξιολογούν αν πληρούνται οι όροι εποπτείας της σύμβασης,

γ) προσδιορίζουν και αξιολογούν όλους τους συναφείς κινδύνους σε σχέση με τη συμβατική ρύθμιση, συμπεριλαμβανομένης της πιθανότητας συμβολής της εν λόγω συμβατικής ρύθμισης στην ενίσχυση του κινδύνου συγκέντρωσης ΤΠΕ, όπως αναφέρεται στο άρθρο 29,

δ) αναλαμβάνουν κάθε δέουσα επιμέλεια των υποψήφιων τρίτων παρόχων υπηρεσιών ΤΠΕ και διασφαλίζουν καθ' όλη τη διαδικασία επιλογής και αξιολόγησης ότι ο τρίτος πάροχος υπηρεσιών ΤΠΕ είναι κατάλληλος,

ε) προσδιορίζουν και αξιολογούν συγκρούσεις συμφερόντων που μπορεί να προκαλέσει η συμβατική ρύθμιση.

5. Οι χρηματοοικονομικές οντότητες μπορούν να συνάπτουν συμβατικές ρυθμίσεις μόνο με τρίτους παρόχους υπηρεσιών ΤΠΕ που συμμορφώνονται με κατάλληλα πρότυπα ασφάλειας των πληροφοριών. Όταν οι εν λόγω συμβατικές ρυθμίσεις αφορούν κρίσιμες ή σημαντικές λειτουργίες, οι χρηματοοικονομικές οντότητες, πριν από τη σύναψη των ρυθμίσεων, λαμβάνουν δεόντως υπόψη τη χρήση, από τρίτους παρόχους υπηρεσιών ΤΠΕ, των πλέον επικαιροποιημένων και ύψιστης ποιότητας προτύπων ασφάλειας πληροφοριών.

6. Κατά την άσκηση των δικαιωμάτων πρόσβασης, επιθεώρησης και ελέγχου έναντι του τρίτου παρόχου υπηρεσιών ΤΠΕ, οι χρηματοοικονομικές οντότητες προκαθορίζουν, σύμφωνα με την προσέγγιση βάσει κινδύνων, τη συχνότητα των ελέγχων και των επιθεωρήσεων, καθώς και τους τομείς που πρέπει να ελέγχονται μέσω της τήρησης κοινώς αποδεκτών προτύπων ελέγχου σύμφωνα με τυχόν εποπτικές οδηγίες σχετικά με τη χρήση και την ενσωμάτωση προτύπων ελέγχου αυτού του είδους.

Όταν οι συμβατικές ρυθμίσεις που συνάπτονται με τρίτους παρόχους υπηρεσιών ΤΠΕ σχετικά με τη χρήση υπηρεσιών ΤΠΕ συνεπάγονται υψηλή τεχνική πολυπλοκότητα, η χρηματοοικονομική οντότητα εξακριβώνει αν οι ελεγκτές, είτε πρόκειται για εσωτερικούς ή εξωτερικούς είτε για ομάδα ελεγκτών, διαθέτουν τις κατάλληλες δεξιότητες και γνώσεις για την αποτελεσματική διενέργεια των σχετικών ελέγχων και αξιολογήσεων.

7. Οι χρηματοοικονομικές οντότητες διασφαλίζουν ότι οι συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ μπορούν να καταγγέλλονται όταν συντρέχει οποιαδήποτε από τις παρακάτω συνθήκες:

α) σημαντική παραβίαση των εφαρμοστέων νομοθετικών, κανονιστικών διατάξεων ή συμβατικών όρων από τον τρίτο πάροχο υπηρεσιών ΤΠΕ,

β) συνθήκες που προσδιορίζονται καθ' όλη τη διάρκεια παρακολούθησης των κινδύνων τρίτων παρόχων ΤΠΕ και οι οποίες θεωρούνται ικανές να μεταβάλουν την εκτέλεση των λειτουργιών που παρέχονται μέσω της συμβατικής ρύθμισης, συμπεριλαμβανομένων σημαντικών μεταβολών που επηρεάζουν τη ρύθμιση ή την κατάσταση του τρίτου παρόχου υπηρεσιών ΤΠΕ,

γ) αποδεδειγμένες αδυναμίες του τρίτου παρόχου υπηρεσιών ΤΠΕ που αφορούν τη συνολική διαχείριση κινδύνου ΤΠΕ από μέρους του και ειδικότερα στον τρόπο με τον οποίο εγγυάται τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα εμπιστευτικών, προσωπικών ή άλλως ευαίσθητων δεδομένων ή μη προσωπικών δεδομένων,

δ) όταν η αρμόδια αρχή δεν μπορεί πλέον να εποπτεύει αποτελεσματικά τη χρηματοοικονομική οντότητα συνεπεία των συνθηκών της αντίστοιχης συμβατικής ρύθμισης ή των περιστάσεων που σχετίζονται με αυτήν.

8. Για τις υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες, οι χρηματοοικονομικές οντότητες θέτουν σε εφαρμογή στρατηγικές εξόδου. Οι στρατηγικές εξόδου λαμβάνουν υπόψη τους κινδύνους που ενδέχεται να ανακύψουν στο επίπεδο των τρίτων παρόχων υπηρεσιών ΤΠΕ, ιδίως όσον αφορά την πιθανότητα αθέτησης υποχρεώσεων εκ μέρους τους, την υποβάθμιση της ποιότητας των παρεχόμενων υπηρεσιών ΤΠΕ, τυχόν διαταραχή της δραστηριότητας λόγω ακατάλληλης ή μη παροχής υπηρεσιών ΤΠΕ ή οποιονδήποτε σημαντικό κίνδυνο που ανακύπτει σε σχέση με την ενδεδειγμένη και συνεχή ανάπτυξη της αντίστοιχης υπηρεσίας ΤΠΕ ή την καταγγελία συμβατικών ρυθμίσεων με τρίτους παρόχους υπηρεσιών ΤΠΕ υπό οποιαδήποτε από τις περιστάσεις οι οποίες προβλέπονται στην παράγραφο 7.

Οι χρηματοοικονομικές οντότητες διασφαλίζουν ότι είναι σε θέση να αποχωρήσουν από συμβατικές ρυθμίσεις:

α) χωρίς διαταραχή των επιχειρηματικών τους δραστηριοτήτων,

β) χωρίς περιορισμό της συμμόρφωσης με τις κανονιστικές απαιτήσεις,

γ) χωρίς αυτό να αποβαίνει εις βάρος της συνέχειας και της ποιότητας των υπηρεσιών που παρέχονται σε πελάτες.

Τα σχέδια εξόδου είναι πλήρη, τεκμηριωμένα και, σύμφωνα με τα κριτήρια που ορίζονται στο άρθρο 4 παράγραφος 2, υποβάλλονται σε επαρκείς δοκιμές και επανεξετάζονται περιοδικά.

Οι χρηματοοικονομικές οντότητες προσδιορίζουν εναλλακτικές λύσεις και καταρτίζουν μεταβατικά σχέδια που τους παρέχουν τη δυνατότητα να αφαιρέσουν τις συμβατικές υπηρεσίες ΤΠΕ και τα σχετικά δεδομένα από τον τρίτο πάροχο υπηρεσιών ΤΠΕ και να τα μεταφέρουν με ασφαλή και ολοκληρωμένο τρόπο σε εναλλακτικούς παρόχους ή να τα ενσωματώνουν εκ νέου εντός της επιχείρησης.

Οι χρηματοοικονομικές οντότητες θέτουν σε εφαρμογή ενδεδειγμένα μέτρα έκτακτης ανάγκης για τη διατήρηση της επιχειρησιακής συνέχειας, εφόσον συντρέχουν οι συνθήκες που αναφέρονται στο πρώτο εδάφιο.

9. Οι ΕΕΑ καταρτίζουν, μέσω της μεικτής επιτροπής, σχέδια εκτελεστικών τεχνικών προτύπων για τη δημιουργία των τυποποιημένων υποδειγμάτων για τους σκοπούς του μητρώου πληροφοριών που αναφέρεται στην παράγραφο 3, συμπεριλαμβανομένων των πληροφοριών που είναι κοινές σε όλες τις συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ. Οι ΕΕΑ υποβάλλουν τα εν λόγω σχέδια εκτελεστικών τεχνικών προτύπων στην Επιτροπή έως τις 17 Ιανουαρίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει τα εκτελεστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο, σύμφωνα με το άρθρο 15 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

10. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, καταρτίζουν σχέδια ρυθμιστικών τεχνικών προτύπων για τον περαιτέρω προσδιορισμό των λεπτομερειών του περιεχομένου της πολιτικής που αναφέρεται στην παράγραφο 2 σε σχέση με τις συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ οι οποίες υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ.

Κατά την κατάρτιση των εν λόγω σχεδίων ρυθμιστικών τεχνικών προτύπων, οι ΕΕΑ λαμβάνουν υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου της χρηματοοικονομικής οντότητας, και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της. Οι ΕΕΑ υποβάλλουν τα εν λόγω σχέδια εκτελεστικών τεχνικών προτύπων στην Επιτροπή έως τις 17 Ιανουαρίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο, σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

Άρθρο 29

Προκαταρκτική αξιολόγηση κινδύνου συγκέντρωσης ΤΠΕ

1. Κατά τον προσδιορισμό και την αξιολόγηση των κινδύνων που αναφέρονται στο άρθρο 28 παράγραφος 4 στοιχείο γ), οι χρηματοοικονομικές οντότητες λαμβάνουν επίσης υπόψη αν η προβλεπόμενη σύναψη συμβατικής ρύθμισης σε σχέση με υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες μπορεί να έχει οποιοδήποτε από τα ακόλουθα αποτελέσματα:

α) εργολαβική ανάθεση σε τρίτο πάροχο υπηρεσιών ΤΠΕ που δεν μπορεί να αντικατασταθεί εύκολα ή

β) εφαρμογή πολλαπλών συμβατικών ρυθμίσεων σχετικά με την παροχή υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες με τον ίδιο τρίτο πάροχο υπηρεσιών ΤΠΕ ή με στενά συνδεδεμένους τρίτους παρόχους υπηρεσιών ΤΠΕ.

Οι χρηματοοικονομικές οντότητες σταθμίζουν τα οφέλη και το κόστος εναλλακτικών λύσεων, όπως η χρήση διαφορετικών τρίτων παρόχων υπηρεσιών ΤΠΕ, λαμβάνοντας υπόψη αν και με ποιον τρόπο οι προτεινόμενες λύσεις ανταποκρίνονται στις επιχειρηματικές ανάγκες και τους στόχους που καθορίζονται στην οικεία στρατηγική ψηφιακής ανθεκτικότητας.

2. Όταν οι συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες περιλαμβάνουν την πιθανότητα ένας τρίτος πάροχος υπηρεσιών ΤΠΕ να αναθέσει περαιτέρω με υπεργολαβία υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμη ή σημαντική λειτουργία σε άλλους τρίτους παρόχους υπηρεσιών ΤΠΕ, οι χρηματοοικονομικές οντότητες σταθμίζουν τα οφέλη και τους κινδύνους που ενδέχεται να προκύψουν σε σχέση με την εν λόγω πιθανή υπεργολαβία, ιδίως σε περίπτωση υπεργολάβου ΤΠΕ εγκατεστημένου σε τρίτη χώρα.

Όταν οι συμβατικές ρυθμίσεις αφορούν υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες, οι χρηματοοικονομικές οντότητες λαμβάνουν δεόντως υπόψη τις διατάξεις της νομοθεσίας περί αφερεγγυότητας που θα ίσχυαν σε περίπτωση πτώχευσης του τρίτου παρόχου υπηρεσιών ΤΠΕ, καθώς και κάθε περιορισμό που ενδέχεται να ανακύψει σε σχέση με την επείγουσα ανάκτηση των δεδομένων της χρηματοοικονομικής οντότητας.

Όταν συνάπτονται συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες με τρίτο πάροχο υπηρεσιών ΤΠΕ εγκατεστημένο σε τρίτη χώρα, οι χρηματοοικονομικές οντότητες, πέραν των εκτιμήσεων που αναφέρονται στο δεύτερο εδάφιο, εξετάζουν επίσης τη συμμόρφωση με τους κανόνες της Ένωσης για την προστασία των δεδομένων και την αποτελεσματική επιβολή του δικαίου στην εν λόγω τρίτη χώρα.

Όταν οι συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες προβλέπουν υπεργολαβική ανάθεση, οι χρηματοοικονομικές οντότητες αξιολογούν αν και με ποιον τρόπο μπορούν οι δυνητικά μεγάλες και πολύπλοκες αλυσίδες υπεργολαβικής ανάθεσης να επηρεάσουν την ικανότητά τους να παρακολουθούν πλήρως τις λειτουργίες που αποτελούν αντικείμενο ανάθεσης, καθώς και την ικανότητα της αρμόδιας αρχής να εποπτεύει αποτελεσματικά τη χρηματοοικονομική οντότητα στο πλαίσιο αυτό.

Άρθρο 30

Βασικές συμβατικές διατάξεις

1. Τα δικαιώματα και οι υποχρεώσεις της χρηματοοικονομικής οντότητας και του τρίτου παρόχου υπηρεσιών ΤΠΕ επιμερίζονται με σαφήνεια και καθορίζονται εγγράφως. Η πλήρης σύμβαση περιλαμβάνει τις συμφωνίες επιπέδου εξυπηρέτησης και τεκμηριώνεται με έγγραφο το οποίο τίθεται στη διάθεση των συμβαλλομένων σε έντυπη μορφή, ή με έγγραφο σε άλλο τηλεφορτώσιμο, σταθερό και προσβάσιμο μορφότυπο.

2. Οι συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ περιλαμβάνουν τουλάχιστον τα ακόλουθα στοιχεία:

α) σαφή και πλήρη περιγραφή όλων των λειτουργιών και υπηρεσιών ΤΠΕ που πρέπει να παρέχονται από τον τρίτο πάροχο υπηρεσιών ΤΠΕ, με αναφορά στη δυνατότητα ή μη υπεργολαβικής ανάθεσης υπηρεσίας ΤΠΕ που υποστηρίζει κρίσιμη ή σημαντική λειτουργία, ή σημαντικών μερών της, και, εάν αυτή επιτρέπεται, αναφορά των όρων που διέπουν την υπεργολαβική ανάθεση,

β) τις τοποθεσίες, δηλαδή τις περιοχές και τις χώρες στις οποίες πρέπει να παρέχονται οι λειτουργίες και υπηρεσίες ΤΠΕ που αποτελούν αντικείμενο ανάθεσης ή υπεργολαβίας και στις οποίες θα πραγματοποιείται η επεξεργασία δεδομένων, συμπεριλαμβανομένου του χώρου αποθήκευσης, και την απαίτηση ενημέρωσης της χρηματοοικονομικής οντότητας από τον τρίτο πάροχο υπηρεσιών ΤΠΕ εκ των προτέρων, σε περίπτωση που προτίθεται να αλλάξει τις τοποθεσίες αυτές,

γ) διατάξεις σχετικά με τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα όσον αφορά την προστασία δεδομένων, συμπεριλαμβανομένων των δεδομένων προσωπικού χαρακτήρα,

δ) διατάξεις σχετικά με τη διασφάλιση της πρόσβασης, της ανάκτησης και της επιστροφής σε εύκολα προσβάσιμη μορφή δεδομένων προσωπικού και μη προσωπικού χαρακτήρα, τα οποία επεξεργάζεται η χρηματοοικονομική οντότητα σε περίπτωση αφερεγγυότητας, εξυγίανσης, διακοπής των επιχειρηματικών δραστηριοτήτων του τρίτου παρόχου υπηρεσιών ΤΠΕ, ή σε περίπτωση καταγγελίας των συμβατικών ρυθμίσεων,

ε) περιγραφές των επιπέδων εξυπηρέτησης, συμπεριλαμβανομένων των επικαιροποιήσεων και των αναθεωρήσεών τους,

στ) την υποχρέωση του τρίτου παρόχου υπηρεσιών ΤΠΕ να παρέχει συνδρομή στη χρηματοοικονομική οντότητα χωρίς πρόσθετο κόστος ή με κόστος που καθορίζεται εκ των προτέρων, σε περίπτωση συμβάντος ΤΠΕ το οποίο σχετίζεται με την υπηρεσία ΤΠΕ που παρέχεται στη χρηματοοικονομική οντότητα,

ζ) την υποχρέωση του τρίτου παρόχου υπηρεσιών ΤΠΕ να συνεργάζεται πλήρως με τις αρμόδιες αρχές και τις αρχές εξυγίανσης της χρηματοοικονομικής οντότητας, συμπεριλαμβανομένων των προσώπων που διορίζονται από αυτές,

η) δικαιώματα καταγγελίας και συναφή ελάχιστη περίοδο προειδοποίησης για την καταγγελία των συμβατικών ρυθμίσεων, σύμφωνα με τις προσδοκίες των αρμόδιων αρχών και των αρχών εξυγίανσης,

θ) τους όρους συμμετοχής τρίτων παρόχων υπηρεσιών ΤΠΕ στα προγράμματα ευαισθητοποίησης για την ασφάλεια ΤΠΕ των χρηματοοικονομικών οντοτήτων και στην κατάρτιση για την ψηφιακή επιχειρησιακή ανθεκτικότητα σύμφωνα με το άρθρο 13 παράγραφος 6.

3. Οι συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες περιλαμβάνουν, επιπλέον των στοιχείων που αναφέρονται στην παράγραφο 2, τουλάχιστον τα ακόλουθα:

α) πλήρεις περιγραφές των επιπέδων εξυπηρέτησης, συμπεριλαμβανομένων των επικαιροποιήσεων και των αναθεωρήσεών τους με ακριβείς ποσοτικούς και ποιοτικούς στόχους επιδόσεων εντός των συμφωνημένων επιπέδων εξυπηρέτησης, ώστε να παρέχεται η δυνατότητα αποτελεσματικής παρακολούθησης από τη χρηματοοικονομική οντότητα των υπηρεσιών ΤΠΕ και να επιτρέπεται η λήψη κατάλληλων διορθωτικών μέτρων, χωρίς αδικαιολόγητη καθυστέρηση, όταν δεν πληρούνται τα συμφωνημένα επίπεδα εξυπηρέτησης,

β) προθεσμίες προειδοποίησης και υποχρεώσεις υποβολής εκθέσεων εκ μέρους του τρίτου παρόχου υπηρεσιών ΤΠΕ προς τη χρηματοοικονομική οντότητα, συμπεριλαμβανομένης της κοινοποίησης οποιασδήποτε εξέλιξης η οποία θα μπορούσε να έχει σημαντικές επιπτώσεις στην ικανότητα του τρίτου παρόχου υπηρεσιών ΤΠΕ όσον αφορά την αποτελεσματική παροχή υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες σύμφωνα με τα συμφωνημένα επίπεδα εξυπηρέτησης,

γ) απαιτήσεις για τον τρίτο πάροχο υπηρεσιών ΤΠΕ να θέτει σε εφαρμογή και να υποβάλλει σε δοκιμή επιχειρησιακά σχέδια έκτακτης ανάγκης και να εφαρμόζει μέτρα, εργαλεία και πολιτικές ασφάλειας των ΤΠΕ που παρέχουν κατάλληλο επίπεδο ασφάλειας για την παροχή υπηρεσιών από τη χρηματοοικονομική οντότητα σύμφωνα με το ρυθμιστικό της πλαίσιο,

δ) την υποχρέωση του τρίτου παρόχου υπηρεσιών ΤΠΕ να συμμετέχει και να συνεργάζεται πλήρως στις TLPT της χρηματοοικονομικής οντότητας, όπως αναφέρεται στα άρθρα 26 και 27,

ε) το δικαίωμα παρακολούθησης, σε διαρκή βάση, των επιδόσεων του τρίτου παρόχου υπηρεσιών ΤΠΕ, το οποίο συνεπάγεται τα ακόλουθα:

i) απεριόριστα δικαιώματα πρόσβασης, επιθεώρησης και ελέγχου από τη χρηματοοικονομική οντότητα ή διορισμένο τρίτο φορέα, και από την αρμόδια αρχή, και το δικαίωμα λήψης αντιγράφων της σχετικής τεκμηρίωσης επιτόπου εάν είναι κρίσιμα για τις δραστηριότητες του τρίτου παρόχου υπηρεσιών ΤΠΕ, η αποτελεσματική άσκηση των οποίων δεν εμποδίζεται ούτε περιορίζεται από άλλες συμβατικές ρυθμίσεις ή την εφαρμογή πολιτικών,

ii) το δικαίωμα συμφωνίας περί εναλλακτικών επιπέδων βεβαιότητας, όταν θίγονται τα δικαιώματα άλλων πελατών,

iii) την υποχρέωση του τρίτου παρόχου υπηρεσιών ΤΠΕ για πλήρη συνεργασία κατά τις επιτόπιες επιθεωρήσεις και τους ελέγχους που διενεργούνται από τις αρμόδιες αρχές, τον κύριο εποπτικό φορέα, τη χρηματοοικονομική οντότητα ή διορισμένο τρίτο φορέα και

iv) την υποχρέωση παροχής λεπτομερειών σχετικά με το εύρος, τις ακολουθητέες διαδικασίες και τη συχνότητα διενέργειας των εν λόγω επιθεωρήσεων και ελέγχων,

στ) στρατηγικές εξόδου, ιδίως όσον αφορά τον καθορισμό υποχρεωτικής επαρκούς μεταβατικής περιόδου:

i) κατά τη διάρκεια της οποίας ο τρίτος πάροχος υπηρεσιών ΤΠΕ θα συνεχίσει να παρέχει τις αντίστοιχες λειτουργίες ή υπηρεσίες ΤΠΕ, με σκοπό τη μείωση του κινδύνου διαταραχής στη χρηματοοικονομική οντότητα ή τη διασφάλιση της αποτελεσματικής εξυγίανσης και αναδιάρθρωσής της,

(ii) η οποία παρέχει στη χρηματοοικονομική οντότητα τη δυνατότητα μετάβασης σε άλλον τρίτο πάροχο υπηρεσιών ΤΠΕ ή τη δυνατότητα επιλογής άλλων λύσεων εντός της επιχείρησης, ανάλογα με την πολυπλοκότητα της παρεχόμενης υπηρεσίας.

Κατά παρέκκλιση από το στοιχείο ε), ο τρίτος πάροχος υπηρεσιών ΤΠΕ και η χρηματοοικονομική οντότητα που αποτελεί πολύ μικρή επιχείρηση μπορούν να συμφωνήσουν ότι τα δικαιώματα πρόσβασης, επιθεώρησης και ελέγχου της χρηματοοικονομικής οντότητας μπορούν να ανατεθούν σε ανεξάρτητο τρίτο μέρος, το οποίο ορίζεται από τον τρίτο πάροχο υπηρεσιών ΤΠΕ, και ότι η χρηματοοικονομική οντότητα είναι σε θέση να ζητήσει από το τρίτο μέρος ανά πάσα στιγμή πληροφορίες και διαβεβαιώσεις σχετικά με τις επιδόσεις του τρίτου παρόχου υπηρεσιών ΤΠΕ.

4. Κατά τη διαπραγμάτευση των συμβατικών ρυθμίσεων, οι χρηματοοικονομικές οντότητες και οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ λαμβάνουν υπόψη τη χρήση τυποποιημένων συμβατικών ρητρών που έχουν καταρτισθεί από τις αρμόδιες αρχές για συγκεκριμένες υπηρεσίες.

5. Οι ΕΕΑ καταρτίζουν, μέσω της μεικτής επιτροπής, σχέδια ρυθμιστικών τεχνικών προτύπων για τον περαιτέρω προσδιορισμό των στοιχείων της παραγράφου 2 στοιχείο α) τα οποία πρέπει να καθορίζει και να αξιολογεί η χρηματοοικονομική οντότητα κατά την υπεργολαβική ανάθεση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες.

Κατά την κατάρτιση των εν λόγω σχεδίων ρυθμιστικών τεχνικών προτύπων, οι ΕΕΑ λαμβάνουν υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου της χρηματοοικονομικής οντότητας και τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της.

Οι ΕΕΑ υποβάλλουν τα εν λόγω σχέδια ρυθμιστικών τεχνικών προτύπων στην Επιτροπή έως τις 17 Ιουλίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο, σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

ΤΜΗΜΑ ΙΙ

Πλαίσιο εποπτείας κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ

Άρθρο 31

Ορισμός κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ

1. Οι ΕΕΑ, μέσω της μεικτής επιτροπής και κατόπιν σύστασης του φόρουμ εποπτείας που συγκροτείται βάσει του άρθρου 32 παράγραφος 1:

α) ορίζουν τους τρίτους παρόχους υπηρεσιών ΤΠΕ που είναι κρίσιμοι για τις χρηματοοικονομικές οντότητες, κατόπιν αξιολόγησης κατά την οποία λαμβάνονται υπόψη τα κριτήρια που καθορίζονται στην παράγραφο 2,

β) ορίζουν ως κύριο εποπτικό φορέα για κάθε κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ την ΕΕΑ η οποία είναι υπεύθυνη, σύμφωνα με τους κανονισμούς (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 ή (ΕΕ) αριθ. 1095/2010, για τις χρηματοοικονομικές οντότητες που έχουν από κοινού το μεγαλύτερο μερίδιο των συνολικών περιουσιακών στοιχείων επί της αξίας των συνολικών περιουσιακών στοιχείων όλων των χρηματοοικονομικών οντοτήτων που χρησιμοποιούν τις υπηρεσίες του σχετικού κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ, όπως αποδεικνύεται από το άθροισμα των επιμέρους ισολογισμών των εν λόγω χρηματοοικονομικών οντοτήτων.

2. Ο ορισμός που αναφέρεται στην παράγραφο 1 στοιχείο α) βασίζεται σε όλα τα ακόλουθα κριτήρια σε σχέση με τις υπηρεσίες ΤΠΕ που παρέχονται από τρίτο πάροχο υπηρεσιών ΤΠΕ:

α) τις συστημικές επιπτώσεις στη σταθερότητα, τη συνέχεια ή την ποιότητα της παροχής χρηματοοικονομικών υπηρεσιών σε περίπτωση που ο σχετικός τρίτος πάροχος υπηρεσιών ΤΠΕ αντιμετωπίσει λειτουργική ανεπάρκεια μεγάλης κλίμακας κατά την παροχή των υπηρεσιών του, λαμβάνοντας υπόψη τον αριθμό των χρηματοοικονομικών οντοτήτων και τη συνολική αξία των περιουσιακών στοιχείων των χρηματοοικονομικών οντοτήτων στις οποίες ο οικείος τρίτος πάροχος υπηρεσιών ΤΠΕ παρέχει τις υπηρεσίες του,

β) τον συστημικό χαρακτήρα ή τη σημασία των χρηματοοικονομικών οντοτήτων οι οποίες βασίζονται στον οικείο τρίτο πάροχο υπηρεσιών ΤΠΕ, που αξιολογείται σύμφωνα με τις ακόλουθες παραμέτρους:

i) τον αριθμό των παγκόσμιων συστημικώς σημαντικών ιδρυμάτων (G-SII) ή άλλων συστημικώς σημαντικών ιδρυμάτων (O-SII) που βασίζονται στον αντίστοιχο τρίτο πάροχο υπηρεσιών ΤΠΕ,

ii) την αλληλεξάρτηση μεταξύ των G-SII ή των O-SII που αναφέρονται στο σημείο i) και άλλων χρηματοοικονομικών οντοτήτων, συμπεριλαμβανομένων των καταστάσεων στις οποίες τα G-SII ή τα O-SII παρέχουν υπηρεσίες χρηματοοικονομικών υποδομών σε άλλες χρηματοοικονομικές οντότητες,

γ) την εξάρτηση των χρηματοοικονομικών οντοτήτων από τις υπηρεσίες που παρέχονται από τον σχετικό τρίτο πάροχο υπηρεσιών ΤΠΕ σε σχέση με κρίσιμες ή σημαντικές λειτουργίες χρηματοοικονομικών οντοτήτων στις οποίες συμμετέχει τελικά ο ίδιος τρίτος πάροχος υπηρεσιών ΤΠΕ, ανεξάρτητα από το αν οι χρηματοοικονομικές οντότητες στηρίζονται στις υπηρεσίες αυτές άμεσα ή έμμεσα, μέσω ρυθμίσεων υπεργολαβίας,

δ) τη δυνατότητα υποκατάστασης του τρίτου παρόχου υπηρεσιών ΤΠΕ, λαμβάνοντας υπόψη τις ακόλουθες παραμέτρους:

i) την έλλειψη πραγματικών εναλλακτικών επιλογών, έστω και εν μέρει, λόγω του περιορισμένου αριθμού τρίτων παρόχων υπηρεσιών ΤΠΕ που δραστηριοποιούνται σε συγκεκριμένη αγορά, ή του μεριδίου αγοράς του σχετικού τρίτου παρόχου υπηρεσιών ΤΠΕ ή της τεχνικής πολυπλοκότητας ή του εξειδικευμένου χαρακτήρα που απαιτείται, μεταξύ άλλων σε σχέση με τυχόν αποκλειστική τεχνολογία, ή των συγκεκριμένων χαρακτηριστικών της οργάνωσης ή της δραστηριότητας του τρίτου παρόχου υπηρεσιών ΤΠΕ,

ii) δυσκολίες σε σχέση με τη μερική ή συνολική μεταφορά των σχετικών δεδομένων και του φόρτου εργασίας από τον οικείο τρίτο πάροχο υπηρεσιών ΤΠΕ σε άλλον τρίτο πάροχο υπηρεσιών ΤΠΕ, είτε λόγω του σημαντικού οικονομικού κόστους, του χρόνου ή άλλου πόρου που μπορεί να συνεπάγεται η διαδικασία μεταφοράς είτε λόγω αυξημένων κινδύνων ΤΠΕ ή άλλων λειτουργικών κινδύνων στους οποίους ενδέχεται να εκτεθεί η χρηματοοικονομική οντότητα λόγω της μεταφοράς αυτής.

3. Όταν ο τρίτος πάροχος υπηρεσιών ΤΠΕ ανήκει σε όμιλο, τα κριτήρια που αναφέρονται στην παράγραφο 2 λαμβάνονται υπόψη σε σχέση με τις υπηρεσίες ΤΠΕ που παρέχονται από τον όμιλο στο σύνολό του.

4. Οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που αποτελούν μέρος ομίλου ορίζουν ένα νομικό πρόσωπο ως σημείο συντονισμού για τη διασφάλιση επαρκούς εκπροσώπησης και επικοινωνίας με τον κύριο εποπτικό φορέα.

5. Ο κύριος εποπτικός φορέας κοινοποιεί στον τρίτο πάροχο υπηρεσιών ΤΠΕ το αποτέλεσμα της αξιολόγησης που οδηγεί στον ορισμό που αναφέρεται στην παράγραφο 1 στοιχείο α). Εντός 6 εβδομάδων από την ημερομηνία της κοινοποίησης, ο τρίτος πάροχος υπηρεσιών ΤΠΕ μπορεί να υποβάλει στον κύριο εποπτικό φορέα αιτιολογημένη δήλωση με κάθε σχετική πληροφορία για τους σκοπούς της αξιολόγησης. Ο κύριος εποπτικός φορέας εξετάζει την αιτιολογημένη δήλωση και μπορεί να ζητήσει την υποβολή πρόσθετων πληροφοριών εντός 30 ημερολογιακών ημερών από την παραλαβή της εν λόγω δήλωσης.

Μετά τον ορισμό τρίτου παρόχου υπηρεσιών ΤΠΕ ως κρίσιμου, οι ΕΕΑ, μέσω της μεικτής επιτροπής, κοινοποιούν στον τρίτο πάροχο υπηρεσιών ΤΠΕ τον εν λόγω ορισμό και την ημερομηνία έναρξης από την οποία θα υπόκεινται ουσιαστικά σε δραστηριότητες εποπτείας. Η εν λόγω ημερομηνία έναρξης δεν υπερβαίνει τον ένα μήνα μετά την κοινοποίηση. Ο τρίτος πάροχος υπηρεσιών ΤΠΕ κοινοποιεί στις χρηματοοικονομικές οντότητες στις οποίες παρέχει υπηρεσίες τον χαρακτηρισμό τους ως κρίσιμων.

6. Ανατίθεται στην Επιτροπή η εξουσία να εκδώσει κατ' εξουσιοδότηση πράξη, σύμφωνα με το άρθρο 57, για τη συμπλήρωση του παρόντος κανονισμού, προσδιορίζοντας περαιτέρω τα κριτήρια που προβλέπονται στην παράγραφο 2 του παρόντος άρθρου έως τις 17 Ιουλίου 2024.

7. Ο ορισμός που αναφέρεται στην παράγραφο 1 στοιχείο α) δεν χρησιμοποιείται έως ότου η Επιτροπή εκδώσει κατ' εξουσιοδότηση πράξη σύμφωνα με την παράγραφο 6.

8. Ο ορισμός που αναφέρεται στην παράγραφο 1 στοιχείο α) δεν εφαρμόζεται στα ακόλουθα:

i) χρηματοοικονομικές οντότητες που παρέχουν υπηρεσίες ΤΠΕ σε άλλες χρηματοοικονομικές οντότητες,

ii) τρίτους παρόχους υπηρεσιών ΤΠΕ που υπόκεινται σε πλαίσια εποπτείας, τα οποία έχουν θεσπιστεί με σκοπό την υποστήριξη των καθηκόντων που αναφέρονται στο άρθρο 127 παράγραφος 2 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης,

iii) ενδοομιλικούς παρόχους υπηρεσιών ΤΠΕ,

iv) τρίτους παρόχους υπηρεσιών ΤΠΕ που παρέχουν υπηρεσίες ΤΠΕ αποκλειστικά σε ένα κράτος μέλος σε χρηματοοικονομικές οντότητες που δραστηριοποιούνται μόνο στο εν λόγω κράτος μέλος.

9. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, καταρτίζουν, δημοσιεύουν και επικαιροποιούν ετησίως τον κατάλογο των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ σε επίπεδο Ένωσης.

10. Για τους σκοπούς της παραγράφου 1 στοιχείο α), οι αρμόδιες αρχές διαβιβάζουν, σε ετήσια και συγκεντρωτική βάση, τις εκθέσεις που αναφέρονται στο άρθρο 28 παράγραφος 3 τρίτο εδάφιο στο φόρουμ εποπτείας, το οποίο συγκροτείται σύμφωνα με το άρθρο 32. Το φόρουμ εποπτείας αξιολογεί τις εξαρτήσεις των τρίτων παρόχων ΤΠΕ από χρηματοοικονομικές οντότητες βάσει των πληροφοριών που λαμβάνει από τις αρμόδιες αρχές.

11. Οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που δεν περιλαμβάνονται στον κατάλογο που αναφέρεται στην παράγραφο 9 μπορούν να ζητήσουν να οριστούν ως κρίσιμοι σύμφωνα με την παράγραφο 1 στοιχείο α).

Για τους σκοπούς του πρώτου εδαφίου, ο τρίτος πάροχος υπηρεσιών ΤΠΕ υποβάλλει αιτιολογημένη αίτηση στην ΕΑΤ, την ΕΑΚΑΑ ή την ΕΑΑΕΣ, οι οποίες αποφασίζουν, μέσω της μεικτής επιτροπής, αν ο εν λόγω τρίτος πάροχος υπηρεσιών ΤΠΕ θα οριστεί ως κρίσιμος σύμφωνα με την παράγραφο 1 στοιχείο α).

Η απόφαση που αναφέρεται στο δεύτερο εδάφιο εκδίδεται και κοινοποιείται στον τρίτο πάροχο υπηρεσιών ΤΠΕ εντός 6 μηνών από την παραλαβή της αίτησης.

12. Οι χρηματοοικονομικές οντότητες χρησιμοποιούν τις υπηρεσίες τρίτου παρόχου υπηρεσιών ΤΠΕ που είναι εγκατεστημένος σε τρίτη χώρα και έχει οριστεί ως κρίσιμος, σύμφωνα με την παράγραφο 1 στοιχείο α) μόνο εφόσον ο εν λόγω πάροχος έχει εγκαταστήσει θυγατρική στην Ένωση εντός των 12 μηνών μετά τον ορισμό.

13. Ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ που αναφέρεται στην παράγραφο 12 κοινοποιεί στον κύριο εποπτικό φορέα τυχόν αλλαγές στη δομή της διοίκησης της θυγατρικής που είναι εγκατεστημένη στην Ένωση.

Άρθρο 32

Δομή του πλαισίου εποπτείας

1. Η μεικτή επιτροπή συγκροτεί, σύμφωνα με το άρθρο 57 παράγραφος 1 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010, το φόρουμ εποπτείας ως υποεπιτροπή για τους σκοπούς της υποστήριξης των εργασιών της μεικτής επιτροπής και του κύριου εποπτικού φορέα που αναφέρεται στο άρθρο 31 παράγραφος 1 στοιχείο β) όσον αφορά τους κινδύνους τρίτων παρόχων ΤΠΕ σε όλους τους χρηματοοικονομικούς τομείς. Το φόρουμ εποπτείας καταρτίζει τα σχέδια κοινών θέσεων και τα σχέδια κοινών πράξεων της μεικτής επιτροπής στο πεδίο αυτό.

Το φόρουμ εποπτείας συζητά τακτικά τις σχετικές εξελίξεις όσον αφορά τους κινδύνους και τις ευπάθειες των ΤΠΕ και προωθεί την υιοθέτηση συνεκτικής προσέγγισης για την παρακολούθηση των κινδύνων τρίτων παρόχων ΤΠΕ στο επίπεδο της Ένωσης.

2. Το φόρουμ εποπτείας προβαίνει ετησίως σε συλλογική αξιολόγηση των αποτελεσμάτων και των ευρημάτων των εποπτικών δραστηριοτήτων που διεξάγονται για όλους τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ και προωθεί μέτρα συντονισμού με σκοπό την αύξηση της ψηφιακής επιχειρησιακής ανθεκτικότητας των χρηματοοικονομικών οντοτήτων, την προώθηση βέλτιστων πρακτικών αντιμετώπισης του κινδύνου συγκέντρωσης ΤΠΕ και τη διερεύνηση μέσων μετριασμού σε περιπτώσεις διατομεακής μεταφοράς κινδύνων.

3. Το φόρουμ εποπτείας υποβάλλει γενικούς δείκτες αναφοράς για κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ προς έγκριση από τη μεικτή επιτροπή ως κοινές θέσεις των ΕΕΑ, σύμφωνα με το άρθρο 56 παράγραφος 1 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

4. Το φόρουμ εποπτείας απαρτίζεται από:

α) τους προέδρους των ΕΕΑ,

β) έναν υψηλόβαθμο εκπρόσωπο από κάθε κράτος μέλος, προερχόμενο από το εν ενεργεία προσωπικό της σχετικής αρμόδιας αρχής που αναφέρεται στο άρθρο 46,

γ) τους εκτελεστικούς διευθυντές κάθε ΕΕΑ και έναν εκπρόσωπο από την Επιτροπή, το ΕΣΣΚ, την ΕΚΤ και τον ENISA ως παρατηρητές,

δ) κατά περίπτωση, έναν επιπλέον εκπρόσωπο αρμόδιας αρχής που αναφέρεται στο άρθρο 46 από κάθε κράτος μέλος ως παρατηρητή,

ε) κατά περίπτωση, έναν εκπρόσωπο των αρμόδιων αρχών που ορίζονται ή συστήνονται σύμφωνα με την οδηγία (ΕΕ) 2022/2555 αρμόδιο για την εποπτεία βασικής ή σημαντικής οντότητας που υπόκειται στις διατάξεις της εν λόγω οδηγίας, και η οποία έχει οριστεί ως κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ, ως παρατηρητής.

Το φόρουμ εποπτείας μπορεί, κατά περίπτωση, να ζητεί τη γνώμη ανεξάρτητων εμπειρογνωμόνων που διορίζονται σύμφωνα με την παράγραφο 6.

5. Κάθε κράτος μέλος ορίζει τη σχετική αρμόδια αρχή της οποίας το μέλος του προσωπικού είναι ο υψηλόβαθμος εκπρόσωπος που αναφέρεται στην παράγραφο 4 πρώτο εδάφιο στοιχείο β), και ενημερώνει σχετικά τον κύριο εποπτικό φορέα.

Οι ΕΕΑ δημοσιεύουν στον ιστότοπό τους τον κατάλογο των υψηλόβαθμων εκπροσώπων προερχόμενων από το εν ενεργεία προσωπικό της σχετικής αρμόδιας αρχής που ορίζονται από τα κράτη μέλη.

6. Το φόρουμ εποπτείας ορίζει τους αναφερόμενους στην παράγραφο 4 δεύτερο εδάφιο ανεξάρτητους εμπειρογνώμονες από ομάδα εμπειρογνωμόνων που επιλέγονται με δημόσια και διαφανή διαδικασία υποβολής αιτήσεων.

Οι ανεξάρτητοι εμπειρογνώμονες διορίζονται με βάση την εμπειρογνωσία τους σε θέματα χρηματοοικονομικής σταθερότητας, ψηφιακής επιχειρησιακής ανθεκτικότητας και ασφάλειας. Ενεργούν ανεξάρτητα και αντικειμενικά αποκλειστικά προς το συμφέρον της Ένωσης συνολικά και ούτε ζητούν ούτε δέχονται οδηγίες από θεσμικά όργανα ή οργανισμούς της Ένωσης, από οποιαδήποτε κυβέρνηση κράτους μέλους ή από οποιονδήποτε άλλον δημόσιο ή ιδιωτικό φορέα.

7. Σύμφωνα με το άρθρο 16 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010, οι ΕΕΑ έως τις 17 Ιουλίου 2024 εκδίδουν, για τους σκοπούς του παρόντος τμήματος, κατευθυντήριες γραμμές σχετικά με τη συνεργασία μεταξύ των ΕΕΑ και των αρμόδιων αρχών οι οποίες καλύπτουν τις λεπτομερείς διαδικασίες και προϋποθέσεις για την κατανομή και την εκτέλεση των καθηκόντων μεταξύ των αρμόδιων αρχών και των ΕΕΑ, καθώς και τις λεπτομέρειες σχετικά με την ανταλλαγή των πληροφοριών οι οποίες είναι απαραίτητες για τις αρμόδιες αρχές, προκειμένου να διασφαλιστεί ότι δίνεται συνέχεια στις συστάσεις που απευθύνονται σύμφωνα με το άρθρο 35 παράγραφος 1 στοιχείο δ) σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ.

8. Οι απαιτήσεις που ορίζονται στο παρόν τμήμα δεν θίγουν την εφαρμογή της οδηγίας (ΕΕ) 2022/2555 και άλλων κανόνων της Ένωσης για την εποπτεία που εφαρμόζεται σε παρόχους υπηρεσιών υπολογιστικού νέφους.

9. Οι ΕΕΑ, μέσω της μεικτής επιτροπής και βάσει των προπαρασκευαστικών εργασιών που διεξάγονται από το φόρουμ εποπτείας, υποβάλλουν ετησίως στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Επιτροπή έκθεση σχετικά με την εφαρμογή του παρόντος τμήματος.

Άρθρο 33

Καθήκοντα του κύριου εποπτικού φορέα

1. Ο κύριος εποπτικός φορέας, ο οποίος διορίζεται σύμφωνα με το άρθρο 31 παράγραφος 1 στοιχείο β), ασκεί την εποπτεία των τρίτων παρόχων υπηρεσιών ΤΠΕ που του έχουν ανατεθεί, και είναι, για τους σκοπούς όλων των θεμάτων που σχετίζονται με την εποπτεία, το κύριο σημείο επαφής για τους εν λόγω κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ.

2. Για τους σκοπούς της παραγράφου 1, ο κύριος εποπτικός φορέας αξιολογεί αν κάθε κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ διαθέτει εμπεριστατωμένους, ορθούς και αποτελεσματικούς κανόνες, διαδικασίες, μηχανισμούς και ρυθμίσεις για τη διαχείριση του κινδύνου ΤΠΕ στον οποίο ενδέχεται να εκθέτει τις χρηματοοικονομικές οντότητες.

Η αξιολόγηση που αναφέρεται στο πρώτο εδάφιο επικεντρώνεται κυρίως στις υπηρεσίες ΤΠΕ που παρέχονται από τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ και υποστηρίζουν τις κρίσιμες ή σημαντικές λειτουργίες των χρηματοοικονομικών οντοτήτων. Όταν είναι αναγκαίο για την αντιμετώπιση όλων των σχετικών κινδύνων, η εν λόγω αξιολόγηση επεκτείνεται σε υπηρεσίες ΤΠΕ που υποστηρίζουν λειτουργίες πέραν των κρίσιμων ή σημαντικών.

3. Η αξιολόγηση που αναφέρεται στην παράγραφο 2 καλύπτει:

α) απαιτήσεις ΤΠΕ για τη διασφάλιση, ιδίως, της ασφάλειας, της διαθεσιμότητας, της συνέχειας, της επεκτασιμότητας και της ποιότητας των υπηρεσιών που παρέχει ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ σε χρηματοοικονομικές οντότητες, καθώς και την ικανότητα να διατηρεί ανά πάσα στιγμή υψηλά πρότυπα διαθεσιμότητας, γνησιότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων,

β) την υλική ασφάλεια που συμβάλλει στη διασφάλιση της ασφάλειας των ΤΠΕ, συμπεριλαμβανομένης της ασφάλειας των χώρων, των εγκαταστάσεων, των κέντρων δεδομένων,

γ) τις διαδικασίες διαχείρισης κινδύνων, συμπεριλαμβανομένων των πολιτικών για τη διαχείριση κινδύνων ΤΠΕ και της πολιτικής επιχειρησιακής συνέχειας των ΤΠΕ και των σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ,

δ) τις ρυθμίσεις διακυβέρνησης, συμπεριλαμβανομένης της οργανωτικής δομής με σαφείς, διαφανείς και συνεκτικούς κανόνες για τα όρια αρμοδιότητας και λογοδοσίας που καθιστούν δυνατή την αποτελεσματική διαχείριση κινδύνων ΤΠΕ,

ε) τον προσδιορισμό, την παρακολούθηση και την έγκαιρη αναφορά σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ στις χρηματοοικονομικές οντότητες, τη διαχείριση και την επίλυση των συμβάντων αυτών, ιδίως κυβερνοεπιθέσεων,

στ) τους μηχανισμούς φορητότητας δεδομένων, φορητότητας εφαρμογών και διαλειτουργικότητας, οι οποίοι διασφαλίζουν την αποτελεσματική άσκηση δικαιωμάτων καταγγελίας από τις χρηματοοικονομικές οντότητες,

ζ) τη δοκιμή συστημάτων, υποδομών και δικλείδων ασφάλειας ΤΠΕ,

η) τους ελέγχους ΤΠΕ,

θ) τη χρήση σχετικών εθνικών και διεθνών προτύπων που ισχύουν για την παροχή των υπηρεσιών ΤΠΕ στις χρηματοοικονομικές οντότητες.

4. Με βάση την αξιολόγηση που αναφέρεται στην παράγραφο 2 και σε συντονισμό με το δίκτυο κοινής εποπτείας (ΔΚΕ) που αναφέρεται στο άρθρο 34 παράγραφος 1, ο κύριος εποπτικός φορέας εγκρίνει σαφές, λεπτομερές και τεκμηριωμένο εξατομικευμένο σχέδιο εποπτείας στο οποίο περιγράφονται οι ετήσιοι στόχοι εποπτείας και οι κύριες δράσεις εποπτείας που σχεδιάζονται για κάθε κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ. Το σχέδιο αυτό κοινοποιείται ετησίως στον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ.

Πριν από την έγκριση του σχεδίου εποπτείας, ο κύριος εποπτικός φορέας κοινοποιεί το προσχέδιο εποπτείας στον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ.

Μετά την παραλαβή του προσχεδίου εποπτείας, ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ μπορεί να υποβάλει αιτιολογημένη δήλωση εντός 15 ημερολογιακών ημερών, αποδεικνύοντας τον αναμενόμενο αντίκτυπο στους πελάτες που είναι οντότητες οι οποίες δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού και, κατά περίπτωση, διατυπώνοντας λύσεις για τον μετριασμό των κινδύνων.

5. Μόλις εγκριθούν τα ετήσια σχέδια εποπτείας που αναφέρονται στην παράγραφο 4 και κοινοποιηθούν στους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, οι αρμόδιες αρχές δύνανται να λάβουν μέτρα για τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ μόνο κατόπιν συμφωνίας με τον κύριο εποπτικό φορέα.

Άρθρο 34

Επιχειρησιακός συντονισμός μεταξύ κύριων εποπτικών φορέων

1. Για να εξασφαλιστεί συνεπής προσέγγιση των δραστηριοτήτων εποπτείας και με σκοπό να καταστούν δυνατές συντονισμένες στρατηγικές γενικής εποπτείας και συνεκτικές επιχειρησιακές προσεγγίσεις και μεθοδολογίες εργασίας, οι τρεις κύριοι εποπτικοί φορείς, οι οποίοι διορίζονται σύμφωνα με το άρθρο 31 παράγραφος 1 στοιχείο β), συγκροτούν ΔΚΕ, ώστε να συντονίζονται μεταξύ τους κατά τα προπαρασκευαστικά στάδια και να συντονίζουν τη διεξαγωγή των δραστηριοτήτων εποπτείας επί των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ τους οποίους επιβλέπουν αντίστοιχα, καθώς και σχετικά με κάθε τρόπο δράσης που ενδέχεται να απαιτείται σύμφωνα με το άρθρο 42.

2. Για τους σκοπούς της παραγράφου 1, οι κύριοι εποπτικοί φορείς καταρτίζουν κοινό πρωτόκολλο εποπτείας στο οποίο καθορίζονται οι λεπτομερείς διαδικασίες που πρέπει να ακολουθούνται για τη διεξαγωγή του καθημερινού συντονισμού και για τη διασφάλιση ταχειών ανταλλαγών και αντιδράσεων. Το πρωτόκολλο αναθεωρείται περιοδικά ώστε να αντικατοπτρίζει τις επιχειρησιακές ανάγκες, ιδίως την εξέλιξη των πρακτικών ρυθμίσεων εποπτείας.

3. Οι κύριοι εποπτικοί φορείς μπορούν, σε ad hoc βάση, να καλούν την ΕΚΤ και τον ENISA να παρέχουν τεχνικές συμβουλές, να ανταλλάσσουν πρακτικές εμπειρίες ή να συμμετέχουν σε ειδικές συντονιστικές συνεδριάσεις του ΔΚΕ.

Άρθρο 35

Εξουσίες του κύριου εποπτικού φορέα

1. Για τους σκοπούς της εκτέλεσης των καθηκόντων που προβλέπονται στο παρόν τμήμα, ο κύριος εποπτικός φορέας διαθέτει τις ακόλουθες εξουσίες όσον αφορά τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ:

α) να ζητεί όλες τις σχετικές πληροφορίες και τα έγγραφα τεκμηρίωσης σύμφωνα με το άρθρο 37,

β) να διενεργεί γενικές έρευνες και επιθεωρήσεις σύμφωνα με τα άρθρα 38 και 39, αντίστοιχα,

γ) να ζητεί την υποβολή εκθέσεων μετά την ολοκλήρωση των εποπτικών δραστηριοτήτων, στις οποίες προσδιορίζονται οι ενέργειες που υλοποίησαν ή τα διορθωτικά μέτρα που έλαβαν οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ όσον αφορά τις συστάσεις που αναφέρονται στο στοιχείο δ) της παρούσας παραγράφου,

δ) να διατυπώνει συστάσεις για τους τομείς που αναφέρονται στο άρθρο 33 παράγραφος 3, ιδίως όσον αφορά τα ακόλουθα:

i) τη χρήση συγκεκριμένων απαιτήσεων ή διαδικασιών ασφάλειας και ποιότητας ΤΠΕ, ιδίως όσον αφορά τη σταδιακή υλοποίηση ενημερώσεων κώδικα, επικαιροποιήσεων, κρυπτογράφησης και άλλων μέτρων ασφάλειας τα οποία ο κύριος εποπτικός φορέας θεωρεί συναφή για τη διασφάλιση της ασφάλειας των υπηρεσιών ΤΠΕ που παρέχονται στις χρηματοοικονομικές οντότητες,

ii) τη χρήση όρων και προϋποθέσεων, συμπεριλαμβανομένης της τεχνικής εφαρμογής τους, σύμφωνα με τις οποίες οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ παρέχουν υπηρεσίες ΤΠΕ σε χρηματοοικονομικές οντότητες, τις οποίες ο κύριος εποπτικός φορέας θεωρεί συναφείς για την αποτροπή της δημιουργίας μοναδικών σημείων αποτυχίας, ή την ενίσχυσή τους, ή για την ελαχιστοποίηση των πιθανών συστημικών επιπτώσεων στον χρηματοοικονομικό τομέα της Ένωσης σε περίπτωση κινδύνου συγκέντρωσης ΤΠΕ,

iii) κάθε προγραμματισμένη υπεργολαβία, όταν ο κύριος εποπτικός φορέας θεωρεί ότι η περαιτέρω υπεργολαβία, συμπεριλαμβανομένων των ρυθμίσεων υπεργολαβικής ανάθεσης τις οποίες οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ προγραμματίζουν να συνάψουν με άλλους τρίτους παρόχους υπηρεσιών ΤΠΕ ή με υπεργολάβους ΤΠΕ εγκατεστημένους σε τρίτη χώρα, ενδέχεται να ενεργοποιήσει κινδύνους όσον αφορά την παροχή υπηρεσιών από τη χρηματοοικονομική οντότητα ή κινδύνους για τη χρηματοοικονομική σταθερότητα, βάσει της εξέτασης των πληροφοριών που συλλέγονται σύμφωνα με τα άρθρα 37 και 38,

iv) την αποτροπή σύναψης περαιτέρω ρύθμισης υπεργολαβίας, εφόσον πληρούνται οι ακόλουθες σωρευτικές προϋποθέσεις:

— ο προβλεπόμενος υπεργολάβος είναι τρίτος πάροχος υπηρεσιών ΤΠΕ ή υπεργολάβος ΤΠΕ εγκατεστημένος σε τρίτη χώρα,

— η υπεργολαβία αφορά κρίσιμη ή σημαντική λειτουργία της χρηματοοικονομικής οντότητας και

— ο κύριος εποπτικός φορέας θεωρεί ότι η χρήση της εν λόγω υπεργολαβίας ενέχει σαφή και σοβαρό κίνδυνο για τη χρηματοοικονομική σταθερότητα της Ένωσης ή για τις χρηματοοικονομικές οντότητες, συμπεριλαμβανομένης της ικανότητας των χρηματοοικονομικών οντοτήτων να συμμορφώνονται με τις εποπτικές απαιτήσεις.

Για τους σκοπούς του σημείου iv) του παρόντος στοιχείου, οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ, χρησιμοποιώντας το υπόδειγμα που προβλέπεται στο άρθρο 41 παράγραφος 1 στοιχείο β), διαβιβάζουν τις πληροφορίες σχετικά με την υπεργολαβία στον κύριο εποπτικό φορέα.

2. Κατά την άσκηση των εξουσιών που αναφέρονται στο παρόν άρθρο, ο κύριος εποπτικός φορέας:

α) διασφαλίζει τον τακτικό συντονισμό εντός του ΔΚΕ και, ειδικότερα, επιδιώκει συνεκτικές προσεγγίσεις, κατά περίπτωση, όσον αφορά την εποπτεία κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ,

β) λαμβάνει δεόντως υπόψη το πλαίσιο που θεσπίζεται με την οδηγία (ΕΕ) 2022/2555 και, όπου κρίνεται αναγκαίο, διαβουλεύεται με τις σχετικές αρμόδιες αρχές που ορίζονται ή συστήνονται σύμφωνα με την εν λόγω οδηγία, προκειμένου να αποφευχθεί η επικάλυψη τεχνικών και οργανωτικών μέτρων που ενδέχεται να εφαρμόζονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ σύμφωνα με την εν λόγω οδηγία,

γ) επιδιώκει να ελαχιστοποιήσει, στο μέτρο του δυνατού, τον κίνδυνο διαταραχής των υπηρεσιών που παρέχονται από κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ σε πελάτες που είναι οντότητες οι οποίες δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού.

3. Ο κύριος εποπτικός φορέας ζητεί τη γνώμη του φόρουμ εποπτείας πριν από την άσκηση των εξουσιών που αναφέρονται στην παράγραφο 1.

Πριν από τη διατύπωση συστάσεων σύμφωνα με την παράγραφο 1 στοιχείο δ), ο κύριος εποπτικός φορέας δίνει στον τρίτο πάροχο υπηρεσιών ΤΠΕ την ευκαιρία να παράσχει, εντός 30 ημερολογιακών ημερών, σχετικές πληροφορίες που αποδεικνύουν τον αναμενόμενο αντίκτυπο στους πελάτες που είναι οντότητες οι οποίες δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού, διατυπώνοντας, κατά περίπτωση, λύσεις για τον μετριασμό των κινδύνων.

4. Ο κύριος εποπτικός φορέας ενημερώνει το ΔΚΕ για το αποτέλεσμα της άσκησης των εξουσιών που αναφέρονται στην παράγραφο 1 στοιχεία α) και β). Ο κύριος εποπτικός φορέας διαβιβάζει, χωρίς αδικαιολόγητη καθυστέρηση, τις εκθέσεις που αναφέρονται στην παράγραφο 1 στοιχείο γ), στο ΔΚΕ και στις αρμόδιες αρχές των χρηματοοικονομικών οντοτήτων που χρησιμοποιούν τις υπηρεσίες ΤΠΕ του εν λόγω κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ.

5. Οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ συνεργάζονται καλόπιστα με τον κύριο εποπτικό φορέα και του παρέχουν τη συνδρομή τους κατά την εκπλήρωση των καθηκόντων του.

6. Σε περίπτωση ολικής ή μερικής μη συμμόρφωσης με τα μέτρα που απαιτείται να ληφθούν σύμφωνα με την εκτέλεση των εξουσιών δυνάμει της παραγράφου 1 στοιχεία α), β) και γ), και μετά την εκπνοή περιόδου τουλάχιστον 30 ημερολογιακών ημερών από την ημερομηνία κατά την οποία ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ έλαβε κοινοποίηση των αντίστοιχων μέτρων, ο κύριος εποπτικός φορέας εκδίδει απόφαση με την οποία επιβάλλει περιοδική χρηματική ποινή για να υποχρεώσει τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ να συμμορφωθεί με τα εν λόγω μέτρα.

7. Η περιοδική χρηματική ποινή που αναφέρεται στην παράγραφο 6 επιβάλλεται σε ημερήσια βάση έως ότου επιτευχθεί συμμόρφωση και για μέγιστο διάστημα έξι μηνών από την κοινοποίηση της απόφασης επιβολής περιοδικής χρηματικής ποινής στον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ.

8. Το ύψος της περιοδικής χρηματικής ποινής, το οποίο υπολογίζεται από την ημερομηνία που ορίζεται στην απόφαση επιβολής της περιοδικής χρηματικής ποινής, ανέρχεται έως το 1 % του μέσου ημερήσιου κύκλου εργασιών που πραγματοποίησε παγκοσμίως ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ κατά την προηγούμενη χρήση. Κατά τον καθορισμό του ποσού της χρηματικής ποινής, ο κύριος εποπτικός φορέας λαμβάνει υπόψη τα ακόλουθα κριτήρια όσον αφορά τη μη συμμόρφωση με τα μέτρα που αναφέρονται στην παράγραφο 6:

α) τη βαρύτητα και τη διάρκεια της μη συμμόρφωσης,

β) αν η μη συμμόρφωση τελέστηκε εκ προθέσεως ή εξ αμελείας,

γ) το επίπεδο συνεργασίας του τρίτου παρόχου υπηρεσιών ΤΠΕ με τον κύριο εποπτικό φορέα.

Για τους σκοπούς του πρώτου εδαφίου, προκειμένου να διασφαλιστεί συνεκτική προσέγγιση, ο κύριος εποπτικός φορέας προβαίνει σε διαβούλευση στο πλαίσιο του ΔΚΕ.

9. Οι χρηματικές ποινές έχουν διοικητικό χαρακτήρα και είναι εκτελεστές. Η εκτέλεση διέπεται από τους κανόνες της πολιτικής δικονομίας που ισχύουν στο κράτος μέλος στο οποίο πραγματοποιούνται οι επιθεωρήσεις και η πρόσβαση. Τα δικαστήρια του οικείου κράτους μέλους είναι αρμόδια για καταγγελίες που αφορούν την παράτυπη διενέργεια της εκτέλεσης. Τα ποσά των χρηματικών ποινών διοχετεύονται στον γενικό προϋπολογισμό της Ευρωπαϊκής Ένωσης.

10. Ο κύριος εποπτικός φορέας δημοσιοποιεί κάθε περιοδική χρηματική ποινή που έχει επιβληθεί, εκτός εάν η εν λόγω δημοσιοποίηση θέτει σε σοβαρό κίνδυνο τις χρηματοοικονομικές αγορές ή προκαλεί δυσανάλογη ζημία στα εμπλεκόμενα μέρη.

11. Πριν από την επιβολή περιοδικής χρηματικής ποινής σύμφωνα με την παράγραφο 6, ο κύριος εποπτικός φορέας παρέχει στους εκπροσώπους του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ που υπόκειται στην πειθαρχική διαδικασία, τη δυνατότητα να εκθέσουν την άποψή τους σχετικά με τα ευρήματα και στηρίζει τις αποφάσεις του μόνο σε ευρήματα για τα οποία είχε την ευκαιρία να διατυπώσει παρατηρήσεις ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ που υπόκειται στην πειθαρχική διαδικασία.

Κατά τη διεξαγωγή της διαδικασίας διασφαλίζονται πλήρως τα δικαιώματα υπεράσπισης των προσώπων που υπόκεινται σε πειθαρχικές διαδικασίες. Ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ που υπόκειται στην εν λόγω διαδικασία έχει δικαίωμα πρόσβασης στον φάκελο, με την επιφύλαξη του έννομου συμφέροντος άλλων προσώπων για την προστασία του επιχειρηματικού απορρήτου τους. Το δικαίωμα πρόσβασης στον φάκελο δεν καλύπτει τις εμπιστευτικές πληροφορίες ή τα προπαρασκευαστικά έγγραφα εσωτερικής χρήσης του κύριου εποπτικού φορέα.

Άρθρο 36

Άσκηση των εξουσιών του κύριου εποπτικού φορέα εκτός της Ένωσης

1. Όταν οι στόχοι εποπτείας δεν μπορούν να επιτευχθούν μέσω αλληλεπίδρασης με τη θυγατρική που έχει συσταθεί για τους σκοπούς του άρθρου 31 παράγραφος 12 ή μέσω άσκησης δραστηριοτήτων εποπτείας σε εγκαταστάσεις που βρίσκονται στην Ένωση, ο κύριος εποπτικός φορέας μπορεί να ασκεί τις εξουσίες που αναφέρονται στις ακόλουθες διατάξεις σε κάθε χώρο που βρίσκεται σε τρίτη χώρα και ανήκει ή χρησιμοποιείται με οποιονδήποτε τρόπο, με σκοπό την παροχή υπηρεσιών σε χρηματοοικονομικές οντότητες της Ένωσης, από κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ, σε σχέση με τις οικείες επιχειρηματικές δραστηριότητες, τις λειτουργίες ή τις υπηρεσίες, μεταξύ άλλων, τυχόν διοικητικές, τις επιχειρήσεις ή τα επιχειρησιακά γραφεία, τις εγκαταστάσεις, τις εκτάσεις, τα κτίρια ή άλλα ακίνητα:

α) στο άρθρο 35 παράγραφος 1 στοιχείο α) και

β) στο άρθρο 35 παράγραφος 1 στοιχείο β), σύμφωνα με το άρθρο 38 παράγραφος 2 στοιχεία α), β) και δ), και στο άρθρο 39 παράγραφος 1 και στο άρθρο 39 παράγραφος 2 στοιχείο α).

Οι εξουσίες που αναφέρονται στο πρώτο εδάφιο μπορούν να ασκούνται υπό όλες τις ακόλουθες προϋποθέσεις:

i) η διενέργεια επιθεώρησης σε τρίτη χώρα κρίνεται αναγκαία από τον κύριο εποπτικό φορέα, ώστε να είναι σε θέση να εκτελεί πλήρως και αποτελεσματικά τα καθήκοντά του δυνάμει του παρόντος κανονισμού,

ii) η επιθεώρηση σε τρίτη χώρα σχετίζεται άμεσα με την παροχή υπηρεσιών ΤΠΕ σε χρηματοοικονομικές οντότητες στην Ένωση,

iii) ο εν λόγω κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ συναινεί στη διενέργεια επιθεώρησης σε τρίτη χώρα και

iv) η αρμόδια αρχή της οικείας τρίτης χώρας έχει ενημερωθεί επίσημα από τον κύριο εποπτικό φορέα και δεν εγείρει αντιρρήσεις.

2. Με την επιφύλαξη των αντίστοιχων αρμοδιοτήτων των θεσμικών οργάνων της Ένωσης και των κρατών μελών, για τους σκοπούς της παραγράφου 1, η ΕΑΤ, η ΕΑΚΑΑ ή η ΕΑΑΕΣ, συνάπτουν συμφωνίες διοικητικής συνεργασίας με την αρμόδια αρχή της τρίτης χώρας, προκειμένου να καταστεί δυνατή η ομαλή διεξαγωγή των επιθεωρήσεων στη συγκεκριμένη τρίτη χώρα από τον κύριο εποπτικό φορέα και την ομάδα του που έχει οριστεί για την αποστολή στην εν λόγω τρίτη χώρα. Οι εν λόγω ρυθμίσεις συνεργασίας δεν δημιουργούν νομικές υποχρεώσεις έναντι της Ένωσης και των κρατών μελών της ούτε εμποδίζουν τα κράτη μέλη και τις αρμόδιες αρχές τους να συνάπτουν διμερείς ή πολυμερείς ρυθμίσεις με τις εν λόγω τρίτες χώρες και τις οικείες αρχές τους.

Οι εν λόγω ρυθμίσεις συνεργασίας προσδιορίζουν τουλάχιστον τα ακόλουθα στοιχεία:

α) τις διαδικασίες για τον συντονισμό των δραστηριοτήτων εποπτείας που διεξάγονται δυνάμει του παρόντος κανονισμού και κάθε ανάλογη παρακολούθηση των κινδύνων τρίτων μερών ΤΠΕ στον χρηματοοικονομικό τομέα που ασκείται από τη σχετική αρχή της οικείας τρίτης χώρας, συμπεριλαμβανομένων λεπτομερειών για τη διαβίβαση της συμφωνίας της τρίτης χώρας, ώστε να καταστεί δυνατή η διεξαγωγή, από τον κύριο εποπτικό φορέα και την ορισθείσα ομάδα του, γενικών ερευνών και επιτόπιων επιθεωρήσεων, όπως αναφέρεται στην παράγραφο 1 πρώτο εδάφιο, στην επικράτεια υπό τη δικαιοδοσία της,

β) τον μηχανισμό για τη διαβίβαση κάθε σχετικής πληροφορίας μεταξύ της ΕΑΤ, της ΕΑΚΑΑ ή της ΕΑΑΕΣ και της σχετικής αρχής της συγκεκριμένης τρίτης χώρας, ιδίως σε σχέση με τις πληροφορίες που μπορεί να ζητήσει ο κύριος εποπτικός φορέας σύμφωνα με το άρθρο 37,

γ) τους μηχανισμούς για την άμεση κοινοποίηση από την αρμόδια αρχή της οικείας τρίτης χώρας στην ΕΑΤ, την ΕΑΚΑΑ ή την ΕΑΑΕΣ των περιπτώσεων κατά τις οποίες ένας τρίτος πάροχος υπηρεσιών ΤΠΕ που είναι εγκατεστημένος σε τρίτη χώρα και έχει οριστεί ως κρίσιμος σύμφωνα με το άρθρο 31 παράγραφος 1 στοιχείο α), θεωρείται ότι έχει παραβιάσει τις απαιτήσεις τις οποίες υποχρεούται να τηρεί σύμφωνα με το εφαρμοστέο δίκαιο της συγκεκριμένης τρίτης χώρας κατά την παροχή υπηρεσιών σε χρηματοοικονομικά ιδρύματα στην εν λόγω τρίτη χώρα, καθώς και τα διορθωτικά μέτρα και τις κυρώσεις που επιβλήθηκαν,

δ) την τακτική διαβίβαση επικαιροποιήσεων σχετικά με τις ρυθμιστικές ή εποπτικές εξελίξεις όσον αφορά την παρακολούθηση των κινδύνων τρίτων μερών ΤΠΕ για χρηματοοικονομικά ιδρύματα στη συγκεκριμένη τρίτη χώρα,

ε) τις λεπτομέρειες που επιτρέπουν, εφόσον απαιτείται, τη συμμετοχή ενός εκπροσώπου της αρμόδιας αρχής της τρίτης χώρας στις επιθεωρήσεις που διενεργούνται από τον κύριο εποπτικό φορέα και την ορισθείσα ομάδα.

3. Όταν ο κύριος εποπτικός φορέας δεν είναι σε θέση να διεξάγει εποπτικές δραστηριότητες, που αναφέρονται στις παραγράφους 1 και 2, ο κύριος εποπτικός φορέας:

α) ασκεί τις εξουσίες της δυνάμει του άρθρου 35 με βάση όλα τα πραγματικά περιστατικά και τα έγγραφα που έχει στη διάθεσή του,

β) τεκμηριώνει και εξηγεί κάθε συνέπεια της αδυναμίας του να διεξαγάγει τις προβλεπόμενες δραστηριότητες εποπτείας που αναφέρονται στο παρόν άρθρο.

Οι πιθανές συνέπειες που αναφέρονται στο στοιχείο β) του παρόντος εδαφίου λαμβάνονται υπόψη στις συστάσεις του κύριου εποπτικού φορέα που εκδίδονται σύμφωνα με το άρθρο 35 παράγραφος 1 στοιχείο δ).

Άρθρο 37

Αίτηση παροχής πληροφοριών

1. Ο κύριος εποπτικός φορέας δύναται να ζητήσει από τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ, με απλό αίτημα ή με απόφαση, να παράσχει όλες τις απαραίτητες πληροφορίες ώστε ο κύριος εποπτικός φορέας να είναι σε θέση να εκτελέσει τα καθήκοντά του σύμφωνα με τον παρόντα κανονισμό, συμπεριλαμβανομένων όλων των σχετικών επιχειρηματικών ή επιχειρησιακών εγγράφων, των συμβολαίων, των εγγράφων τεκμηρίωσης πολιτικών, των εκθέσεων ελέγχου της ασφάλειας ΤΠΕ, των αναφορών συμβάντων που σχετίζονται με τις ΤΠΕ, καθώς και κάθε πληροφορία σε σχέση με συμβαλλόμενα μέρη στα οποία ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ έχει αναθέσει εξωτερικά επιχειρησιακές λειτουργίες ή δραστηριότητες.

2. Κατά τη διαβίβαση απλού αιτήματος παροχής πληροφοριών δυνάμει της παραγράφου 1, ο κύριος εποπτικός φορέας:

α) παραπέμπει στο παρόν άρθρο ως νομική βάση του αιτήματος,

β) αναφέρει τον σκοπό του αιτήματος,

γ) προσδιορίζει τις πληροφορίες που ζητούνται,

δ) τάσσει προθεσμία εντός της οποίας πρέπει να παρασχεθούν οι πληροφορίες,

ε) ενημερώνει τον εκπρόσωπο του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ από τον οποίο ζητούνται οι πληροφορίες ότι δεν υφίσταται υποχρέωση παροχής πληροφοριών, αλλά ότι στην περίπτωση εκούσιας απάντησης στο αίτημα οι παρεχόμενες πληροφορίες δεν πρέπει να είναι ανακριβείς ή παραπλανητικές.

3. Κατά την υποβολή, κατόπιν αποφάσεως, αιτήματος παροχής πληροφοριών σύμφωνα με την παράγραφο 1, ο κύριος εποπτικός φορέας:

α) παραπέμπει στο παρόν άρθρο ως νομική βάση του αιτήματος,

β) αναφέρει τον σκοπό του αιτήματος,

γ) προσδιορίζει τις πληροφορίες που ζητούνται,

δ) τάσσει προθεσμία εντός της οποίας πρέπει να παρασχεθούν οι πληροφορίες,

ε) επισημαίνει τις περιοδικές χρηματικές ποινές που προβλέπονται στο άρθρο 35 παράγραφος 6 στην περίπτωση ελλιπούς παροχής των απαιτούμενων πληροφοριών ή όταν οι πληροφορίες αυτές δεν παρέχονται εντός της προθεσμίας που αναφέρεται στο στοιχείο δ) του παρόντος εδαφίου,

στ) επισημαίνει το δικαίωμα άσκησης προσφυγής κατά της απόφασης στο συμβούλιο προσφυγών των ΕΕΑ και του δικαιώματος υποβολής αίτησης επανεξέτασης της απόφασης από το Δικαστήριο της Ευρωπαϊκής Ένωσης (Δικαστήριο) σύμφωνα με τα άρθρα 60 και 61 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

4. Οι εκπρόσωποι των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ παρέχουν τις ζητούμενες πληροφορίες. Οι πληροφορίες μπορούν να παρέχονται από δεόντως εξουσιοδοτημένους δικηγόρους εξ ονόματος των πελατών τους. Ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ εξακολουθεί να ευθύνεται πλήρως για την παροχή ελλιπών, ανακριβών ή παραπλανητικών πληροφοριών.

5. Ο κύριος εποπτικός φορέας διαβιβάζει αμελλητί αντίγραφο της απόφασης για την παροχή πληροφοριών στις αρμόδιες αρχές των χρηματοοικονομικών οντοτήτων που χρησιμοποιούν τις υπηρεσίες των σχετικών κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ και στο ΔΚΕ.

Άρθρο 38

Γενικές έρευνες

1. Για την εκτέλεση των καθηκόντων του σύμφωνα με τον παρόντα κανονισμό, ο κύριος εποπτικός φορέας, επικουρούμενος από την κοινή εξεταστική ομάδα που αναφέρεται στο άρθρο 40 παράγραφος 1, μπορεί, εφόσον απαιτείται, να διεξαγάγει τις απαραίτητες έρευνες σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ:

2. Ο κύριος εποπτικός φορέας έχει την εξουσία:

α) να εξετάζει αρχεία, δεδομένα, διαδικασίες και κάθε άλλο συναφές υλικό για την εκτέλεση των καθηκόντων του, ανεξάρτητα από το μέσο στο οποίο αποθηκεύονται,

β) να λαμβάνει ή να αποκτά θεωρημένα αντίγραφα ή αποσπάσματα από τα εν λόγω αρχεία, τα δεδομένα, τις τεκμηριωμένες διαδικασίες και κάθε άλλο υλικό,

γ) να καλεί εκπροσώπους του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ για προφορικές ή γραπτές εξηγήσεις σχετικά με γεγονότα ή έγγραφα που αφορούν το αντικείμενο και τον σκοπό της έρευνας και να καταγράφει τις απαντήσεις,

δ) να εξετάζει κάθε άλλο φυσικό ή νομικό πρόσωπο που συναινεί να ερωτηθεί με σκοπό τη συγκέντρωση πληροφοριών σχετικά με το αντικείμενο της έρευνας,

ε) να ζητεί αρχεία τηλεφωνικών κλήσεων και διαβίβασης δεδομένων.

3. Οι υπάλληλοι και άλλα πρόσωπα που εξουσιοδοτούνται από τον κύριο εποπτικό φορέα για τους σκοπούς της έρευνας, κατά τα οριζόμενα στην παράγραφο 1, ασκούν τις εξουσίες τους επιδεικνύοντας έγγραφη εξουσιοδότηση που ορίζει το αντικείμενο και τον σκοπό της έρευνας.

Στην εν λόγω εξουσιοδότηση επισημαίνονται επίσης οι περιοδικές χρηματικές ποινές που προβλέπονται στο άρθρο 35 παράγραφος 6, όταν τα απαιτούμενα αρχεία, τα δεδομένα, οι τεκμηριωμένες διαδικασίες ή οποιοδήποτε άλλο υλικό, ή οι απαντήσεις σε ερωτήσεις που υποβάλλονται σε εκπροσώπους του τρίτου παρόχου υπηρεσιών ΤΠΕ, δεν παρέχονται ή παρουσιάζουν ελλείψεις.

4. Οι εκπρόσωποι των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ υποχρεούνται να αποδέχονται τις έρευνες βάσει απόφασης του κύριου εποπτικού φορέα. Η απόφαση προσδιορίζει το αντικείμενο και τον σκοπό της έρευνας, τις περιοδικές χρηματικές ποινές που προβλέπονται στο άρθρο 35 παράγραφος 6, τα ένδικα μέσα που διατίθενται δυνάμει των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010, καθώς και το δικαίωμα επανεξέτασης της απόφασης από το Δικαστήριο.

5. Πριν από την έναρξη της έρευνας, ο κύριος εποπτικός φορέας ενημερώνει εγκαίρως την αρμόδια αρχή της χρηματοοικονομικής οντότητας που χρησιμοποιεί τις υπηρεσίες ΤΠΕ του εν λόγω κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ σχετικά με την έρευνα και την ταυτότητα των εξουσιοδοτημένων προσώπων.

Ο κύριος εποπτικός φορέας κοινοποιεί στο ΔΚΕ όλες τις πληροφορίες που μεταβιβάζονται σύμφωνα με το πρώτο εδάφιο.

Άρθρο 39

Επιθεωρήσεις

1. Για την εκπλήρωση των καθηκόντων του σύμφωνα με τον παρόντα κανονισμό, ο κύριος εποπτικός φορέας, επικουρούμενος από τις κοινές εξεταστικές ομάδες που αναφέρονται στο άρθρο 40 παράγραφος 1, μπορεί να εισέλθει και να διενεργήσει όλες τις απαραίτητες επιτόπιες επιθεωρήσεις σε κάθε επιχειρηματικό χώρο, έκταση ή ιδιοκτησία των τρίτων παρόχων υπηρεσιών ΤΠΕ, όπως κεντρικά γραφεία, επιχειρησιακά κέντρα, δευτερεύοντες χώροι, καθώς και να διενεργεί επιθεωρήσεις εξ αποστάσεως.

Για τους σκοπούς της άσκησης των εξουσιών που αναφέρονται στο πρώτο εδάφιο, ο κύριος εποπτικός φορέας συμβουλεύεται το ΔΚΕ.

2. Οι υπάλληλοι και τα λοιπά άτομα που έχουν εξουσιοδοτηθεί από τον κύριο εποπτικό φορέα για τη διενέργεια επιτόπιας επιθεώρησης έχουν την εξουσία:

α) να εισέρχονται σε αυτούς τους επαγγελματικούς χώρους, εκτάσεις ή ακίνητα και

β) να σφραγίζουν κάθε τέτοιο επαγγελματικό χώρο, βιβλία ή έγγραφα κατά την περίοδο και στον βαθμό που απαιτούνται για την επιθεώρηση.

Οι υπάλληλοι και τα λοιπά άτομα που έχουν εξουσιοδοτηθεί από τον κύριο εποπτικό φορέα ασκούν τις εξουσίες τους επιδεικνύοντας έγγραφη εξουσιοδότηση που ορίζει το αντικείμενο και τον σκοπό της επιθεώρησης και τις περιοδικές χρηματικές ποινές που προβλέπονται στο άρθρο 35 παράγραφος 6, σε περίπτωση που οι εκπρόσωποι των εν λόγω κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ δεν αποδέχονται την επιθεώρηση.

3. Πριν από την έναρξη της επιθεώρησης, ο κύριος εποπτικός φορέας ενημερώνει εγκαίρως τις αρμόδιες αρχές των χρηματοοικονομικών οντοτήτων που χρησιμοποιούν τον εν λόγω τρίτο πάροχο υπηρεσιών ΤΠΕ.

4. Οι επιθεωρήσεις καλύπτουν το πλήρες φάσμα των σχετικών συστημάτων, δικτύων, συσκευών, πληροφοριών και δεδομένων ΤΠΕ που χρησιμοποιούνται ή συμβάλλουν στην παροχή υπηρεσιών ΤΠΕ προς χρηματοοικονομικές οντότητες.

5. Πριν από κάθε προγραμματισμένη επιτόπια επιθεώρηση, ο κύριος εποπτικός φορέας ειδοποιεί ευλόγως τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, εκτός εάν η ειδοποίηση αυτή δεν είναι δυνατή λόγω καταστάσεων έκτακτης ανάγκης ή κρίσης, ή εάν δημιουργεί κατάσταση κατά την οποία η επιθεώρηση ή ο έλεγχος δεν συνιστούν πλέον αποτελεσματική ενέργεια.

6. Ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ αποδέχεται τις επιτόπιες επιθεωρήσεις που έχουν διαταχθεί με απόφαση του κύριου εποπτικού φορέα. Η απόφαση προσδιορίζει το αντικείμενο και τον σκοπό της επιθεώρησης, καθορίζει την ημερομηνία έναρξης της επιθεώρησης και αναφέρει τις περιοδικές χρηματικές ποινές που προβλέπονται στο άρθρο 35 παράγραφος 6, τα ένδικα βοηθήματα που είναι διαθέσιμα βάσει των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010, καθώς και το δικαίωμα επανεξέτασης της απόφασης από το Δικαστήριο.

7. Όταν οι υπάλληλοι και άλλα πρόσωπα που εξουσιοδοτούνται από τον κύριο εποπτικό φορέα διαπιστώσουν ότι ένας κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ προβάλει αντίρρηση για τη διεξαγωγή επιθεώρησης που έχει διαταχθεί σύμφωνα με το παρόν άρθρο, ο κύριος εποπτικός φορέας ενημερώνει τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ σχετικά με τις συνέπειες της αντίρρησης, συμπεριλαμβανομένης της δυνατότητας των αρμόδιων αρχών των σχετικών χρηματοοικονομικών οντοτήτων να απαιτήσουν από τις χρηματοοικονομικές οντότητες να καταγγείλουν τις συμβατικές ρυθμίσεις που έχουν συναφθεί με τον εν λόγω κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ.

Άρθρο 40

Εν εξελίξει εποπτεία

1. Κατά τη διεξαγωγή εποπτικών δραστηριοτήτων, ιδίως γενικών ερευνών ή επιθεωρήσεων, ο κύριος εποπτικός φορέας επικουρείται από την κοινή εξεταστική ομάδα που έχει συγκροτηθεί για κάθε κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ.

2. Η κοινή εξεταστική ομάδα που αναφέρεται στην παράγραφο 1 απαρτίζεται από μέλη του προσωπικού:

α) των ΕΕΑ,

β) των σχετικών αρμόδιων αρχών που εποπτεύουν τις χρηματοοικονομικές οντότητες στις οποίες παρέχει υπηρεσίες ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ,

γ) της εθνικής αρμόδιας αρχής που αναφέρεται στο άρθρο 32 παράγραφος 4 στοιχείο ε), σε προαιρετική βάση,

δ) μίας εθνικής αρμόδιας αρχής από το κράτος μέλος στο οποίο είναι εγκατεστημένος ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ, σε προαιρετική βάση.

Τα μέλη της κοινής εξεταστικής ομάδας διαθέτουν εμπειρογνωσία όσον αφορά θέματα ΤΠΕ και τον λειτουργικό κίνδυνο. Η κοινή εξεταστική ομάδα εκτελεί τις εργασίες της υπό τον συντονισμό ενός μέλους του προσωπικού που ορίζεται κύριος εποπτικός φορέας (στο εξής: συντονιστής κύριου εποπτικού φορέα).

3. Εντός 3 μηνών από την ολοκλήρωση μιας έρευνας ή επιθεώρησης, ο κύριος εποπτικός φορέας, κατόπιν διαβούλευσης με το φόρουμ εποπτείας, εγκρίνει συστάσεις τις οποίες πρέπει να απευθύνει στον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ σύμφωνα με τις εξουσίες που αναφέρονται στο άρθρο 35.

4. Οι συστάσεις που αναφέρονται στην παράγραφο 3 κοινοποιούνται αμέσως στον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ και στις αρμόδιες αρχές των χρηματοοικονομικών οντοτήτων στις οποίες παρέχει υπηρεσίες ΤΠΕ.

Για την εκπλήρωση των δραστηριοτήτων εποπτείας, ο κύριος εποπτικός φορέας μπορεί να λαμβάνει υπόψη τυχόν σχετικές πιστοποιήσεις τρίτων και εσωτερικές ή εξωτερικές εκθέσεις ελέγχου τρίτων παρόχων ΤΠΕ, τις οποίες θέτει στη διάθεσή του ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ.

Άρθρο 41

Εναρμόνιση με τους όρους που καθιστούν δυνατή την άσκηση δραστηριοτήτων εποπτείας

1. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, καταρτίζουν σχέδια ρυθμιστικών τεχνικών προτύπων με σκοπό να προσδιορίσουν:

α) τις πληροφορίες που πρέπει να παρέχει ο τρίτος πάροχος υπηρεσιών ΤΠΕ στην αίτηση για προαιρετικό αίτημα ορισμού ως κρίσιμος βάσει του άρθρου 31 παράγραφος 11,

β) το περιεχόμενο, τη δομή και τη μορφή των πληροφοριών που πρέπει να υποβάλλονται, να γνωστοποιούνται ή να αναφέρονται από τους τρίτους παρόχους υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 35 παράγραφος 1, συμπεριλαμβανομένου του υποδείγματος για την παροχή πληροφοριών σχετικά με τις ρυθμίσεις υπεργολαβίας,

γ) τα κριτήρια για τον καθορισμό της σύνθεσης της κοινής εξεταστικής ομάδας, διασφαλίζοντας την ισόρροπη συμμετοχή των μελών του προσωπικού των ΕΕΑ και των σχετικών αρμόδιων αρχών, τον ορισμό τους, τα καθήκοντά τους και τις ρυθμίσεις εργασίας τους,

δ) τις λεπτομέρειες της αξιολόγησης των αρμόδιων αρχών όσον αφορά τα μέτρα που έλαβε ο τρίτος πάροχος υπηρεσιών ΤΠΕ βάσει των συστάσεων του κύριου εποπτικού φορέα σύμφωνα με το άρθρο 42 παράγραφος 3.

2. Οι ΕΕΑ υποβάλλουν τα εν λόγω σχέδια ρυθμιστικών τεχνικών προτύπων στην Επιτροπή έως τις 17 Ιουλίου 2024.

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στην παράγραφο 1, σύμφωνα με τη διαδικασία που ορίζεται στα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010.

Άρθρο 42

Συνέχεια που δίνεται από τις αρμόδιες αρχές

1. Εντός 60 ημερολογιακών ημερών από την παραλαβή των συστάσεων που εκδίδει ο κύριος εποπτικός φορέας σύμφωνα με το άρθρο 35 παράγραφος 1 στοιχείο δ), οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ είτε ενημερώνουν τον κύριο εποπτικό φορέα για την πρόθεσή τους να ακολουθήσουν τις συστάσεις είτε παρέχουν αιτιολογημένη εξήγηση για τη μη τήρηση των εν λόγω συστάσεων. Ο κύριος εποπτικός φορέας διαβιβάζει αμέσως τις πληροφορίες αυτές στις αρμόδιες αρχές των σχετικών χρηματοοικονομικών οντοτήτων.

2. Ο κύριος εποπτικός φορέας δημοσιοποιεί το γεγονός ότι ένας κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ δεν ενημερώνει τον κύριο εποπτικό φορέα σύμφωνα με την παράγραφο 1 ή ότι η εξήγηση που παρέχεται από τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ δεν κρίνεται επαρκής. Οι πληροφορίες που δημοσιεύονται αποκαλύπτουν την ταυτότητα του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ, καθώς και πληροφορίες σχετικά με το είδος και τη φύση της μη συμμόρφωσης. Οι πληροφορίες αυτές περιορίζονται σε ό,τι είναι σημαντικό και αναλογικό για τη διασφάλιση της ευαισθητοποίησης του κοινού, εκτός εάν η δημοσιοποίηση αυτή θα προκαλούσε δυσανάλογη ζημία στα εμπλεκόμενα μέρη ή θα μπορούσε να θέσει σε σοβαρό κίνδυνο την εύρυθμη λειτουργία και την ακεραιότητα των χρηματοοικονομικών αγορών ή τη σταθερότητα ολόκληρου ή μέρους του χρηματοοικονομικού συστήματος της Ένωσης.

Ο κύριος εποπτικός φορέας ενημερώνει τον τρίτο πάροχο υπηρεσιών ΤΠΕ σχετικά με την εν λόγω δημοσιοποίηση.

3. Οι αρμόδιες αρχές ενημερώνουν τις σχετικές χρηματοοικονομικές οντότητες για τους κινδύνους που προσδιορίζονται στις συστάσεις που απευθύνονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 35 παράγραφος 1 στοιχείο δ).

Κατά τη διαχείριση του κινδύνου τρίτων μερών ΤΠΕ, οι χρηματοοικονομικές οντότητες λαμβάνουν υπόψη τους κινδύνους που αναφέρονται στο πρώτο εδάφιο.

4. Όταν μια αρμόδια αρχή κρίνει ότι μια χρηματοοικονομική οντότητα δεν λαμβάνει υπόψη ή δεν αντιμετωπίζει επαρκώς στο πλαίσιο της διαχείρισης του κινδύνου τρίτων μερών ΤΠΕ τους συγκεκριμένους κινδύνους που προσδιορίζονται στις συστάσεις, κοινοποιεί στη χρηματοοικονομική οντότητα την πιθανότητα να ληφθεί απόφαση, εντός 60 ημερολογιακών ημερών από την παραλαβή της εν λόγω κοινοποίησης, σύμφωνα με την παράγραφο 6, ελλείψει κατάλληλων συμβατικών ρυθμίσεων με στόχο την αντιμετώπιση των εν λόγω κινδύνων.

5. Μετά την παραλαβή των αναφορών που προβλέπονται στο άρθρο 35 παράγραφος 1 στοιχείο γ) και πριν από τη λήψη της απόφασης όπως αναφέρεται στην παράγραφο 6 του παρόντος άρθρου, οι αρμόδιες αρχές μπορούν, σε προαιρετική βάση, να διαβουλεύονται με τις αρμόδιες αρχές οι οποίες έχουν οριστεί ή συσταθεί σύμφωνα με την οδηγία (ΕΕ) 2022/2555 και είναι υπεύθυνες για την εποπτεία μιας βασικής ή σημαντικής οντότητας που υπόκειται στις διατάξεις της εν λόγω οδηγίας και η οποία έχει οριστεί ως κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ.

6. Οι αρμόδιες αρχές δύνανται, ως μέτρο έσχατης ανάγκης, μετά την κοινοποίηση και, κατά περίπτωση, τη διαβούλευση κατά τα οριζόμενα στις παραγράφους 4 και 5 του παρόντος άρθρου, σύμφωνα με το άρθρο 50, να λάβουν απόφαση με την οποία απαιτούν από τις χρηματοοικονομικές οντότητες να αναστείλουν προσωρινά, εν μέρει ή πλήρως, τη χρήση ή την ανάπτυξη μιας υπηρεσίας που παρέχεται από τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ, έως ότου αντιμετωπιστούν οι κίνδυνοι που προσδιορίζονται στις συστάσεις που απευθύνονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ. Εάν κρίνεται σκόπιμο, μπορούν να ζητήσουν από τις χρηματοοικονομικές οντότητες να προβούν σε μερική ή ολική καταγγελία των σχετικών ρυθμίσεων που έχουν συναφθεί με τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ.

7. Όταν ένας κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ αρνείται να εγκρίνει συστάσεις βασιζόμενος σε αποκλίνουσα προσέγγιση από εκείνη που συνιστά ο κύριος εποπτικός φορέας, και η εν λόγω αποκλίνουσα προσέγγιση μπορεί να επηρεάσει αρνητικά μεγάλο αριθμό χρηματοοικονομικών οντοτήτων ή σημαντικό μέρος του χρηματοοικονομικό τομέα, και οι μεμονωμένες προειδοποιήσεις που εκδίδονται από αρμόδιες αρχές δεν έχουν οδηγήσει σε συνεπείς προσεγγίσεις για τον μετριασμό του δυνητικού κινδύνου για τη χρηματοοικονομική σταθερότητα, ο κύριος εποπτικός φορέας μπορεί, κατόπιν διαβούλευσης με το φόρουμ εποπτείας, να εκδίδει μη δεσμευτικές και μη δημόσιες γνώμες προς τις αρμόδιες αρχές, προκειμένου να προωθήσει συνεπή και συγκλίνοντα εποπτικά μέτρα παρακολούθησης, κατά περίπτωση.

8. Μετά την παραλαβή των εκθέσεων που αναφέρονται στο άρθρο 35 παράγραφος 1 στοιχείο γ), οι αρμόδιες αρχές, κατά τη λήψη απόφασης που προβλέπεται στην παράγραφο 6 του παρόντος άρθρου, λαμβάνουν υπόψη το είδος και το μέγεθος του κινδύνου που δεν αντιμετωπίστηκε από τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ, καθώς και τη σοβαρότητα της μη συμμόρφωσης, λαμβάνοντας υπόψη τα ακόλουθα κριτήρια:

α) τη βαρύτητα και τη διάρκεια της μη συμμόρφωσης,

β) αν η μη συμμόρφωση αποκάλυψε σοβαρές αδυναμίες στις διαδικασίες, τα συστήματα διαχείρισης, τη διαχείριση κινδύνων και τις εσωτερικές δικλείδες ασφάλειας του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ,

γ) αν η μη συμμόρφωση διευκόλυνε, προκάλεσε ή ευθύνεται με άλλον τρόπο για την τέλεση οικονομικού εγκλήματος,

δ) αν η μη συμμόρφωση οφείλεται σε πρόθεση ή σε αμέλεια,

ε) αν η αναστολή ή η καταγγελία των συμβατικών ρυθμίσεων ενέχει κίνδυνο για τη συνέχεια των επιχειρηματικών δραστηριοτήτων της χρηματοοικονομικής οντότητας, παρά τις προσπάθειες της χρηματοοικονομικής οντότητας να αποφευχθεί η διαταραχή στην παροχή των υπηρεσιών της,

στ) κατά περίπτωση, τη γνώμη των αρμόδιων αρχών που έχουν οριστεί ή συσταθεί σύμφωνα με την οδηγία (ΕΕ) 2022/2555 ως υπεύθυνες για την εποπτεία μιας βασικής ή σημαντικής οντότητας που υπόκειται στις διατάξεις της εν λόγω οδηγίας και η οποία έχει οριστεί ως κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ, η οποία ζητείται σε προαιρετική βάση σύμφωνα με την παράγραφο 5 του παρόντος άρθρου.

Οι αρμόδιες αρχές παρέχουν στις χρηματοοικονομικές οντότητες το αναγκαίο χρονικό διάστημα, ώστε να μπορέσουν να προσαρμόσουν τις συμβατικές ρυθμίσεις με κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, προκειμένου να αποφευχθούν οι αρνητικές επιπτώσεις στην ψηφιακή επιχειρησιακή ανθεκτικότητά τους και να μπορέσουν να αναπτύξουν στρατηγικές εξόδου και σχέδια μετάβασης όπως αναφέρονται στο άρθρο 28.

9. Η απόφαση που αναφέρεται στην παράγραφο 6 του παρόντος άρθρου κοινοποιείται στα μέλη του φόρουμ εποπτείας που αναφέρεται στο άρθρο 32 παράγραφος 4 στοιχεία α), β) και γ) και στο ΔΚΕ.

Οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που επηρεάζονται από τις αποφάσεις της παραγράφου 6 συνεργάζονται πλήρως με τις θιγόμενες χρηματοοικονομικές οντότητες, ιδίως στο πλαίσιο της διαδικασίας αναστολής ή καταγγελίας των συμβατικών τους ρυθμίσεων.

10. Οι αρμόδιες αρχές ενημερώνουν τακτικά τον κύριο εποπτικό φορέα σχετικά με τις προσεγγίσεις και τα μέτρα που λαμβάνονται κατά την εκτέλεση των εποπτικών καθηκόντων τους σε σχέση με τις χρηματοοικονομικές οντότητες, καθώς και σε σχέση με τις συμβατικές ρυθμίσεις που έχουν συνάψει, σε περίπτωση που οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ δεν έχουν εγκρίνει εν μέρει ή πλήρως τις συστάσεις που τους απηύθυνε ο κύριος εποπτικός φορέας.

11. Ο κύριος εποπτικός φορέας μπορεί, κατόπιν αιτήματος, να παράσχει περαιτέρω διευκρινίσεις σχετικά με τις εκδοθείσες συστάσεις για να καθοδηγήσει τις αρμόδιες αρχές σχετικά με τα μέτρα παρακολούθησης.

Άρθρο 43

Εποπτικά τέλη

1. Ο κύριος εποπτικός φορέας χρεώνει, σύμφωνα με την κατ' εξουσιοδότηση πράξη που αναφέρεται στην παράγραφο 2 του παρόντος άρθρου, κρίσιμες αμοιβές τρίτων παρόχων υπηρεσιών ΤΠΕ που καλύπτουν πλήρως τις αναγκαίες δαπάνες του κύριου εποπτικού φορέα σε σχέση με την εκτέλεση των καθηκόντων εποπτείας σύμφωνα με τον παρόντα κανονισμό, συμπεριλαμβανομένης της επιστροφής τυχόν δαπανών που ενδέχεται να προκύψουν ως αποτέλεσμα των εργασιών της κοινής εξεταστικής ομάδας που αναφέρεται στο άρθρο 40, καθώς και των δαπανών για συμβουλές που παρέχονται από τους ανεξάρτητους εμπειρογνώμονες, όπως αναφέρεται στο άρθρο 32 δεύτερο εδάφιο παράγραφος 4, σε σχέση με θέματα που εμπίπτουν στην αρμοδιότητα των δραστηριοτήτων άμεσης εποπτείας.

Το ύψος των τελών που χρεώνονται σε κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ καλύπτει όλες τις δαπάνες που προκύπτουν ως αποτέλεσμα της εκτέλεσης των καθηκόντων που προβλέπονται στην παρούσα ενότητα και είναι ανάλογο προς τον κύκλο εργασιών του.

2. Ανατίθεται στην Επιτροπή η εξουσία να εκδώσει κατ' εξουσιοδότηση πράξη, σύμφωνα με το άρθρο 57, για τη συμπλήρωση του παρόντος κανονισμού με τον προσδιορισμό του ύψους των τελών και του τρόπου καταβολής τους έως τις 17 Ιουλίου 2024.

Άρθρο 44

Διεθνής συνεργασία

1. Με την επιφύλαξη του άρθρου 36, η ΕΑΤ, η ΕΑΚΑΑ και η ΕΑΑΕΣ δύνανται, σύμφωνα με το άρθρο 33 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1095/2010 και (ΕΕ) αριθ. 1094/2010, αντίστοιχα, να συνάπτουν διοικητικές ρυθμίσεις με κανονιστικές και εποπτικές αρχές τρίτων χωρών, με σκοπό την προώθηση της διεθνούς συνεργασίας όσον αφορά τους κινδύνους τρίτων παρόχων ΤΠΕ σε διάφορους χρηματοοικονομικούς τομείς, ιδίως με την ανάπτυξη βέλτιστων πρακτικών για την επανεξέταση των πρακτικών και των ελέγχων διαχείρισης κινδύνων ΤΠΕ, των μέτρων μετριασμού και της αντιμετώπισης συμβάντων.

2. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, υποβάλλουν ανά πενταετία στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Επιτροπή κοινή εμπιστευτική έκθεση, στην οποία συνοψίζονται τα ευρήματα των σχετικών συζητήσεων που διεξάγονται με τις αρχές τρίτων χωρών που αναφέρονται στην παράγραφο 1, εστιάζοντας στην εξέλιξη των κινδύνων τρίτων παρόχων ΤΠΕ και στις συνέπειες που έχει για τη χρηματοοικονομική σταθερότητα, την ακεραιότητα της αγοράς, την προστασία των επενδυτών ή τη λειτουργία της εσωτερικής αγοράς.

ΚΕΦΑΛΑΙΟ VI

Ρυθμίσεις ανταλλαγής πληροφοριών

Άρθρο 45

Ρυθμίσεις ανταλλαγής πληροφοριών όσον αφορά στοιχεία και πληροφορίες για κυβερνοαπειλές

1. Οι χρηματοοικονομικές οντότητες μπορούν να ανταλλάσσουν μεταξύ τους στοιχεία και πληροφορίες για κυβερνοαπειλές, συμπεριλαμβανομένων των δεικτών έκθεσης σε κίνδυνο, τακτικών, τεχνικών και διαδικασιών, ειδοποιήσεων κυβερνοασφάλειας και εργαλείων παραμετροποίησης, στον βαθμό που η εν λόγω ανταλλαγή στοιχείων και πληροφοριών:

α) έχει ως στόχο την ενίσχυση της ψηφιακής επιχειρησιακής ανθεκτικότητας των χρηματοοικονομικών οντοτήτων, ιδίως μέσω της ευαισθητοποίησης σχετικά με τις κυβερνοαπειλές, του περιορισμού ή της παρεμπόδισης της ικανότητας διάδοσης των κυβερνοαπειλών, της υποστήριξης των αμυντικών ικανοτήτων, των τεχνικών ανίχνευσης απειλών, των στρατηγικών μετριασμού ή των σταδίων αντιμετώπισης και ανάκαμψης,

β) πραγματοποιείται στο πλαίσιο αξιόπιστων κοινοτήτων χρηματοοικονομικών οντοτήτων,

γ) υλοποιείται μέσω ρυθμίσεων ανταλλαγής πληροφοριών που προστατεύουν τον δυνητικά ευαίσθητο χαρακτήρα των ανταλλασσόμενων πληροφοριών, και οι οποίες διέπονται από κανόνες δεοντολογίας, τηρουμένων πλήρως του επιχειρηματικού απορρήτου, της προστασίας των δεδομένων προσωπικού χαρακτήρα σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 και των κατευθυντήριων γραμμών για την πολιτική ανταγωνισμού.

2. Για τους σκοπούς της παραγράφου 1 στοιχείο γ), οι ρυθμίσεις ανταλλαγής πληροφοριών καθορίζουν τους όρους συμμετοχής και, ανάλογα με την περίπτωση, τις λεπτομέρειες σχετικά με την εξασφάλιση της συμμετοχής των δημόσιων αρχών και την ιδιότητα με την οποία μπορούν να συνδέονται με τις ρυθμίσεις ανταλλαγής πληροφοριών, σχετικά με τη συμμετοχή των τρίτων παρόχων υπηρεσιών ΤΠΕ, καθώς και σχετικά με τα επιχειρησιακά στοιχεία, συμπεριλαμβανομένης της χρήσης ειδικών πλατφορμών ΤΠ.

3. Οι χρηματοοικονομικές οντότητες κοινοποιούν στις αρμόδιες αρχές τη συμμετοχή τους στις ρυθμίσεις ανταλλαγής πληροφοριών που αναφέρονται στην παράγραφο 1, κατά την επικύρωση της συμμετοχής τους ως μελών ή, κατά περίπτωση, της παύσης της συμμετοχής τους ως μελών, αμέσως μετά την έναρξη ισχύος της.

ΚΕΦΑΛΑΙΟ VII

Αρμόδιες αρχές

Άρθρο 46

Αρμόδιες αρχές

Με την επιφύλαξη των διατάξεων σχετικά με το πλαίσιο εποπτείας κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ που αναφέρονται στο κεφάλαιο V τμήμα II του παρόντος κανονισμού, η συμμόρφωση με τον παρόντα κανονισμό διασφαλίζεται από τις κατωτέρω αρμόδιες αρχές σύμφωνα με τις εξουσίες που τους έχουν χορηγηθεί βάσει των αντίστοιχων νομικών πράξεων:

α) για πιστωτικά ιδρύματα και για ιδρύματα που εξαιρούνται δυνάμει της οδηγίας 2013/36/ΕΕ, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 4 της εν λόγω οδηγίας, και για πιστωτικά ιδρύματα που χαρακτηρίζονται ως σημαντικά σύμφωνα με το άρθρο 6 παράγραφος 4 του κανονισμού (ΕΕ) αριθ. 1024/2013, την ΕΚΤ σύμφωνα με τις εξουσίες και τα καθήκοντα που ανατίθενται με τον εν λόγω κανονισμό,

β) για ιδρύματα πληρωμών, συμπεριλαμβανομένων των ιδρυμάτων πληρωμών που εξαιρούνται δυνάμει της οδηγίας (ΕΕ) 2015/2366, για ιδρύματα ηλεκτρονικού χρήματος, συμπεριλαμβανομένων εκείνων που εξαιρούνται δυνάμει της οδηγίας 2009/110/ΕΚ, και για παρόχους υπηρεσιών πληροφοριών λογαριασμού, όπως αναφέρονται στο άρθρο 33 παράγραφος 1 της οδηγίας (ΕΕ) 2015/2366, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 22 της οδηγίας (ΕΕ) 2015/2366,

γ) για επιχειρήσεις επενδύσεων, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 4 της οδηγίας (ΕΕ) 2019/2034 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([38]),

δ) για παρόχους υπηρεσιών κρυπτοστοιχείων που έχουν λάβει άδεια βάσει του του κανονισμού σχετικά με τις αγορές κρυπτοστοιχείων και για εκδότες ψηφιακών μαρκών με εγγύηση περιουσιακών στοιχείων, την αρμόδια αρχή που ορίζεται σύμφωνα με τη σχετική διάταξη του εν λόγω κανονισμού,

ε) για κεντρικά αποθετήρια τίτλων, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 11 του κανονισμού (ΕΕ) αριθ. 909/2014,

στ) για κεντρικούς αντισυμβαλλομένους, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 22 του κανονισμού (ΕΕ) αριθ. 648/2012,

ζ) για τόπους διαπραγμάτευσης και παρόχους υπηρεσιών αναφοράς δεδομένων, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 67 της οδηγίας 2014/65/ΕΕ και την αρμόδια αρχή όπως ορίζεται στο άρθρο 2 παράγραφος 1 σημείο 18) του κανονισμού (ΕΕ) αριθ. 600/2014,

η) για αρχεία καταγραφής συναλλαγών, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 22 του κανονισμού (ΕΕ) αριθ. 648/2012,

θ) για διαχειριστές οργανισμών εναλλακτικών επενδύσεων, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 44 της οδηγίας 2011/61/ΕΕ,

ι) για εταιρείες διαχείρισης, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 97 της οδηγίας 2009/65/ΕΚ,

ια) για ασφαλιστικές και αντασφαλιστικές επιχειρήσεις, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 30 της οδηγίας 2009/138/ΕΚ,

ιβ) για ασφαλιστικούς διαμεσολαβητές, αντασφαλιστικούς διαμεσολαβητές και ασφαλιστικούς διαμεσολαβητές που ασκούν ως δευτερεύουσα δραστηριότητα την ασφαλιστική διαμεσολάβηση, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 12 της οδηγίας (ΕΕ) 2016/97,

ιγ) για ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 47 της οδηγίας (ΕΕ) 2016/2341,

ιδ) για οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 21 του κανονισμού (ΕΚ) αριθ. 1060/2009,

ιε) για διαχειριστές δεικτών αναφοράς κρίσιμης σημασίας, την αρμόδια αρχή που ορίζεται σύμφωνα με τα άρθρα 40 και 41 του κανονισμού (ΕΕ) 2016/1011,

([38]) Οδηγία (ΕΕ) 2019/2034 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Νοεμβρίου 2019, σχετικά με την προληπτική εποπτεία επιχειρήσεων επενδύσεων και την τροποποίηση των οδηγιών 2002/87/ΕΚ, 2009/65/ΕΚ, 2011/61/ΕΕ, 2013/36/ΕΕ, 2014/59/ΕΕ και 2014/65/ΕΕ (ΕΕ L 314 της 5.12.2019, σ. 64).

ιστ) για παρόχους υπηρεσιών συμμετοχικής χρηματοδότησης, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 29 του κανονισμού (ΕΕ) 2020/1503,

ιζ) για αρχεία καταγραφής τιτλοποιήσεων, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 10 και το άρθρο 14 παράγραφος 1 του κανονισμού (ΕΕ) 2017/2402.

Άρθρο 47

Συνεργασία με δομές και αρχές που έχουν συγκροτηθεί βάσει της οδηγίας (ΕΕ) 2022/2555

1. Για την ενίσχυση της συνεργασίας και τη διευκόλυνση των ανταλλαγών εποπτικών πληροφοριών μεταξύ των αρμόδιων αρχών, που ορίζονται σύμφωνα με τον παρόντα κανονισμό, και της ομάδας συνεργασίας, που έχει συγκροτηθεί σύμφωνα με το άρθρο 14 της οδηγίας (ΕΕ) 2022/2555 οι ΕΕΑ και οι αρμόδιες αρχές μπορούν να συμμετέχουν στις δραστηριότητες της ομάδας συνεργασίας για θέματα που αφορούν τις εποπτικές δραστηριότητές τους σε σχέση με χρηματοοικονομικές οντότητες. Οι ΕΕΑ και οι αρμόδιες αρχές μπορούν να ζητήσουν να κληθούν να συμμετάσχουν στις δραστηριότητες της ομάδας συνεργασίας για θέματα που αφορούν βασικές ή σημαντικές οντότητες που υπόκεινται στις διατάξεις της οδηγίας (ΕΕ) 2022/2555 οι οποίες έχουν επίσης οριστεί ως κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 31 του παρόντος κανονισμού.

2. Κατά περίπτωση, οι αρμόδιες αρχές μπορούν να συμβουλεύονται και να ανταλλάσσουν πληροφορίες με τα ενιαία σημεία επαφής και τις CSIRT που έχουν οριστεί ή συσταθεί σύμφωνα με την οδηγία (ΕΕ) 2022/2555

3. Κατά περίπτωση, οι αρμόδιες αρχές μπορούν να ζητούν κάθε σχετική τεχνική συμβουλή και βοήθεια από τις αρμόδιες αρχές που ορίζονται ή συστήνονται σύμφωνα με την οδηγία (ΕΕ) 2022/2555 και να θεσπίζουν ρυθμίσεις συνεργασίας για τη δημιουργία αποτελεσματικών μηχανισμών συντονισμού ταχείας απόκρισης.

4. Οι ρυθμίσεις που αναφέρονται στην παράγραφο 3 του παρόντος άρθρου μπορούν, μεταξύ άλλων, να προσδιορίζουν τις διαδικασίες για τον συντονισμό των δραστηριοτήτων εποπτείας, αντίστοιχα, σε σχέση με τις βασικές ή σημαντικές οντότητες που υπόκεινται στις διατάξεις της οδηγίας (ΕΕ) 2022/2555 οι οποίοι έχουν οριστεί ως κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 31 του παρόντος κανονισμού, μεταξύ άλλων για τη διεξαγωγή, σύμφωνα με το εθνικό δίκαιο, ερευνών και επιτόπιων επιθεωρήσεων, καθώς και για μηχανισμούς ανταλλαγής πληροφοριών μεταξύ των αρμόδιων αρχών δυνάμει του παρόντος κανονισμού και των αρμόδιων αρχών που ορίζονται ή συστήνονται σύμφωνα με την εν λόγω οδηγία, συμπεριλαμβανομένης της πρόσβασης σε πληροφορίες που ζητούν οι τελευταίες αυτές αρχές.

Άρθρο 48

Συνεργασία μεταξύ αρχών

1. Οι αρμόδιες αρχές συνεργάζονται στενά μεταξύ τους και, κατά περίπτωση, με τον κύριο εποπτικό φορέα.

2. Οι αρμόδιες αρχές και ο κύριος εποπτικός φορέας ανταλλάσσουν εγκαίρως όλες τις σχετικές πληροφορίες που αφορούν κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ και είναι απαραίτητες για την εκτέλεση των αντίστοιχων καθηκόντων τους δυνάμει του παρόντος κανονισμού, ιδίως σε σχέση με προσδιορισμένους κινδύνους, προσεγγίσεις και μέτρα που λαμβάνονται στο πλαίσιο των εποπτικών καθηκόντων του κύριου εποπτικού φορέα.

Άρθρο 49

Ασκήσεις, επικοινωνία και συνεργασία μεταξύ των χρηματοοικονομικών τομέων

1. Οι ΕΕΑ, μέσω της μεικτής επιτροπής και σε συνεργασία με τις αρμόδιες αρχές, τις αρχές εξυγίανσης που αναφέρονται στο άρθρο 3 της οδηγίας 2014/59/ΕΕ, την ΕΚΤ, το Ενιαίο Συμβούλιο Εξυγίανσης όσον αφορά πληροφορίες σχετικά με οντότητες που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού (ΕΕ) αριθ. 806/2014, το ΕΣΣΚ και τον ENISA, κατά περίπτωση, μπορούν να θεσπίσουν μηχανισμούς ώστε να είναι δυνατή η ανταλλαγή αποτελεσματικών πρακτικών μεταξύ των χρηματοοικονομικών τομέων για την ενίσχυση της επίγνωσης των καταστάσεων και τον εντοπισμό κοινών ευπαθειών στον κυβερνοχώρο και κινδύνων μεταξύ των τομέων.

Μπορούν να αναπτύξουν ασκήσεις διαχείρισης κρίσεων και έκτακτης ανάγκης που περιλαμβάνουν σενάρια κυβερνοεπιθέσεων, με σκοπό την ανάπτυξη διαύλων επικοινωνίας και τη σταδιακή εξασφάλιση της δυνατότητας αποτελεσματικής συντονισμένης απόκρισης σε επίπεδο ΕΕ, σε περίπτωση μείζονος διασυνοριακού συμβάντος που σχετίζεται με τις ΤΠΕ ή σχετικής απειλής με συστημικές επιπτώσεις στον χρηματοοικονομικό τομέα της Ένωσης συνολικά.

Στο πλαίσιο των ασκήσεων αυτών παρέχεται, κατά περίπτωση, η δυνατότητα ελέγχου των εξαρτήσεων του χρηματοοικονομικού τομέα από άλλους οικονομικούς τομείς.

2. Οι αρμόδιες αρχές, οι ΕΕΑ και η ΕΚΤ συνεργάζονται στενά μεταξύ τους και ανταλλάσσουν πληροφορίες στο πλαίσιο της εκτέλεσης των καθηκόντων τους, σύμφωνα με τα άρθρα 47 έως 54. Συντονίζουν στενά την εποπτεία τους ώστε να εντοπίζουν και να διορθώνουν παραβιάσεις του παρόντος κανονισμού, να αναπτύσσουν και να προωθούν βέλτιστες πρακτικές, να διευκολύνουν τη συνεργασία, να προάγουν τη συνεπή ερμηνεία και να παρέχουν αξιολογήσεις σε περισσότερες από μία περιοχές δικαιοδοσίας σε περίπτωση διαφωνίας.

Άρθρο 50

Διοικητικές κυρώσεις και διορθωτικά μέτρα

1. Οι αρμόδιες αρχές διαθέτουν όλες τις εξουσίες εποπτείας, έρευνας και επιβολής κυρώσεων που απαιτούνται για την εκπλήρωση των καθηκόντων τους σύμφωνα με τον παρόντα κανονισμό.

2. Οι εξουσίες που αναφέρονται στην παράγραφο 1 περιλαμβάνουν τουλάχιστον τις ακόλουθες εξουσίες:

α) πρόσβαση σε οποιοδήποτε έγγραφο ή δεδομένο που τηρείται σε οποιαδήποτε μορφή, το οποίο η αρμόδια αρχή θεωρεί ότι μπορεί να είναι συναφές για την εκτέλεση των καθηκόντων τους, και να λαμβάνουν αντίγραφό του,

β) διενέργεια επιτόπιων ελέγχων ή ερευνών, που περιλαμβάνουν, μεταξύ άλλων:

   i) πρόσκληση εκπροσώπων των χρηματοοικονομικών υπηρεσιών για προφορικές ή γραπτές εξηγήσεις σχετικά με γεγονότα ή έγγραφα που αφορούν το αντικείμενο και τον σκοπό της έρευνας και καταγραφή των απαντήσεων,

   ii) εξέταση κάθε άλλου φυσικού ή νομικού προσώπου που συναινεί να ερωτηθεί με σκοπό τη συγκέντρωση πληροφοριών σχετικά με το αντικείμενο της έρευνας,

γ) αίτηση λήψης διορθωτικών μέτρων για παραβιάσεις των απαιτήσεων του παρόντος κανονισμού.

3. Με την επιφύλαξη του δικαιώματος των κρατών μελών να επιβάλλουν ποινικές κυρώσεις σύμφωνα με το άρθρο 52, τα κράτη μέλη θεσπίζουν κανόνες για τη θέσπιση κατάλληλων διοικητικών κυρώσεων και διορθωτικών μέτρων σε περιπτώσεις παραβίασης του παρόντος κανονισμού και διασφαλίζουν την αποτελεσματική εφαρμογή τους.

Ο χαρακτήρας των εν λόγω κυρώσεων και μέτρων είναι αποτελεσματικός, αναλογικός και αποτρεπτικός.

4. Τα κράτη μέλη αναθέτουν στις αρμόδιες αρχές την εξουσία να εφαρμόζουν τουλάχιστον τις ακόλουθες διοικητικές κυρώσεις ή διορθωτικά μέτρα σε περιπτώσεις παραβίασης του παρόντος κανονισμού:

α) να εκδίδουν εντολή βάσει της οποίας το φυσικό ή νομικό πρόσωπο υποχρεούται να παύσει τη συμπεριφορά που παραβιάζει τον παρόντα κανονισμό και να μην την επαναλάβει,

β) να απαιτούν την προσωρινή ή οριστική παύση κάθε πρακτικής ή συμπεριφοράς που η αρμόδια αρχή θεωρεί ότι αντιβαίνει στις διατάξεις του παρόντος κανονισμού και να προλαμβάνουν την επανάληψη της εν λόγω πρακτικής ή συμπεριφοράς,

γ) να εγκρίνουν κάθε είδους μέτρα, μεταξύ άλλων χρηματικής φύσης, ώστε να διασφαλίζεται ότι οι χρηματοοικονομικές οντότητες εξακολουθούν να συμμορφώνονται με τις νομικές απαιτήσεις,

δ) να ζητούν, στον βαθμό που επιτρέπεται από το εθνικό δίκαιο, τα υφιστάμενα αρχεία κίνησης δεδομένων που τηρούνται από πάροχο τηλεπικοινωνιακών υπηρεσιών, όταν υπάρχει εύλογη υπόνοια παραβίασης του παρόντος κανονισμού και όταν τα εν λόγω αρχεία μπορεί να είναι συναφή για τη διερεύνηση περιπτώσεων παραβίασης του παρόντος κανονισμού, και

ε) να εκδίδουν δημόσιες ανακοινώσεις, συμπεριλαμβανομένων των δημόσιων δηλώσεων, στις οποίες αναφέρεται το υπαίτιο φυσικό ή νομικό πρόσωπο και η φύση της παραβίασης.

5. Σε περίπτωση που η παράγραφος 2 στοιχείο γ) και η παράγραφος 4 εφαρμόζονται σε νομικά πρόσωπα, τα κράτη μέλη αναθέτουν στις αρμόδιες αρχές την εξουσία επιβολής των διοικητικών κυρώσεων και των διορθωτικών μέτρων, με την επιφύλαξη των προϋποθέσεων που προβλέπονται στο εθνικό δίκαιο, σε μέλη του διοικητικού οργάνου, καθώς και σε οποιοδήποτε άλλο φυσικό πρόσωπο το οποίο θεωρείται υπαίτιο για την παραβίαση δυνάμει του εθνικού δικαίου.

6. Τα κράτη μέλη διασφαλίζουν ότι οποιαδήποτε απόφαση επιβολής διοικητικών κυρώσεων ή διορθωτικών μέτρων που προβλέπεται από την παράγραφο 2 στοιχείο γ) αιτιολογείται δεόντως και υπόκειται σε δικαίωμα προσφυγής.

Άρθρο 51

Άσκηση της εξουσίας επιβολής διοικητικών κυρώσεων και διορθωτικών μέτρων

1. Οι αρμόδιες αρχές ασκούν την εξουσία επιβολής των διοικητικών κυρώσεων και των διορθωτικών μέτρων του άρθρου 50 σύμφωνα με το εκάστοτε εθνικό νομικό πλαίσιο, ανάλογα με την περίπτωση, ως εξής:

α) άμεσα,

β) σε συνεργασία με άλλες αρχές,

γ) υπό την ευθύνη τους με ανάθεση καθηκόντων σε άλλες αρχές ή

δ) κατόπιν αίτησης στις αρμόδιες δικαστικές αρχές.

2. Οι αρμόδιες αρχές, όταν καθορίζουν το είδος και το επίπεδο διοικητικών κυρώσεων ή διορθωτικών μέτρων που πρέπει να επιβληθούν δυνάμει του άρθρου 50, λαμβάνουν υπόψη αν η παραβίαση τελέστηκε εκ προθέσεως ή εξ αμελείας, καθώς και όλες τις άλλες σχετικές περιστάσεις, μεταξύ των οποίων τα ακόλουθα, κατά περίπτωση:

α) τη σημαντικότητα, τη βαρύτητα και τη διάρκεια της παραβίασης,

β) τον βαθμό υπαιτιότητας του φυσικού ή νομικού προσώπου που ευθύνεται για την παραβίαση,

γ) την οικονομική ευρωστία του υπαίτιου φυσικού ή νομικού προσώπου,

δ) τη σημασία των κερδών που αποκομίστηκαν ή των ζημιών που αποφεύχθηκαν από το υπαίτιο φυσικό ή νομικό πρόσωπο, στον βαθμό που μπορούν να προσδιοριστούν,

ε) τις ζημίες τρίτων που προκλήθηκαν λόγω της παραβίασης, στον βαθμό που μπορούν να προσδιοριστούν,

στ) τον βαθμό συνεργασίας του υπαίτιου φυσικού ή νομικού προσώπου με την αρμόδια αρχή, με την επιφύλαξη της ανάγκης να διασφαλιστεί η παραίτηση του εν λόγω φυσικού ή νομικού προσώπου από αποκτηθέντα κέρδη ή αποφευχθείσες ζημίες,

ζ) προηγούμενες παραβιάσεις από το υπαίτιο φυσικό ή νομικό πρόσωπο.

Άρθρο 52

Ποινικές κυρώσεις

1. Τα κράτη μέλη δύνανται να αποφασίζουν να μην θεσπίσουν κανόνες σχετικά με τις διοικητικές κυρώσεις ή τα διορθωτικά μέτρα για παραβιάσεις που υπόκεινται σε ποινικές κυρώσεις βάσει του εθνικού τους δικαίου.

2. Σε περίπτωση που τα κράτη μέλη έχουν επιλέξει να θεσπίσουν ποινικές κυρώσεις σε περιπτώσεις παραβίασης του παρόντος κανονισμού, διασφαλίζουν ότι εφαρμόζονται κατάλληλα μέτρα ώστε οι αρμόδιες αρχές να διαθέτουν όλες τις απαραίτητες εξουσίες για να συνεργάζονται με τις δικαστικές, εισαγγελικές αρχές και τις αρχές ποινικής δικαιοσύνης εντός της δικαιοδοσίας τους, προκειμένου να λαμβάνουν συγκεκριμένες πληροφορίες σχετικά με ποινικές έρευνες ή κινηθείσες διαδικασίες σε σχέση με περιπτώσεις παραβίασης του παρόντος κανονισμού και να παρέχουν τις ίδιες πληροφορίες σε άλλες αρμόδιες αρχές, καθώς και στην ΕΑΤ, την ΕΑΚΑΑ και την ΕΑΑΕΣ, στο πλαίσιο της τήρησης των υποχρεώσεών τους όσον αφορά τη συνεργασία για τους σκοπούς του παρόντος κανονισμού.

Άρθρο 53

Απαιτήσεις κοινοποίησης

Τα κράτη μέλη κοινοποιούν τους νόμους, τους κανονισμούς και τις διοικητικές διατάξεις εφαρμογής του παρόντος κεφαλαίου, συμπεριλαμβανομένων ενδεχόμενων σχετικών ποινικών διατάξεων, στην Επιτροπή, την ΕΑΚΑΑ, την ΕΑΤ και την ΕΑΑΕΣ, έως τις 17 Ιανουαρίου 2025. Τα κράτη μέλη κοινοποιούν στην Επιτροπή, την ΕΑΚΑΑ, την ΕΑΤ και την ΕΑΑΕΣ, χωρίς αδικαιολόγητη καθυστέρηση, κάθε μεταγενέστερη τροποποίησή τους.

Άρθρο 54

Δημοσίευση διοικητικών κυρώσεων

1. Οι αρμόδιες αρχές δημοσιεύουν, χωρίς αδικαιολόγητη καθυστέρηση, στους επίσημους δικτυακούς τους τόπους κάθε απόφαση που επιβάλλει διοικητική κύρωση η οποία δεν επιδέχεται άσκηση προσφυγής, μόλις η απόφαση αυτή κοινοποιηθεί στο πρόσωπο στο οποίο επιβλήθηκε η κύρωση.

2. Η δημοσίευση που αναφέρεται στην παράγραφο 1 περιλαμβάνει πληροφορίες σχετικά με το είδος και τον χαρακτήρα της παραβίασης, την ταυτότητα των υπαίτιων προσώπων και τις επιβληθείσες κυρώσεις.

3. Όταν η αρμόδια αρχή, κατόπιν αξιολόγησης βάσει κατά περίπτωση εξέτασης, κρίνει ότι η δημοσίευση της ταυτότητας, στην περίπτωση νομικών προσώπων, ή της ταυτότητας και των δεδομένων προσωπικού χαρακτήρα, στην περίπτωση φυσικών προσώπων, θα ήταν δυσανάλογη, μεταξύ άλλων ενέχοντας κινδύνους σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα, θα έθετε σε κίνδυνο τη σταθερότητα των χρηματοοικονομικών αγορών ή τη διενέργεια υπό εξέλιξη ποινικής έρευνας, ή θα προξενούσε, στον βαθμό που μπορεί να προσδιοριστεί, δυσανάλογη ζημία στο συγκεκριμένο πρόσωπο, εγκρίνει μία από τις ακόλουθες λύσεις σε σχέση με την απόφαση επιβολής διοικητικής κύρωσης:

α) αναβάλλει τη δημοσίευσή της έως ότου παύσουν να συντρέχουν οι λόγοι για τη μη δημοσίευσή της,

β) τη δημοσιεύει σε ανώνυμη βάση, σύμφωνα με το εθνικό δίκαιο, ή

γ) απέχει από τη δημοσίευσή της, όταν οι επιλογές που αναφέρονται στα στοιχεία α) και β) θεωρούνται ανεπαρκείς ώστε να εγγυηθούν ότι δεν θα υπάρξει κίνδυνος για τη σταθερότητα των χρηματοοικονομικών αγορών ή σε περίπτωση που η δημοσίευση δεν θα ήταν αναλογική της επιείκειας της επιβληθείσας κύρωσης.

4. Σε περίπτωση απόφασης για δημοσίευση διοικητικής κύρωσης σε ανώνυμη βάση σύμφωνα με την παράγραφο 3 στοιχείο β), η δημοσίευση των σχετικών δεδομένων μπορεί να αναβληθεί.

5. Όταν αρμόδια αρχή δημοσιεύει απόφαση επιβολής διοικητικής κύρωσης κατά της οποίας ασκήθηκε προσφυγή ενώπιον των αρμόδιων δικαστικών αρχών, οι αρμόδιες αρχές προσθέτουν πάραυτα στον επίσημο δικτυακό τους τόπο τα στοιχεία αυτά και, σε μεταγενέστερο στάδιο, τυχόν επακόλουθες πληροφορίες σχετικά με την έκβαση της προσφυγής. Δημοσιεύεται επίσης κάθε δικαστική απόφαση που ακυρώνει απόφαση επιβολής διοικητικής κύρωσης.

6. Οι αρμόδιες αρχές διασφαλίζουν ότι τυχόν δημοσίευση σύμφωνα με τις παραγράφους 1 έως 4 θα παραμείνει στον επίσημο δικτυακό τόπο τους μόνο κατά το χρονικό διάστημα που απαιτείται για την προβολή του παρόντος άρθρου. Το διάστημα αυτό δεν υπερβαίνει τα πέντε έτη από τη δημοσίευση.

Άρθρο 55

Επαγγελματικό απόρρητο

1. Τυχόν εμπιστευτικές πληροφορίες που λαμβάνονται, ανταλλάσσονται ή διαβιβάζονται βάσει του παρόντος κανονισμού υπόκεινται στους όρους της παραγράφου 2 περί επαγγελματικού απορρήτου.

2. Η υποχρέωση τήρησης του επαγγελματικού απορρήτου ισχύει για όλα τα πρόσωπα που εργάζονται ή έχουν εργαστεί για τις αρμόδιες αρχές σύμφωνα με τον παρόντα κανονισμό ή για οποιαδήποτε αρχή ή επιχείρηση της αγοράς ή για οποιοδήποτε άλλο φυσικό ή νομικό πρόσωπο στο οποίο οι αρμόδιες αρχές έχουν αναθέσει τις εξουσίες τους, συμπεριλαμβανομένων των ελεγκτών και εμπειρογνωμόνων που προσλαμβάνονται από αυτές.

3. Απαγορεύεται η κοινοποίηση των πληροφοριών που καλύπτονται από το επαγγελματικό απόρρητο, συμπεριλαμβανομένης της ανταλλαγής πληροφοριών μεταξύ των αρμόδιων αρχών δυνάμει του παρόντος κανονισμού και των αρμόδιων αρχών που ορίζονται ή συστήνονται σύμφωνα την οδηγία (ΕΕ) 2022/2555 σε οποιοδήποτε άλλο πρόσωπο ή αρχή, εκτός εάν προβλέπεται από τις διατάξεις του ενωσιακού ή εθνικού δικαίου.·

4. Όλες οι πληροφορίες που ανταλλάσσονται μεταξύ των αρμόδιων αρχών δυνάμει του παρόντος κανονισμού και αφορούν επιχειρηματικές ή επιχειρησιακές συνθήκες και άλλες οικονομικές ή προσωπικές υποθέσεις θεωρούνται εμπιστευτικές και υπόκεινται στις απαιτήσεις τήρησης του επαγγελματικού απορρήτου, εκτός εάν η αρμόδια αρχή δηλώσει κατά τον χρόνο επικοινωνίας ότι η συγκεκριμένη πληροφορία δύναται να γνωστοποιηθεί ή εκτός εάν η γνωστοποίηση είναι αναγκαία στο πλαίσιο νομικών διαδικασιών.

Άρθρο 56

Προστασία δεδομένων

1. Οι ΕΕΑ και οι αρμόδιες αρχές επιτρέπεται να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα μόνον όταν αυτό είναι αναγκαίο για την εκπλήρωση των αντίστοιχων υποχρεώσεων και καθηκόντων τους δυνάμει του παρόντος κανονισμού, ιδίως όσον αφορά την έρευνα, την επιθεώρηση, το αίτημα παροχής πληροφοριών, την κοινοποίηση, τη δημοσίευση, την αξιολόγηση, την εξακρίβωση, την εκτίμηση και την κατάρτιση σχεδίων εποπτείας. Τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 ή τον κανονισμό (ΕΕ) 2018/1725, ανάλογα με την περίπτωση.

2. Εκτός εάν προβλέπεται διαφορετικά σε άλλες τομεακές πράξεις, τα δεδομένα προσωπικού χαρακτήρα που αναφέρονται στην παράγραφο 1 διατηρούνται μέχρι την εκπλήρωση των εφαρμοστέων εποπτικών καθηκόντων και, σε κάθε περίπτωση, για μέγιστο χρονικό διάστημα 15 ετών, εκτός από την περίπτωση εκκρεμών δικαστικών διαδικασιών που απαιτούν περαιτέρω διατήρηση των δεδομένων αυτών.

ΚΕΦΑΛΑΙΟ VIII

Κατ' εξουσιοδότηση πράξεις

Άρθρο 57

Άσκηση της εξουσιοδότησης

1. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις υπό τους όρους του παρόντος άρθρου.

2. Η προβλεπόμενη στο άρθρο 31 παράγραφος 6 και στο άρθρο 43 παράγραφος 2 εξουσία έκδοσης κατ' εξουσιοδότηση πράξεων ανατίθεται στην Επιτροπή για περίοδο πέντε ετών από τις 17 Ιανουαρίου 2024. Η Επιτροπή υποβάλλει έκθεση σχετικά με τις εξουσίες που της έχουν ανατεθεί το αργότερο εννέα μήνες πριν από τη λήξη της περιόδου των πέντε ετών. Η εξουσιοδότηση ανανεώνεται σιωπηρά για περιόδους ίδιας διάρκειας, εκτός αν το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο προβάλουν αντιρρήσεις το αργότερο τρεις μήνες πριν από τη λήξη της κάθε περιόδου.

3. Η εξουσιοδότηση που προβλέπεται στο άρθρο 31 παράγραφος 6 και στο άρθρο 43 παράγραφος 2 μπορεί να ανακληθεί ανά πάσα στιγμή από το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο. Η απόφαση ανάκλησης περατώνει την εξουσιοδότηση που προσδιορίζεται στην εν λόγω απόφαση. Αρχίζει να ισχύει την επομένη της δημοσίευσης της απόφασης στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης* ή σε μεταγενέστερη ημερομηνία που ορίζεται σε αυτήν. Δεν θίγει το κύρος των κατ' εξουσιοδότηση πράξεων που ισχύουν ήδη.

4. Πριν από την έκδοση μιας κατ' εξουσιοδότηση πράξης, η Επιτροπή διεξάγει διαβουλεύσεις με εμπειρογνώμονες που ορίζουν τα κράτη μέλη σύμφωνα με τις αρχές της διοργανικής συμφωνίας της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου.

5. Μόλις εκδώσει μια κατ' εξουσιοδότηση πράξη, η Επιτροπή την κοινοποιεί ταυτόχρονα στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο.

6. Οι κατ' εξουσιοδότηση πράξεις που εκδίδονται σύμφωνα με το άρθρο 31 παράγραφος 6 και το άρθρο 43 παράγραφος 2 τίθενται σε ισχύ μόνον εάν δεν διατυπωθούν αντιρρήσεις είτε από το Ευρωπαϊκό Κοινοβούλιο είτε από το Συμβούλιο εντός προθεσμίας τριών μηνών από την κοινοποίηση της πράξης αυτής στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ή εάν, πριν από τη λήξη της προθεσμίας αυτής, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ενημερώσουν και τα δύο την Επιτροπή ότι δεν πρόκειται να προβάλουν αντιρρήσεις. Η προθεσμία αυτή παρατείνεται κατά τρεις μήνες κατόπιν πρωτοβουλίας του Ευρωπαϊκού Κοινοβουλίου ή του Συμβουλίου.

ΚΕΦΑΛΑΙΟ IX

Μεταβατικές και τελικές διατάξεις

Τμήμα I

Άρθρο 58

Ρήτρα επανεξέτασης

1. Έως τις 17 Ιανουαρίου 2028, η Επιτροπή, κατόπιν διαβούλευσης με τις ΕΕΑ και το ΕΣΣΚ, ανάλογα με την περίπτωση, επανεξετάζει και υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο έκθεση, συνοδευόμενη από νομοθετική πρόταση. Η επανεξέταση περιλαμβάνει τουλάχιστον τα ακόλουθα:

α) τα κριτήρια ορισμού των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 31 παράγραφος 2,

β) τον προαιρετικό χαρακτήρα της κοινοποίησης σημαντικών κυβερνοαπειλών, που αναφέρεται στο άρθρο 19,

γ) το καθεστώς που αναφέρεται στο άρθρο 31 παράγραφος 12 και τις εξουσίες του κύριου εποπτικού φορέα που προβλέπονται στο άρθρο 35 παράγραφος 1 στοιχείο δ) σημείο iv) πρώτη περίπτωση, με σκοπό την αξιολόγηση της αποτελεσματικότητας των εν λόγω διατάξεων όσον αφορά τη διασφάλιση της αποτελεσματικής εποπτείας κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ που είναι εγκατεστημένοι σε τρίτη χώρα, καθώς και της ανάγκης ίδρυσης θυγατρικής στην Ένωση.

Για τους σκοπούς του πρώτου εδαφίου του παρόντος στοιχείου, η επανεξέταση περιλαμβάνει ανάλυση του καθεστώτος που αναφέρεται στο άρθρο 31 παράγραφος 12, μεταξύ άλλων όσον αφορά την πρόσβαση των χρηματοοικονομικών οντοτήτων της Ένωσης σε υπηρεσίες από τρίτες χώρες και τη διαθεσιμότητα των εν λόγω υπηρεσιών στην αγορά της Ένωσης, και λαμβάνει υπόψη τις περαιτέρω εξελίξεις στις αγορές για τις υπηρεσίες που καλύπτονται από τον παρόντα κανονισμό, την πρακτική εμπειρία των χρηματοοικονομικών οντοτήτων και των χρηματοοικονομικών εποπτικών αρχών όσον αφορά την εφαρμογή και, αντίστοιχα, την εποπτεία του εν λόγω καθεστώτος, καθώς και τυχόν σχετικές ρυθμιστικές και εποπτικές εξελίξεις που σημειώνονται σε διεθνές επίπεδο,

δ) τη σκοπιμότητα της συμπερίληψης στο πεδίο εφαρμογής του παρόντος κανονισμού των χρηματοοικονομικών οντοτήτων που αναφέρονται στο άρθρο 2 παράγραφος 3 στοιχείο ε), οι οποίες κάνουν χρήση αυτοματοποιημένων συστημάτων πωλήσεων, υπό το πρίσμα των μελλοντικών εξελίξεων της αγοράς όσον αφορά τη χρήση των εν λόγω συστημάτων,

ε) τη λειτουργία και την αποτελεσματικότητα του ΔΚΕ όσον αφορά την υποστήριξη της συνέπειας της εποπτείας και της αποδοτικότητας της ανταλλαγής πληροφοριών εντός του πλαισίου εποπτείας.

2. Στο πλαίσιο της επανεξέτασης της οδηγίας (ΕΕ) 2015/2366, η Επιτροπή αξιολογεί την ανάγκη για αυξημένη κυβερνοανθεκτικότητα των συστημάτων πληρωμών και των δραστηριοτήτων επεξεργασίας πληρωμών, καθώς και τη σκοπιμότητα της επέκτασης του πεδίου εφαρμογής του παρόντος κανονισμού στους διαχειριστές συστημάτων πληρωμών και στις οντότητες που συμμετέχουν σε δραστηριότητες επεξεργασίας πληρωμών. Υπό το πρίσμα της αξιολόγησης αυτής, η Επιτροπή υποβάλλει, στο πλαίσιο της επανεξέτασης της οδηγίας (ΕΕ) 2015/2366, έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο το αργότερο έως τις 17 Ιουλίου 2023.

Με βάση την εν λόγω έκθεση επανεξέτασης και κατόπιν διαβούλευσης με τις ΕΕΑ, την ΕΚΤ και το ΕΣΣΚ, η Επιτροπή μπορεί να υποβάλει, κατά περίπτωση και στο πλαίσιο της νομοθετικής πρότασης που μπορεί να εγκρίνει σύμφωνα με το άρθρο 108 δεύτερο εδάφιο της οδηγίας (ΕΕ) 2015/2366, πρόταση για να εξασφαλιστεί ότι όλοι οι φορείς εκμετάλλευσης συστημάτων πληρωμών και οι οντότητες που συμμετέχουν σε δραστηριότητες επεξεργασίας πληρωμών υπόκεινται σε κατάλληλη εποπτεία, λαμβάνοντας παράλληλα υπόψη την υφιστάμενη εποπτεία της κεντρικής τράπεζας.

3. Έως τις 17 Ιανουαρίου 2026, η Επιτροπή, κατόπιν διαβούλευσης με τις ΕΕΑ και την Επιτροπή Ευρωπαϊκών Φορέων Εποπτείας των Ελεγκτών, επανεξετάζει και υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο έκθεση, συνοδευόμενη, κατά περίπτωση, από νομοθετική πρόταση, σχετικά με την καταλληλότητα των ενισχυμένων απαιτήσεων για τους νόμιμους ελεγκτές και τα ελεγκτικά γραφεία όσον αφορά την ψηφιακή επιχειρησιακή ανθεκτικότητα, μέσω της συμπερίληψης νόμιμων ελεγκτών και ελεγκτικών γραφείων στο πεδίο εφαρμογής του παρόντος κανονισμού ή μέσω τροποποιήσεων της οδηγίας 2006/43/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([39]).

ΤΜΉΜΑ ΙΙ

Τροποποιήσεις

Άρθρο 59

Τροποποιήσεις του κανονισμού (ΕΚ) αριθ. 1060/2009

Ο κανονισμός (ΕΚ) αριθ. 1060/2009 τροποποιείται ως εξής:

1) Στο παράρτημα Ι τμήμα Α σημείο 4), το πρώτο εδάφιο αντικαθίσταται από το ακόλουθο κείμενο:

«Ο οργανισμός αξιολόγησης πιστοληπτικής ικανότητας διαθέτει υγιείς διοικητικές και λογιστικές διαδικασίες, μηχανισμούς εσωτερικού ελέγχου, αποτελεσματικές διαδικασίες αξιολόγησης κινδύνων, καθώς και αποτελεσματικές ρυθμίσεις ελέγχου και προστασίας για τη διαχείριση των συστημάτων ΤΠΕ σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*).

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).».

2) Στο παράρτημα ΙΙΙ, το σημείο 12) αντικαθίσταται από το ακόλουθο κείμενο:

«12. Ο οργανισμός αξιολόγησης πιστοληπτικής ικανότητας παραβαίνει το άρθρο 6 παράγραφος 2, σε συνδυασμό με το σημείο 4) της ενότητας Α του παραρτήματος Ι, όταν δεν διαθέτει ορθές διοικητικές ή λογιστικές διαδικασίες, μηχανισμούς εσωτερικού ελέγχου, αποτελεσματικές διαδικασίες αξιολόγησης κινδύνων ή αποτελεσματικές ρυθμίσεις ελέγχου και προστασίας για τη διαχείριση συστημάτων ΤΠΕ σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 ή όταν δεν εφαρμόζει ή δεν διατηρεί διαδικασίες λήψης αποφάσεων ή οργανωτική διάρθρωση κατά τα απαιτούμενα από το εν λόγω σημείο.».

Άρθρο 60

Τροποποιήσεις του κανονισμού (ΕΕ) αριθ. 648/2012

Ο κανονισμός (ΕΕ) αριθ. 648/2012 τροποποιείται ως εξής:

1) Το άρθρο 26 τροποποιείται ως εξής:

α) η παράγραφος 3 αντικαθίσταται από το ακόλουθο κείμενο:

«3. Ο κεντρικός αντισυμβαλλόμενος διατηρεί και εφαρμόζει οργανωτική δομή η οποία διασφαλίζει τη συνέχεια και την εύρυθμη λειτουργία κατά την παροχή των υπηρεσιών και την άσκηση των δραστηριοτήτων του. Χρησιμοποιεί κατάλληλα και ανάλογα συστήματα, πόρους και διαδικασίες, συμπεριλαμβανομένων συστημάτων ΤΠΕ τα οποία διαχειρίζεται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*).

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).»·

([39]) Οδηγία 2006/43/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Μαΐου 2006**,** για τους υποχρεωτικούς ελέγχους των ετήσιων και των ενοποιημένων λογαριασμών, για την τροποποίηση των οδηγιών 78/660/ΕΟΚ και 83/349/ΕΟΚ του Συμβουλίου και για την κατάργηση της οδηγίας 84/253/ΕΟΚ του Συμβουλίου (ΕΕ L 157 της 9.6.2006, σ. 87).

β) η παράγραφος 6 διαγράφεται.

2) Το άρθρο 34 τροποποιείται ως εξής:

α) η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Ο κεντρικός αντισυμβαλλόμενος διαμορφώνει, εφαρμόζει και διατηρεί κατάλληλη πολιτική επιχειρησιακής συνέχειας και σχέδιο ανάκαμψης της λειτουργίας μετά από καταστροφή, στα οποία περιλαμβάνονται σχέδια πολιτικής επιχειρησιακής συνέχειας και αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ που λειτουργούν και εφαρμόζονται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 με σκοπό να διασφαλίσει τη διατήρηση των λειτουργιών του, την έγκαιρη αποκατάσταση των εργασιών και την εκπλήρωση των υποχρεώσεων του κεντρικού αντισυμβαλλομένου.»·

β) στην παράγραφο 3, το πρώτο εδάφιο αντικαθίσταται από το ακόλουθο κείμενο:

«3. Για να εξασφαλιστεί συνεπής εφαρμογή του παρόντος άρθρου, η ΕΑΚΑΑ, μετά από διαβούλευση με τα μέλη του ΕΣΚΤ, καταρτίζει σχέδια ρυθμιστικών τεχνικών προτύπων που να διευκρινίζουν το ελάχιστο περιεχόμενο και τις απαιτήσεις της πολιτικής επιχειρησιακής συνέχειας και του σχεδίου ανάκαμψης της λειτουργίας μετά από καταστροφή, με εξαίρεση τα σχέδια πολιτικής επιχειρησιακής συνέχειας και ανάκαμψης της λειτουργίας των ΤΠΕ μετά από καταστροφή.».

3) Στο άρθρο 56 παράγραφος 3, το πρώτο εδάφιο αντικαθίσταται από το ακόλουθο κείμενο:

«3. Προκειμένου να διασφαλίσει τη συνεπή εφαρμογή του παρόντος άρθρου, η ΕΑΚΑΑ καταρτίζει σχέδια ρυθμιστικών τεχνικών προτύπων για τον καθορισμό των λεπτομερών στοιχείων της αίτησης καταχώρισης που αναφέρεται στην παράγραφο 1, εκτός των απαιτήσεων που αφορούν τη διαχείριση κινδύνων ΤΠΕ.».

4) Στο άρθρο 79, οι παράγραφοι 1 και 2 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Το αρχείο καταγραφής συναλλαγών εντοπίζει τις πηγές λειτουργικού κινδύνου και τις ελαχιστοποιεί, με την ανάπτυξη επίσης κατάλληλων συστημάτων, δικλείδων ασφάλειας και διαδικασιών, συμπεριλαμβανομένων συστημάτων ΤΠΕ τα οποία διαχειρίζεται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554

2. Το αρχείο καταγραφής συναλλαγών διαμορφώνει, εφαρμόζει και διατηρεί κατάλληλη πολιτική επιχειρησιακής συνέχειας και σχέδιο ανάκαμψης της λειτουργίας μετά από καταστροφή, συμπεριλαμβανομένων σχεδίων πολιτικής επιχειρησιακής συνέχειας και αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ τα οποία καταρτίζονται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 με σκοπό να διασφαλίσει τη διατήρηση των λειτουργιών του, την έγκαιρη αποκατάσταση των εργασιών και την εκπλήρωση των υποχρεώσεων του αρχείου καταγραφής συναλλαγών.».

5) Στο άρθρο 80, η παράγραφος 1 διαγράφεται.

6) Στο παράρτημα Ι, το τμήμα ΙΙ τροποποιείται ως εξής:

α) τα στοιχεία α) και β) αντικαθίστανται από το ακόλουθο κείμενο:

«α) το αρχείο καταγραφής συναλλαγών παραβαίνει το άρθρο 79 παράγραφος 1 όταν δεν εντοπίζει τις πηγές λειτουργικού κινδύνου ή δεν ελαχιστοποιεί αυτούς τους κινδύνους με την ανάπτυξη κατάλληλων συστημάτων, δικλείδων ασφάλειας και διαδικασιών, συμπεριλαμβανομένων συστημάτων ΤΠΕ τα οποία διαχειρίζεται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554

β) το αρχείο καταγραφής συναλλαγών παραβαίνει το άρθρο 79 παράγραφος 2 όταν δεν καταρτίζει, δεν εφαρμόζει ή δεν διατηρεί κατάλληλο σχέδιο επιχειρησιακής συνέχειας και ανάκαμψης της λειτουργίας μετά από καταστροφή, το οποίο καταρτίζεται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 με σκοπό να διασφαλίσει τη διατήρηση των λειτουργιών του, την έγκαιρη αποκατάσταση των εργασιών και την εκπλήρωση των υποχρεώσεων του αρχείου καταγραφής συναλλαγών·»·

β) το στοιχείο γ) διαγράφεται.

7) Το παράρτημα ΙΙΙ τροποποιείται ως εξής:

α) το τμήμα ΙΙ τροποποιείται ως εξής:

i) το στοιχείο γ) αντικαθίσταται από το ακόλουθο κείμενο:

«γ) κεντρικός αντισυμβαλλόμενος κατηγορίας 2 παραβαίνει το άρθρο 26 παράγραφος 3 όταν δεν διατηρεί ή δεν εφαρμόζει οργανωτική δομή που διασφαλίζει τη συνέχεια και την εύρυθμη λειτουργία κατά την εκτέλεση των υπηρεσιών και των δραστηριοτήτων του ή όταν δεν χρησιμοποιεί κατάλληλα και αναλογικά συστήματα, πόρους ή διαδικασίες, συμπεριλαμβανομένων των συστημάτων ΤΠΕ τα οποία διαχειρίζεται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554»·

ii) το στοιχείο στ) διαγράφεται·

β) στο τμήμα III, το στοιχείο α) αντικαθίσταται από το ακόλουθο κείμενο:

«α) κεντρικός αντισυμβαλλόμενος κατηγορίας 2 παραβαίνει το άρθρο 34 παράγραφος 1 όταν δεν διαμορφώνει, δεν εφαρμόζει και δεν διατηρεί κατάλληλη πολιτική επιχειρησιακής συνέχειας και σχέδιο αντιμετώπισης και ανάκαμψης το οποίο καταρτίζεται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 με σκοπό να διασφαλίσει τη διατήρηση των λειτουργιών του, την έγκαιρη αποκατάσταση των εργασιών και την εκπλήρωση των υποχρεώσεων του κεντρικού αντισυμβαλλομένου, η οποία επιτρέπει τουλάχιστον την αποκατάσταση όλων των συναλλαγών κατά τη στιγμή της διαταραχής, ώστε να είναι σε θέση ο κεντρικός αντισυμβαλλόμενος να εξακολουθήσει να λειτουργεί με ασφάλεια και να ολοκληρώσει τον διακανονισμό στην καθορισμένη ημερομηνία·».

Άρθρο 61

Τροποποιήσεις του κανονισμού (ΕΕ) αριθ. 909/2014

Το άρθρο 45 του κανονισμού (ΕΕ) αριθ. 909/2014 τροποποιείται ως εξής:

1) Η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Το ΚΑΤ προσδιορίζει όλες τις πηγές λειτουργικού κινδύνου, εσωτερικές και εξωτερικές, και ελαχιστοποιεί τον αντίκτυπό τους μέσω της ανάπτυξης κατάλληλων εργαλείων, διαδικασιών και πολιτικών ΤΠΕ που έχουν θεσπιστεί και τελούν υπό διαχείριση σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*), καθώς και μέσω οποιωνδήποτε άλλων σχετικών κατάλληλων εργαλείων, δικλείδων ασφάλειας και διαδικασιών για άλλα είδη λειτουργικού κινδύνου, μεταξύ άλλων για όλα τα συστήματα διακανονισμού αξιογράφων που διαχειρίζεται.

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).».

2) Η παράγραφος 2 διαγράφεται.

3) Οι παράγραφοι 3 και 4 αντικαθίστανται από το ακόλουθο κείμενο:

«3. Για τις υπηρεσίες που παρέχει καθώς και για κάθε σύστημα διακανονισμού αξιογράφων που διαχειρίζεται, το ΚΑΤ διαμορφώνει, εφαρμόζει και διατηρεί κατάλληλη πολιτική επιχειρησιακής συνέχειας και σχέδιο ανάκαμψης της λειτουργίας μετά από καταστροφή, συμπεριλαμβανομένων πολιτικής επιχειρησιακής συνέχειας και σχεδίων αντιμετώπισης και ανάκαμψης της λειτουργίας των ΤΠΕ μετά από καταστροφή τα οποία καταρτίζονται σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 για να διασφαλίσει τη διατήρηση των υπηρεσιών του, την έγκαιρη αποκατάσταση των εργασιών και την εκπλήρωση των υποχρεώσεών του, σε περίπτωση γεγονότων που συνεπάγονται σημαντικό κίνδυνο διαταραχής των λειτουργιών.

4. Το σχέδιο που αναφέρεται στην παράγραφο 3 προβλέπει την αποκατάσταση όλων των συναλλαγών και των θέσεων των συμμετεχόντων κατά τον χρόνο της διακοπής, ώστε να μπορέσουν οι συμμετέχοντες του ΚΑΤ να εξακολουθήσουν να λειτουργούν με ασφάλεια και να ολοκληρώσουν τον διακανονισμό στην καθορισμένη ημερομηνία, μεταξύ άλλων διασφαλίζοντας ότι τα κρίσιμα συστήματα ΤΠ μπορούν ταχέως να αποκαταστήσουν τη λειτουργία τους ως είχε κατά τη στιγμή της διαταραχής, όπως προβλέπεται στο άρθρο 12 παράγραφοι 5 και 7 του κανονισμού (ΕΕ) 2022/2554».

4) Η παράγραφος 6 αντικαθίσταται από το ακόλουθο κείμενο:

«6. Το ΚΑΤ προσδιορίζει, παρακολουθεί και διαχειρίζεται τους κινδύνους που ενδέχεται να συνεπάγονται για τις δραστηριότητές του οι βασικοί συμμετέχοντες στα συστήματα διακανονισμού αξιογράφων που διαχειρίζεται, καθώς και οι πάροχοι υπηρεσιών και υπηρεσιών κοινής ωφελείας, άλλα ΚΑΤ ή άλλες υποδομές της αγοράς. Παρέχει πληροφορίες στις αρμόδιες και τις σχετικές αρχές, κατόπιν αιτήματος, σχετικά με οποιονδήποτε τέτοιον κίνδυνο εντοπιστεί. Ενημερώνει επίσης χωρίς καθυστέρηση την αρμόδια αρχή και τις σχετικές αρχές σχετικά με οποιαδήποτε περιστατικά που αφορούν τη λειτουργία του, εκτός των συμβάντων που σχετίζονται με κινδύνους ΤΠΕ, και οφείλονται στους εν λόγω κινδύνους.».

5) Στην παράγραφο 7, το πρώτο εδάφιο αντικαθίσταται από το ακόλουθο κείμενο:

«7. Η ΕΑΚΑΑ, σε στενή συνεργασία με τα μέλη του ΕΣΚΤ, καταρτίζει σχέδια ρυθμιστικών τεχνικών προτύπων για να εξειδικεύσει τους λειτουργικούς κινδύνους που αναφέρονται στις παραγράφους 1 και 6, πλην του κινδύνου ΤΠΕ, τις μεθόδους ελέγχου, αντιμετώπισης ή ελαχιστοποίησης των εν λόγω κινδύνων, συμπεριλαμβανομένων των πολιτικών επιχειρησιακής συνέχειας και των σχεδίων ανάκαμψης της λειτουργίας μετά από καταστροφή, που αναφέρονται στις παραγράφους 3 και 4, καθώς και των μεθόδων αξιολόγησής τους.».

Άρθρο 62

Τροποποιήσεις του κανονισμού (ΕΕ) αριθ. 600/2014

Ο κανονισμός (ΕΕ) αριθ. 600/2014 τροποποιείται ως εξής:

1) Το άρθρο 27ζ τροποποιείται ως εξής:

α) η παράγραφος 4 αντικαθίσταται από το ακόλουθο κείμενο:

«4. Οι ΕΜΔ συμμορφώνονται με τις απαιτήσεις σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών που ορίζονται στον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*).

_____

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).»·

β) στην παράγραφο 8, το στοιχείο γ) αντικαθίσταται από το ακόλουθο κείμενο:

«γ) τις συγκεκριμένες οργανωτικές απαιτήσεις που ορίζονται στις παραγράφους 3 και 5.».

2) Το άρθρο 27η τροποποιείται ως εξής:

α) η παράγραφος 5 αντικαθίσταται από το ακόλουθο κείμενο:

«5. Οι ΠΕΔ συμμορφώνονται με τις απαιτήσεις σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών που ορίζονται στον κανονισμό (ΕΕ) 2022/2554»·

β) στην παράγραφο 8, το στοιχείο ε) αντικαθίσταται από το ακόλουθο κείμενο:

«ε) τις συγκεκριμένες οργανωτικές απαιτήσεις που ορίζονται στην παράγραφο 4.».

3) Το άρθρο 27θ τροποποιείται ως εξής:

α) η παράγραφος 3 αντικαθίσταται από το ακόλουθο κείμενο:

«3. Οι ΕΜΑ συμμορφώνονται με τις απαιτήσεις σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών που ορίζονται στον κανονισμό (ΕΕ) 2022/2554»·

β) στην παράγραφο 5, το στοιχείο β) αντικαθίσταται από το ακόλουθο κείμενο:

«β) τις συγκεκριμένες οργανωτικές απαιτήσεις που ορίζονται στις παραγράφους 2 και 4.».

Άρθρο 63

Τροποποίηση του κανονισμού (ΕΕ) 2016/1011

Στο άρθρο 6 του κανονισμού (ΕΕ) 2016/1011, προστίθεται η ακόλουθη παράγραφος:

«6. Για τους δείκτες αναφοράς κρίσιμης σημασίας, ένας διαχειριστής διαθέτει υγιείς διοικητικές και λογιστικές διαδικασίες, μηχανισμούς εσωτερικού ελέγχου, αποτελεσματικές διαδικασίες αξιολόγησης κινδύνων, καθώς και αποτελεσματικές ρυθμίσεις ελέγχου και προστασίας για τη διαχείριση των συστημάτων ΤΠΕ σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*).·

_____

(*) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).».

Άρθρο 64

Έναρξη ισχύος και εφαρμογή

Ο παρών κανονισμός αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Εφαρμόζεται από τις 17 Ιανουαρίου 2025.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Στρασβούργο, 14 Δεκεμβρίου 2022.

Για το Ευρωπαϊκό Κοινοβούλιο	*Για το Συμβούλιο*
Η Πρόεδρος	*Ο Πρόεδρος*
R. METSOLA	M. BEK