Ευρωπαϊκό Κοινοβούλιο
2019-2024

Έγγραφο συνόδου

A9-0341/2021

7.12.2021

***I
ΕΚΘΕΣΗ

σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που αφορά 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
(COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

Επιτροπή Οικονομικής και Νομισματικής Πολιτικής

Εισηγητής: Billy Kelleher

Υπόμνημα για τα χρησιμοποιούμενα σύμβολα

*	Διαδικασία διαβούλευσης
***	Διαδικασία έγκρισης
***I	Συνήθης νομοθετική διαδικασία (πρώτη ανάγνωση)
***II	Συνήθης νομοθετική διαδικασία (δεύτερη ανάγνωση)
***III	Συνήθης νομοθετική διαδικασία (τρίτη ανάγνωση)

(Η ενδεικνυόμενη διαδικασία στηρίζεται στη νομική βάση που προτείνεται στο σχέδιο πράξης)

Τροπολογίες σε σχέδιο πράξης

Τροπολογίες του Κοινοβουλίου σε δύο στήλες

Η διαγραφή κειμένου σημαίνεται με ***πλάγιους έντονους χαρακτήρες*** στην αριστερή στήλη. Η αντικατάσταση κειμένου σημαίνεται με ***πλάγιους έντονους χαρακτήρες*** και στις δύο στήλες. Το νέο κείμενο σημαίνεται με ***πλάγιους έντονους χαρακτήρες*** στη δεξιά στήλη.

Η πρώτη και η δεύτερη γραμμή της επικεφαλίδας κάθε τροπολογίας προσδιορίζουν το σχετικό τμήμα του εξεταζόμενου σχεδίου πράξης. Εάν μία τροπολογία αναφέρεται σε ήδη υφιστάμενη πράξη την οποία το σχέδιο πράξης αποσκοπεί να τροποποιήσει, η επικεφαλίδα περιέχει επιπλέον και μία τρίτη και μία τέταρτη γραμμή που προσδιορίζουν αντίστοιχα την υφιστάμενη πράξη και τη διάταξή της στην οποία αναφέρεται η τροπολογία.

Τροπολογίες του Κοινοβουλίου με μορφή ενοποιημένου κειμένου

Τα νέα τμήματα του κειμένου σημαίνονται με ***πλάγιους έντονους χαρακτήρες.*** Τα τμήματα του κειμένου που απαλείφονται σημαίνονται με το σύμβολο ▌ ή με διαγραφή. Η αντικατάσταση κειμένου σημαίνεται με πλάγιους έντονους χαρακτήρες που υποδηλώνουν το νέο κείμενο και με διαγραφή του κειμένου που αντικαθίσταται.
Κατ' εξαίρεση, δεν σημαίνονται οι τροποποιήσεις αυστηρά τεχνικής φύσης που επιφέρουν οι υπηρεσίες κατά την επεξεργασία του τελικού κειμένου.

ΠΕΡΙΕΧΟΜΕΝΑ

Σελίδα

ΣΧΕΔΙΟ ΝΟΜΟΘΕΤΙΚΟΥ ΨΗΦΙΣΜΑΤΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ

σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που αφορά 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
(COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

(Συνήθης νομοθετική διαδικασία: πρώτη ανάγνωση)

Το Ευρωπαϊκό Κοινοβούλιο,

– έχοντας υπόψη την πρόταση της Επιτροπής προς το Κοινοβούλιο και το Συμβούλιο (COM(2020)0595),

– έχοντας υπόψη το άρθρο 294 παράγραφος 2 και το άρθρο 114 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, σύμφωνα με τα οποία του υποβλήθηκε η πρόταση από την Επιτροπή (C9-0304/2020),

– έχοντας υπόψη το άρθρο 294 παράγραφος 3 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης,

– έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής της 24ης Φεβρουαρίου 2021[1],

– έχοντας υπόψη το άρθρο 59 του Κανονισμού του,

– έχοντας υπόψη την έκθεση της Επιτροπής Οικονομικής και Νομισματικής Πολιτικής (A9-0341/2021),

1. εγκρίνει τη θέση του σε πρώτη ανάγνωση όπως παρατίθεται κατωτέρω·

2. ζητεί από την Επιτροπή να υποβάλει εκ νέου την πρόταση στο Κοινοβούλιο, αν την αντικαταστήσει με νέο κείμενο, αν της επιφέρει σημαντικές τροποποιήσεις ή αν προτίθεται να της επιφέρει σημαντικές τροποποιήσεις·

2. αναθέτει στον Πρόεδρό του να διαβιβάσει τη θέση του Κοινοβουλίου στο Συμβούλιο, στην Επιτροπή και στα εθνικά κοινοβούλια.

[1] ΕΕ C 155 της 30.4.2021, σ. 38.

Τροπολογία 1

ΤΡΟΠΟΛΟΓΙΕΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ*

στην πρόταση της Επιτροπής

2020/0266(COD)

Πρόταση

ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

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

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ 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[2],

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής[3],

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία,

Εκτιμώντας τα ακόλουθα:

(1) Στην ψηφιακή εποχή, οι τεχνολογίες των πληροφοριών και των επικοινωνιών (ΤΠΕ) υποστηρίζουν σύνθετα συστήματα που χρησιμοποιούνται για καθημερινές κοινωνικές δραστηριότητες. Διασφαλίζουν την αδιάλειπτη λειτουργία των οικονομιών μας σε βασικούς τομείς, συμπεριλαμβανομένου του χρηματοοικονομικού τομέα, και ενισχύουν τη λειτουργία της ενιαίας αγοράς. Η αυξημένη ψηφιοποίηση και διασυνδεσιμότητα εντείνουν επίσης τους κινδύνους ΤΠΕ, οι οποίοι καθιστούν την

* Τροπολογίες: το νέο ή το τροποποιημένο κείμενο σημειώνεται με έντονους πλάγιους χαρακτήρες· οι διαγραφές σημειώνονται με το σύμβολο ▌.

2 [*Να προστεθεί παραπομπή*] ΕΕ C της, σ. .

3 ΕΕ C 155 της 30.4.2021, σ. 38.

κοινωνία συνολικά – και ειδικότερα το χρηματοπιστωτικό 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 όλων των δραστηριοτήτων των χρηματοπιστωτικών οντοτήτων της Ένωσης, η ψηφιακή ανθεκτικότητα δεν έχει ενσωματωθεί ακόμη επαρκώς στα επιχειρησιακά τους πλαίσια.

(2) Κατά τις τελευταίες δεκαετίες, η χρήση ΤΠΕ έχει αποκτήσει καθοριστικό ρόλο στον χρηματοοικονομικό τομέα, δεδομένου ότι είναι πλέον σήμερα κρίσιμης σημασίας για τη διασφάλιση των συνήθων καθημερινών λειτουργιών όλων των χρηματοπιστωτικών οντοτήτων. Η ψηφιοποίηση καλύπτει, 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 απαιτήσεων και τις υπηρεσίες υποστήριξης (back-office). ***Η χρήση της τεχνολογίας ΤΠΕ έχει επίσης μετασχηματίσει τον ασφαλιστικό τομέα, από την εμφάνιση ψηφιακών ασφαλιστικών διαμεσολαβητών που λειτουργούν με την InsurTech έως την ψηφιακή ανάληψη ασφαλιστικών κινδύνων και τη διανομή συμβάσεων.*** Εκτός του υψηλού βαθμού ψηφιοποίησης σε ολόκληρο τον χρηματοοικονομικό τομέα, η ψηφιοποίηση έχει εμβαθύνει επίσης τις διασυνδέσεις και τις εξαρτήσεις εντός του χρηματοπιστωτικού τομέα, καθώς και με τρίτους παρόχους υποδομών και υπηρεσιών.

(3) Σε έκθεση του 2020 σχετικά με τον συστημικό κίνδυνο στον κυβερνοχώρο[4], το Ευρωπαϊκό Συμβούλιο Συστημικών Κινδύνων (ΕΕΣΚ) επιβεβαίωσε τον τρόπο με τον οποίο το υφιστάμενο υψηλό επίπεδο διασυνδεσιμότητας μεταξύ των χρηματοπιστωτικών οντοτήτων, των χρηματοπιστωτικών αγορών και των υποδομών χρηματοπιστωτικών αγορών, και ιδίως οι αλληλεξαρτήσεις των οικείων συστημάτων ΤΠΕ, μπορεί δυνητικά να αποτελέσει συστημική ευπάθεια, δεδομένου ότι τοπικά κυβερνοπεριστατικά θα μπορούσαν να εξαπλωθούν ταχέως από οποιαδήποτε από τις περίπου 22 000 χρηματοπιστωτικές οντότητες της Ένωσης[5] σε ολόκληρο το χρηματοπιστωτικό σύστημα, χωρίς να εμποδίζονται από τα γεωγραφικά σύνορα. Οι σοβαρές παραβιάσεις των ΤΠΕ που ανακύπτουν στον χρηματοπιστωτικό τομέα δεν επηρεάζουν μόνο μεμονωμένες χρηματοπιστωτικές οντότητες. Διευκολύνουν επίσης τη διάδοση τοπικών ευπαθειών στους διαύλους μετάδοσης και μπορούν να έχουν δυσμενείς συνέπειες για τη σταθερότητα του χρηματοπιστωτικού συστήματος της Ένωσης, προκαλώντας εκροές ρευστότητας και συνολική απώλεια της αξιοπιστίας των

---

4 Έκθεση της ΕΕΣΚ σχετικά με τον συστημικό κίνδυνο στον κυβερνοχώρο, Φεβρουάριος 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

5 Σύμφωνα με την εκτίμηση επιπτώσεων που συνοδεύει την επανεξέταση των ευρωπαϊκών εποπτικών αρχών [SWD(2017) 308], υπάρχουν περίπου 5 665 πιστωτικά ιδρύματα, 5 934 επιχειρήσεις επενδύσεων, 2 666 ασφαλιστικές επιχειρήσεις, 1 573 ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών (ΙΕΣΠ), 2 500 εταιρείες διαχείρισης επενδύσεων, 350 υποδομές αγοράς [όπως κεντρικοί αντισυμβαλλόμενοι, χρηματιστήρια, συστημικοί εσωτερικοποιητές, αρχεία καταγραφής συναλλαγών και πολυμερείς μηχανισμοί διαπραγμάτευσης (ΠΜΔ)], 45 οργανισμοί αξιολόγησης της πιστοληπτικής ικανότητας, καθώς και 2 500 ιδρύματα πληρωμών με άδεια λειτουργίας και ιδρύματα ηλεκτρονικού χρήματος. Αθροιστικά, πρόκειται για περίπου 21 233 οντότητες, μη συμπεριλαμβανομένων των οντοτήτων πληθοχρηματοδότησης, των νόμιμων ελεγκτών και ελεγκτικών γραφείων, των παρόχων υπηρεσιών κρυπτοστοιχείων και των διαχειριστών δεικτών αναφοράς.

χρηματοπιστωτικών αγορών και της εμπιστοσύνης σε αυτές.

(4) Κατά τα τελευταία έτη οι κίνδυνοι ΤΠΕ έχουν προσελκύσει την προσοχή εθνικών, ευρωπαϊκών και διεθνών φορέων χάραξης πολιτικής, ρυθμιστικών αρχών και οργανισμών τυποποίησης, στο πλαίσιο μιας απόπειρας ενίσχυσης της ανθεκτικότητας, καθορισμού προτύπων και συντονισμού των κανονιστικών ή εποπτικών εργασιών. 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 ομάδες χωρών 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 χρηματοπιστωτικών τους συστημάτων. ***Κατά συνέπεια, είναι απαραίτητο να ληφθούν υπόψη οι κίνδυνοι ΤΠΕ στο πλαίσιο ενός εξαιρετικά διασυνδεδεμένου παγκόσμιου χρηματοπιστωτικού συστήματος στο οποίο πρέπει να δίδεται προτεραιότητα στη συνοχή των διεθνών κανονισμών και τη συνεργασία μεταξύ των αρμόδιων αρχών παγκοσμίως.***

(5) Παρά την ανάληψη στοχευμένων εθνικών και ευρωπαϊκών πολιτικών και νομοθετικών πρωτοβουλιών, οι κίνδυνοι ΤΠΕ εξακολουθούν να συνιστούν πρόκληση για την επιχειρησιακή ανθεκτικότητα, τις επιδόσεις και τη σταθερότητα του χρηματοπιστωτικού συστήματος της Ένωσης. Η μεταρρύθμιση που ακολούθησε μετά τη χρηματοπιστωτική κρίση του 2008 ενίσχυσε πρωτίστως τη χρηματοπιστωτική ανθεκτικότητα του χρηματοπιστωτικού τομέα της Ένωσης και αποσκοπούσε στη διαφύλαξη της ανταγωνιστικότητας και της σταθερότητας της Ένωσης από πλευράς οικονομίας, προληπτικής εποπτείας και 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 την κρίση, ενώ έχουν αναπτυχθεί μόνο σε ορισμένους τομείς του πολιτικού και κανονιστικού πλαισίου της Ένωσης για τις χρηματοπιστωτικές υπηρεσίες ή μόνο σε μερικά κράτη μέλη.

(6) Στο σχέδιο δράσης της Επιτροπής του 2018 για τη χρηματοοικονομική τεχνολογία[6] επισημάνθηκε η θεμελιώδης σημασία της ενίσχυσης της ανθεκτικότητας του χρηματοπιστωτικού τομέα της Ένωσης και 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 χρηματοπιστωτικών 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 Αρχή Τραπεζών (ΕΒΑ), η Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών (ESMA) και η Ευρωπαϊκή Αρχή Ασφαλίσεων και Επαγγελματικών Συντάξεων (EIOPA) (συλλογικά στο εξής: ευρωπαϊκές εποπτικές

[6] Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Κεντρική Τράπεζα, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, *Σχέδιο δράσης για τη χρηματοοικονομική τεχνολογία: Για έναν πιο ανταγωνιστικό και καινοτόμο ευρωπαϊκό χρηματοπιστωτικό τομέα*, COM(2018)0109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.

αρχές ή ΕΕΑ) εξέδωσαν από κοινού δύο έγγραφα τεχνικών γνωμοδοτήσεων, στις οποίες διατύπωναν έκκληση για συνεκτική προσέγγιση όσον αφορά τον κίνδυνο ΤΠΕ στον χρηματοπιστωτικό τομέα και σύσταση για ενίσχυση της ψηφιακής επιχειρησιακής ανθεκτικότητας του κλάδου των χρηματοπιστωτικών υπηρεσιών, κατά τρόπο αναλογικό, μέσω ειδικής τομεακής πρωτοβουλίας της Ένωσης.

(8) Ο χρηματοπιστωτικός τομέας της Ένωσης ρυθμίζεται από το εναρμονισμένο ενιαίο εγχειρίδιο κανόνων και διέπεται από το ευρωπαϊκό σύστημα χρηματοπιστωτικής 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 χρηματοπιστωτικής 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 αυτή τη συνιστώσα, με ***την ενίσχυση*** των εντολών των αρχών χρηματοπιστωτικής εποπτείας ***να διαχειρίζονται τους κινδύνους ΤΠΕ στον χρηματοπιστωτικό τομέα, να προστατεύουν την ακεραιότητα και την αποτελεσματικότητα*** της ***ενιαίας*** αγοράς ***και να διευκολύνουν την εύρυθμη λειτουργία της***.

(9) Οι νομοθετικές διαφορές και οι ανομοιόμορφες εθνικές κανονιστικές και εποπτικές προσεγγίσεις όσον αφορά τον κίνδυνο ΤΠΕ εγείρουν φραγμούς στην ενιαία αγορά χρηματοπιστωτικών υπηρεσιών, παρεμποδίζοντας με τον τρόπο αυτόν την απρόσκοπτη άσκηση της ελευθερίας εγκατάστασης και της παροχής υπηρεσιών για τις χρηματοπιστωτικές οντότητες με διασυνοριακή παρουσία. Είναι επίσης πιθανό να προκαλούνται στρεβλώσεις στον ανταγωνισμό μεταξύ των χρηματοπιστωτικών οντοτήτων του ιδίου τύπου που δραστηριοποιούνται σε διαφορετικά κράτη μέλη. Ειδικότερα σε τομείς στους οποίους η εναρμόνιση σε ενωσιακό επίπεδο ήταν εξαιρετικά περιορισμένη –όπως οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας– ή απούσα –όπως η παρακολούθηση του κινδύνου τρίτων παρόχων ΤΠΕ–, οι διαφορές που οφείλονται στις προβλεπόμενες εξελίξεις σε εθνικό επίπεδο θα μπορούσαν να δημιουργήσουν περαιτέρω φραγμούς για τη λειτουργία της ενιαίας αγοράς εις βάρος των συμμετεχόντων στην αγορά και της χρηματοπιστωτικής σταθερότητας.

(10) Ο αποσπασματικός τρόπος με τον οποίο έχουν εξεταστεί μέχρι στιγμής οι σχετικές με τον κίνδυνο ΤΠΕ διατάξεις σε επίπεδο Ένωσης καταδεικνύει κενά ή αλληλεπικαλύψεις σε σημαντικούς τομείς, όπως η αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ και οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας, ενώ δημιουργεί επίσης ασυνέπειες λόγω 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 χρηματοπιστωτικός τομέας αναπτύσσει τις υπηρεσίες του σε ευρεία διασυνοριακή βάση, τόσο εντός όσο και εκτός της Ένωσης.

Οι μεμονωμένες χρηματοπιστωτικές οντότητες που δραστηριοποιούνται σε διασυνοριακή βάση ή είναι κάτοχοι πολλών αδειών (π.χ. μία χρηματοπιστωτική 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, επενδυτική εταιρεία και άδεια ιδρύματος πληρωμών, καθεμία από τις οποίες εκδίδεται 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.

(10α) Η δημιουργία και η διατήρηση επαρκών υποδομών συστημάτων δικτύου και πληροφοριών αποτελεί επίσης θεμελιώδη προϋπόθεση για την αποτελεσματική συγκέντρωση δεδομένων κινδύνου και πρακτικών αναφοράς κινδύνων, οι οποίες με τη σειρά τους αποτελούν βασική προϋπόθεση για την ορθή και βιώσιμη διαχείριση των κινδύνων και για τις διαδικασίες λήψης αποφάσεων των πιστωτικών ιδρυμάτων. Η Επιτροπή της Βασιλείας για την τραπεζική εποπτεία (BCBS) δημοσίευσε το 2013 ένα σύνολο αρχών για την αποτελεσματική συγκέντρωση δεδομένων κινδύνου και την υποβολή στοιχείων κινδύνου («BCBS 239») βάσει δύο γενικών αρχών διακυβέρνησης και υποδομής ΤΠ, που θα εφαρμοστούν στις αρχές του 2016. Σύμφωνα με την έκθεση της Ευρωπαϊκής Κεντρικής Τράπεζας (ΕΚΤ) του Μαΐου 2018 σχετικά με τη θεματική επισκόπηση για την αποτελεσματική συγκέντρωση δεδομένων κινδύνου και την υποβολή εκθέσεων σχετικά με τους κινδύνους, του Μαΐου 2018, και την έκθεση προόδου της BCBS του Απριλίου 2020, η πρόοδος που σημείωσαν οι παγκόσμιες συστημικά σημαντικές τράπεζες όσον αφορά την εφαρμογή δεν ήταν ικανοποιητική και αποτέλεσε πηγή ανησυχίας. Προκειμένου να διευκολυνθεί η συμμόρφωση και η ευθυγράμμιση με τα διεθνή πρότυπα, η Επιτροπή, σε στενή συνεργασία με την ΕΚΤ και κατόπιν διαβούλευσης με την ΕΑΤ και το ΕΣΣΚ, θα πρέπει να εκπονήσει έκθεση για την αξιολόγηση του τρόπου με τον οποίο οι αρχές BCBS 239 αλληλεπιδρούν με τις διατάξεις του παρόντος κανονισμού και, κατά περίπτωση, του τρόπου με τον οποίο οι αρχές αυτές θα πρέπει να ενσωματωθούν στο δίκαιο της Ένωσης.

(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 χρηματοπιστωτικές οντότητες. Οι ικανότητες και η συνολική ανθεκτικότητα που θα αναπτύξουν οι χρηματοπιστωτικές οντότητες, σύμφωνα με τις εν λόγω βασικές απαιτήσεις, με σκοπό την αντιμετώπιση επιχειρησιακών διακοπών λειτουργίας, θα συμβάλουν στη διατήρηση της σταθερότητας και της ακεραιότητας των χρηματοπιστωτικών 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 ΣΛΕΕ, όπως ερμηνεύονται σύμφωνα με την πάγια νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης.

(12) Με τον παρόντα κανονισμό επιδιώκεται καταρχάς η ενοποίηση και η αναβάθμιση των απαιτήσεων σχετικά με τους κινδύνους ΤΠΕ, οι οποίες αντιμετωπίζονται μέχρι στιγμής χωριστά στους διάφορους κανονισμούς και οδηγίες. Παρότι οι εν λόγω νομικές πράξεις της Ένωσης κάλυπταν τις κύριες κατηγορίες χρηματοοικονομικών κινδύνων (π.χ. πιστωτικό κίνδυνο, κίνδυνο αγοράς, πιστωτικό κίνδυνο αντισυμβαλλομένου και

κίνδυνο ρευστότητας, κίνδυνο συμπεριφοράς της αγοράς), δεν μπορούσαν να αντιμετωπίσουν συνολικά, κατά τον χρόνο έκδοσής τους, όλες τις συνιστώσες της επιχειρησιακής ανθεκτικότητας. Οι απαιτήσεις 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 θέσπισης στοχευμένων ποιοτικών απαιτήσεων για την ενίσχυση των ικανοτήτων μέσω απαιτήσεων που αφορούν τις ικανότητες προστασίας, εντοπισμού, περιορισμού, αποκατάστασης και επιδιόρθωσης συμβάντων σχετικών με τις ΤΠΕ ή μέσω της θέσπισης ικανοτήτων αναφοράς και ψηφιακών δοκιμών. Οι εν λόγω οδηγίες και κανονισμοί είχαν ως πρωταρχικό στόχο την κάλυψη βασικών κανόνων προληπτικής εποπτείας, ακεραιότητας ή δεοντολογίας της αγοράς.

Μέσω της διαδικασίας αυτής, η οποία ενοποιεί και επικαιροποιεί τους κανόνες σχετικά με τον κίνδυνο ΤΠΕ, όλες οι διατάξεις που αφορούν τον ψηφιακό κίνδυνο στον χρηματοοικονομικό τομέα θα συγκεντρωθούν για πρώτη φορά με συνεκτικό τρόπο σε μια ενιαία νομοθετική πράξη. Κατά συνέπεια, η παρούσα πρωτοβουλία θα πρέπει να καλύπτει τα κενά ή να διορθώνει τις ασυνέπειες που παρουσιάζουν ορισμένες από τις συγκεκριμένες νομοθετικές πράξεις, μεταξύ άλλων σε σχέση με την ορολογία που χρησιμοποιείται σε αυτές, ενώ θα πρέπει επίσης να αναφέρεται ρητά στον κίνδυνο ΤΠΕ μέσω στοχευμένων κανόνων για τις ικανότητες διαχείρισης κινδύνων ΤΠΕ, την υποβολή εκθέσεων και τις δοκιμές, καθώς και για την παρακολούθηση των κινδύνων τρίτων παρόχων. ***Η πρωτοβουλία αυτή αποσκοπεί επίσης στην ευαισθητοποίηση σχετικά με τους κινδύνους ΤΠΕ και αναγνωρίζει ότι τα συμβάντα ΤΠΕ και η έλλειψη επιχειρησιακής ανθεκτικότητας ενδέχεται να θέσουν σε κίνδυνο την οικονομική ευρωστία των χρηματοπιστωτικών οντοτήτων.***

(13) Κατά την αντιμετώπιση του κινδύνου ΤΠΕ, οι χρηματοπιστωτικές οντότητες θα πρέπει να ακολουθούν την ίδια προσέγγιση και τους ίδιους κανόνες βάσει αρχών, ***ανάλογα με το μέγεθος, τη φύση, την πολυπλοκότητα και το προφίλ κινδύνου τους***. Η συνοχή συμβάλλει στην ενίσχυση της εμπιστοσύνης στο χρηματοπιστωτικό σύστημα και στη διατήρηση της σταθερότητάς του, ιδίως σε περιόδους ***υψηλής εξάρτησης*** από συστήματα, πλατφόρμες και υποδομές ΤΠΕ, η οποία συνεπάγεται αυξημένο ψηφιακό κίνδυνο.

Στο πλαίσιο της τήρησης μιας 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) Η χρήση κανονισμού συμβάλλει στη μείωση της πολυπλοκότητας του κανονιστικού πλαισίου, ενισχύει την εποπτική σύγκλιση, αυξάνει την ασφάλεια δικαίου, ενώ συνδράμει επίσης στον περιορισμό του κόστους συμμόρφωσης, ιδίως για τις χρηματοπιστωτικές οντότητες που δραστηριοποιούνται σε διασυνοριακή βάση, καθώς και στη μείωση των στρεβλώσεων του ανταγωνισμού. Ως εκ τούτου, φαίνεται ότι η επιλογή κανονισμού για τη θέσπιση κοινού πλαισίου για την ψηφιακή επιχειρησιακή ανθεκτικότητα των χρηματοπιστωτικών οντοτήτων συνιστά τον πλέον κατάλληλο τρόπο για τη διασφάλιση ομοιογενούς και συνεκτικής εφαρμογής όλων των συνιστωσών της διαχείρισης κινδύνων ΤΠΕ από τους χρηματοπιστωτικούς τομείς της Ένωσης.

(14α) Ωστόσο, η εφαρμογή του παρόντος κανονισμού δεν θα πρέπει να παρεμποδίζει την καινοτομία όσον αφορά τον τρόπο με τον οποίο οι χρηματοπιστωτικές οντότητες αντιμετωπίζουν ζητήματα ψηφιακής επιχειρησιακής ανθεκτικότητας, τηρώντας παράλληλα τις διατάξεις του, ούτε όσον αφορά τις υπηρεσίες που προσφέρουν ή τις υπηρεσίες που προσφέρονται από τρίτους παρόχους υπηρεσιών ΤΠΕ.

(15) Παράλληλα με τη νομοθεσία για τις χρηματοπιστωτικές υπηρεσίες, η οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[7] αποτελεί το ισχύον γενικό πλαίσιο για την κυβερνοασφάλεια σε επίπεδο Ένωσης. Μεταξύ των επτά κρίσιμων τομέων, η εν λόγω οδηγία εφαρμόζεται επίσης σε τρεις τύπους χρηματοπιστωτικών οντοτήτων, και συγκεκριμένα στα πιστωτικά ιδρύματα, στους τόπους διαπραγμάτευσης και στους κεντρικούς αντισυμβαλλομένους. Ωστόσο, δεδομένου ότι η οδηγία (ΕΕ) 2016/1148 θεσπίζει μηχανισμό προσδιορισμού, σε εθνικό επίπεδο, των φορέων εκμετάλλευσης βασικών υπηρεσιών, μόνο ορισμένα πιστωτικά ιδρύματα, τόποι διαπραγμάτευσης και κεντρικοί αντισυμβαλλόμενοι που προσδιορίζονται από τα κράτη μέλη εμπίπτουν στην πράξη στο πεδίο εφαρμογής της και, ως εκ τούτου, υποχρεούνται να συμμορφώνονται με τις απαιτήσεις σχετικά με την ασφάλεια ΤΠΕ και την κοινοποίηση συμβάντων που προβλέπονται σε αυτήν.

(16) Λαμβανομένου υπόψη ότι ο παρών κανονισμός αυξάνει το επίπεδο εναρμόνισης των 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 χρηματοπιστωτικές υπηρεσίες, διασφαλίζεται επίσης αυξημένη εναρμόνιση σε σύγκριση με τις απαιτήσεις που καθορίζονται στην οδηγία (ΕΕ) 2016/1148. Συνεπώς, για τις χρηματοπιστωτικές οντότητες, ο παρών κανονισμός συνιστά lex specialis σε σχέση με την οδηγία (ΕΕ) 2016/1148.

Είναι καίριας σημασίας να διατηρηθεί ισχυρή σχέση μεταξύ του χρηματοπιστωτικού τομέα και του οριζόντιου πλαισίου της Ένωσης για την κυβερνοασφάλεια, ώστε να διασφαλιστεί η συνοχή με τις στρατηγικές κυβερνοασφάλειας που έχουν θεσπίσει ήδη τα κράτη μέλη και να εξασφαλιστεί η δυνατότητα ενημέρωσης των αρχών χρηματοπιστωτικής εποπτείας για κυβερνοπεριστατικά τα οποία έχουν αντίκτυπο σε άλλους τομείς που καλύπτονται από την οδηγία (ΕΕ) 2016/1148.

(17) Προκειμένου να καταστεί δυνατή η διατομεακή διαδικασία άντλησης διδαγμάτων και αποτελεσματικής αξιοποίησης των εμπειριών από άλλους τομείς όσον αφορά την αντιμετώπιση κυβερνοαπειλών, οι χρηματοπιστωτικές οντότητες που αναφέρονται στην οδηγία (ΕΕ) 2016/1148 θα πρέπει να εξακολουθήσουν να αποτελούν μέρος του «οικοσυστήματος» της εν λόγω οδηγίας [π.χ. ομάδα συνεργασίας για την ασφάλεια συστημάτων δικτύου και πληροφοριών (NIS) και ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT)].

Οι ΕΕΑ και οι εθνικές αρμόδιες αρχές, αντίστοιχα, θα πρέπει να είναι σε θέση να συμμετέχουν στις συζητήσεις στρατηγικής πολιτικής και στις τεχνικές εργασίες της ομάδας συνεργασίας NIS, αντίστοιχα, να ανταλλάσσουν πληροφορίες και να

[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).

συνεργάζονται περαιτέρω με τα ενιαία κέντρα επαφής που ορίζονται βάσει της οδηγίας (ΕΕ) 2016/1148. ***Το όργανο κοινής εποπτείας, οι κύριοι εποπτικοί φορείς και*** οι αρμόδιες αρχές δυνάμει του παρόντος κανονισμού θα πρέπει επίσης να διαβουλεύονται και να συνεργάζονται με τις εθνικές CSIRT που ορίζονται σύμφωνα με το άρθρο 9 της οδηγίας (ΕΕ) 2016/1148.

Επιπλέον, ο παρών κανονισμός θα πρέπει να διασφαλίζει ότι θα παρέχονται στο δίκτυο των CSIRT που θεσπίστηκε με την οδηγία (ΕΕ) 2016/1148 οι λεπτομέρειες των σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ.

(18) Είναι επίσης σημαντικό να διασφαλιστεί η συνοχή ***τόσο*** με την οδηγία για τις ευρωπαϊκές υποδομές ζωτικής σημασίας (ECI), η οποία αποτελεί επί του παρόντος αντικείμενο επανεξέτασης, ώστε να βελτιωθεί η προστασία και η ανθεκτικότητα των υποδομών ζωτικής σημασίας έναντι κυβερνοαπειλών***, όσο και με την οδηγία σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων***[8], με πιθανές επιπτώσεις για τον χρηματοοικονομικό τομέα.31

(19) Οι πάροχοι υπηρεσιών υπολογιστικού νέφους αποτελούν μια κατηγορία παρόχων ψηφιακών υπηρεσιών που καλύπτονται από την οδηγία (ΕΕ) 2016/1148. Ως εκ τούτου, υπόκεινται σε εκ των υστέρων εποπτεία που ασκείται από τις εθνικές αρχές που ορίζονται σύμφωνα με την εν λόγω οδηγία, η οποία περιορίζεται στις απαιτήσεις σχετικά με την ασφάλεια ΤΠΕ και την κοινοποίηση συμβάντων που προβλέπονται στη συγκεκριμένη πράξη. Δεδομένου ότι το 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 χρηματοπιστωτικές οντότητες, το πλαίσιο αυτό θα πρέπει να θεωρείται συμπληρωματικό της εποπτείας που ασκείται δυνάμει της οδηγίας (ΕΕ) 2016/1148 ***και τόσο οι ουσιαστικές όσο και οι διαδικαστικές απαιτήσεις που ισχύουν για τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ βάσει του παρόντος κανονισμού θα πρέπει να είναι συνεκτικές και απρόσκοπτες με εκείνες που ισχύουν βάσει της εν λόγω οδηγίας***. Επιπλέον, το πλαίσιο εποπτείας που θεσπίζεται με τον παρόντα κανονισμό θα πρέπει να καλύπτει τους παρόχους υπηρεσιών υπολογιστικού νέφους ελλείψει ενωσιακού οριζόντιου πλαισίου, ανεξαρτήτως του τομέα, για τη σύσταση αρχής ψηφιακής εποπτείας.

(20) Προκειμένου οι χρηματοπιστωτικές οντότητες να εξακολουθούν να ελέγχουν πλήρως τους κινδύνους ΤΠΕ, πρέπει να διαθέτουν ολοκληρωμένες ικανότητες που να επιτρέπουν την αυστηρή και αποτελεσματική διαχείριση κινδύνων ΤΠΕ, παράλληλα με ειδικούς μηχανισμούς και πολιτικές για την αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ, τις δοκιμές συστημάτων ΤΠΕ, τους σχετικούς ελέγχους και τις διαδικασίες, καθώς και για τη διαχείριση του κινδύνου τρίτων παρόχων ΤΠΕ ***και των κινδύνων ΤΠΕ σε ενδοομιλικό επίπεδο***. Το επίπεδο ψηφιακής επιχειρησιακής ανθεκτικότητας του χρηματοπιστωτικού συστήματος θα πρέπει να αυξηθεί, επιτρέποντας παράλληλα την αναλογική εφαρμογή των απαιτήσεων ***λαμβάνοντας υπόψη τη φύση, την κλίμακα, την πολυπλοκότητα και το συνολικό προφίλ κινδύνου τους***.

---

[8] Οδηγία 2008/114/ΕΚ του Συμβουλίου, της 8ης Δεκεμβρίου 2008, σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους (ΕΕ L 345 της 23.12.2008, σ. 75).

(21) Τα κατώτατα όρια και οι ταξινομήσεις αναφοράς συμβάντων 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)[9] και η ομάδα συνεργασίας NIS για τις χρηματοπιστωτικές οντότητες δυνάμει της οδηγίας (ΕΕ) 2016/1148, όσον αφορά τα κατώτατα όρια και τις ταξινομήσεις εξακολουθούν να υπάρχουν αποκλίνουσες προσεγγίσεις ή μπορεί να προκύψουν για τις υπόλοιπες χρηματοπιστωτικές οντότητες. Η κατάσταση αυτή συνεπάγεται πολλαπλές απαιτήσεις τις οποίες πρέπει να τηρούν οι χρηματοπιστωτικές οντότητες, ιδίως όταν δραστηριοποιούνται σε διάφορες δικαιοδοσίες της Ένωσης και όταν ανήκουν σε χρηματοπιστωτικό όμιλο. Επιπλέον, οι αποκλίσεις αυτές ενδέχεται να παρεμποδίζουν τη δημιουργία περαιτέρω ενιαίων ή κεντρικών μηχανισμών της Ένωσης για την επιτάχυνση της διαδικασίας υποβολής εκθέσεων 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.

(21α) Προκειμένου να μειωθεί ο διοικητικός φόρτος και να αποφευχθούν η πολυπλοκότητα και η διπλή αναφορά για τους παρόχους υπηρεσιών πληρωμών που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού, οι απαιτήσεις αναφοράς συμβάντων βάσει της οδηγίας (ΕΕ) 2015/2366 θα πρέπει να παύσουν να ισχύουν. Ως εκ τούτου, τα πιστωτικά ιδρύματα, τα ιδρύματα ηλεκτρονικού χρήματος και τα ιδρύματα πληρωμών θα πρέπει να αναφέρουν, βάσει του παρόντος κανονισμού, όλα τα επιχειρησιακά ή σχετικά με πληρωμές και μη σχετικά με πληρωμές συμβάντα ασφαλείας που αναφέρονταν προηγουμένως βάσει της οδηγίας (ΕΕ) 2015/2366, ανεξάρτητα από το εάν τα συμβάντα σχετίζονται με τις ΤΠΕ ή όχι.

(22) Προκειμένου οι αρμόδιες αρχές να είναι σε θέση να επιτελούν τους εποπτικούς τους ρόλους, διαμορφώνοντας 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, είναι απαραίτητο να θεσπιστούν κανόνες για ***την επίτευξη ενός ισχυρού*** καθεστώτος αναφοράς συμβάντων που σχετίζονται με τις ΤΠΕ με απαιτήσεις που ***καλύπτουν τα κενά στην τομεακή νομοθεσία για τις χρηματοπιστωτικές υπηρεσίες***, καθώς και να εξαλειφθούν τυχόν υφιστάμενες αλληλεπικαλύψεις και επαναλήψεις για την ελάφρυνση του κόστους. Επομένως, είναι σημαντικό να διασφαλιστεί η εναρμόνιση του καθεστώτος αναφοράς συμβάντων που σχετίζονται με τις ΤΠΕ με την επιβολή της υποχρέωσης σε όλες τις χρηματοπιστωτικές 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 στοιχεία αναφοράς συμβάντων που σχετίζονται με ΤΠΕ, όπως η ταξινόμηση, τα χρονοδιαγράμματα, τα σύνολα δεδομένων, τα υποδείγματα και τα εφαρμοστέα κατώτατα όρια.

(23) Σε ορισμένους υποτομείς του χρηματοπιστωτικού τομέα έχουν αναπτυχθεί απαιτήσεις

[9] ENISA Reference Incident Classification Taxonomy, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας στο πλαίσιο διαφόρων και ***ενίοτε*** μη συντονισμένων εθνικών πλαισίων για την αντιμετώπιση των ίδιων ζητημάτων με διαφορετικό τρόπο. Η κατάσταση αυτή συνεπάγεται αλληλεπικάλυψη του κόστους για τις διασυνοριακές χρηματοπιστωτικές οντότητες και ***θα μπορούσε να παρεμποδίσει*** την αμοιβαία αναγνώριση των αποτελεσμάτων. Ως εκ τούτου, οι μη συντονισμένες δοκιμές μπορούν να κατακερματίσουν την ενιαία αγορά.

(24) Επιπλέον, όταν δεν απαιτούνται δοκιμές, οι ευπάθειες εξακολουθούν να μην εντοπίζονται, γεγονός που θέτει σε μεγαλύτερο κίνδυνο τη χρηματοπιστωτική οντότητα και, εντέλει, τη σταθερότητα και την ακεραιότητα του χρηματοπιστωτικού τομέα. Χωρίς την παρέμβαση της Ένωσης, οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας θα εξακολουθήσουν να είναι ανομοιογενείς και δεν θα υπάρχει αμοιβαία αναγνώριση των αποτελεσμάτων των δοκιμών σε διάφορες δικαιοδοσίες. Επίσης, λαμβανομένου υπόψη ότι είναι απίθανο άλλοι χρηματοπιστωτικοί υποτομείς να υιοθετήσουν συστήματα αυτού του είδους σε ουσιαστική κλίμακα, θα χάσουν τα δυνητικά οφέλη, όπως η αποκάλυψη ευπαθειών και κινδύνων, οι δοκιμές ικανοτήτων άμυνας και συνέχισης των δραστηριοτήτων, καθώς και η αυξημένη εμπιστοσύνη των πελατών, των προμηθευτών και των επιχειρηματικών εταίρων. Για τη διόρθωση αλληλεπικαλύψεων, αποκλίσεων και κενών αυτού του είδους, είναι απαραίτητο να θεσπιστούν κανόνες με στόχο τον συντονισμό των δοκιμών από τις χρηματοπιστωτικές οντότητες και τις αρμόδιες αρχές, διευκολύνοντας με τον τρόπο αυτόν την αμοιβαία αναγνώριση των προηγμένων δοκιμών για σημαντικές χρηματοπιστωτικές οντότητες.

(25) Η στήριξη των χρηματοπιστωτικών οντοτήτων στις υπηρεσίες 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 τελευταία έτη, με αποτέλεσμα τη μείωση του κόστους της χρηματοπιστωτικής διαμεσολάβησης, την εξασφάλιση της δυνατότητας επέκτασης των επιχειρήσεων και κλιμάκωσης όσον αφορά την ανάπτυξη χρηματοπιστωτικών δραστηριοτήτων, ενώ προσφέρεται παράλληλα ευρύ φάσμα εργαλείων ΤΠΕ για τη διαχείριση πολύπλοκων εσωτερικών διαδικασιών.

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

(27) Παρά το γεγονός ότι σε ορισμένες νομοθετικές πράξεις της Ένωσης για τις

χρηματοπιστωτικές υπηρεσίες προβλέπονται ορισμένοι γενικοί κανόνες σχετικά με την εξωτερική ανάθεση, η παρακολούθηση της συμβατικής διάστασης δεν θεμελιώνεται πλήρως στη νομοθεσία της Ένωσης. Ελλείψει της εφαρμογής σαφών και εξειδικευμένων ενωσιακών προτύπων στις συμβατικές ρυθμίσεις που συνάπτονται με τρίτους παρόχους υπηρεσιών ΤΠΕ, η εξωτερική πηγή κινδύνου 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 χρηματοπιστωτικές οντότητες, οι οποίες θα συνοδεύονται από ένα σύνολο βασικών συμβατικών δικαιωμάτων σε σχέση με διάφορα στοιχεία της εκτέλεσης και της καταγγελίας των συμβάσεων, με σκοπό την κατοχύρωση ορισμένων ελάχιστων διασφαλίσεων που θα στηρίζουν την ικανότητα των χρηματοπιστωτικών οντοτήτων να παρακολουθούν αποτελεσματικά όλους τους κινδύνους που προκύπτουν σε επίπεδο τρίτων παρόχων ΤΠΕ.

(28) Διαπιστώνεται έλλειψη ομοιογένειας και σύγκλισης όσον αφορά τον κίνδυνο τρίτων παρόχων ΤΠΕ και τις εξαρτήσεις από τρίτους παρόχους ΤΠΕ. Παρά την καταβολή ορισμένων προσπαθειών για την αντιμετώπιση του συγκεκριμένου τομέα εξωτερικής ανάθεσης, όπως οι συστάσεις του 2017 για την εξωτερική ανάθεση σε παρόχους υπηρεσιών υπολογιστικού νέφους[10], το ζήτημα του συστημικού κινδύνου που ενδέχεται να προκύψει από την έκθεση του χρηματοπιστωτικού τομέα σε περιορισμένο αριθμό κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ εξετάζεται ελάχιστα στην ενωσιακή νομοθεσία. Η έλλειψη αυτή σε επίπεδο Ένωσης επιδεινώνεται από την απουσία ειδικών εντολών και εργαλείων που να επιτρέπουν στις εθνικές εποπτικές αρχές να κατανοούν δεόντως τις εξαρτήσεις από τρίτους παρόχους ΤΠΕ και να παρακολουθούν επαρκώς τους κινδύνους που προκύπτουν λόγω της συγκέντρωσης εξαρτήσεων από τρίτους παρόχους ΤΠΕ αυτού του είδους.

(29) Λαμβανομένων υπόψη των δυνητικών συστημικών κινδύνων που συνεπάγεται η αύξηση των πρακτικών εξωτερικής ανάθεσης και η συγκέντρωση τρίτων παρόχων ΤΠΕ, και έχοντας επίγνωση της ανεπάρκειας εθνικών μηχανισμών που να παρέχουν στις ιεραρχικά ανώτερες χρηματοπιστωτικές οντότητες τη δυνατότητα ποσοτικού προσδιορισμού, χαρακτηρισμού και αποκατάστασης των επιπτώσεων των κινδύνων ΤΠΕ που αφορούν κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, είναι απαραίτητο να θεσπιστεί κατάλληλο ενωσιακό πλαίσιο εποπτείας, το οποίο θα επιτρέπει τη διαρκή παρακολούθηση των δραστηριοτήτων τρίτων παρόχων υπηρεσιών ΤΠΕ που ***παρέχουν κρίσιμες υπηρεσίες σε χρηματοπιστωτικές οντότητες***. ***Δεδομένου ότι η ενδοομιλική παροχή υπηρεσιών ΤΠΕ δεν ενέχει τους ίδιους κινδύνους, οι πάροχοι υπηρεσιών ΤΠΕ που ανήκουν στον ίδιο όμιλο ή στο ίδιο θεσμικό σύστημα προστασίας δεν θα πρέπει να οριστούν ως κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ.***

(30) Καθώς οι απειλές ΤΠΕ καθίστανται ολοένα και πιο πολύπλοκες και εξελιγμένες, η λήψη άρτιων μέτρων εντοπισμού και πρόληψης εξαρτώνται σε μεγάλο βαθμό από την τακτική ανταλλαγή πληροφοριών και στοιχείων σχετικά με απειλές και ευπάθειες μεταξύ των χρηματοπιστωτικών οντοτήτων. Η ανταλλαγή πληροφοριών συμβάλλει στην αύξηση της ευαισθητοποίησης σχετικά με τις κυβερνοαπειλές, η οποία ενισχύει με τη σειρά της την ικανότητα των χρηματοπιστωτικών οντοτήτων να αποτρέπουν τη

[10] Συστάσεις για την εξωτερική ανάθεση σε παρόχους υπηρεσιών υπολογιστικού νέφους (EBA/REC/2017/03), οι οποίες έχουν πλέον καταργηθεί από τις κατευθυντήριες γραμμές της ΕΒΑ σχετικά με την εξωτερική ανάθεση δραστηριοτήτων (EBA/GL/2019/02).

μετατροπή απειλών σε πραγματικά συμβάντα, ενώ παρέχει επίσης στις χρηματοπιστωτικές οντότητες τη δυνατότητα να περιορίζουν καλύτερα τις επιπτώσεις των συμβάντων που σχετίζονται με τις ΤΠΕ και να ανακάμπτουν με αποτελεσματικότερο τρόπο. 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. ***Είναι επομένως σημαντικό να ενισχυθούν οι ρυθμίσεις συνεργασίας και η αναφορά μεταξύ χρηματοπιστωτικών οντοτήτων και αρμόδιων αρχών, καθώς και η ανταλλαγή πληροφοριών με το κοινό, με σκοπό να αναπτυχθεί ένα ανοικτό πλαίσιο ανταλλαγής πληροφοριών και η προσέγγιση της «ασφάλειας βάσει σχεδιασμού», τα οποία είναι απαραίτητα προκειμένου να αυξηθεί η επιχειρησιακή ανθεκτικότητα και ετοιμότητα του χρηματοπιστωτικού τομέα έναντι των κινδύνων ΤΠΕ. Οι ρυθμίσεις ανταλλαγής πληροφοριών θα πρέπει πάντα να λαμβάνουν δεόντως υπόψη τους πιθανούς κινδύνους που σχετίζονται με την κυβερνοασφάλεια, την προστασία των δεδομένων ή το εμπορικό απόρρητο.***

(31) Επιπροσθέτως, οι επιφυλάξεις 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. Η έκταση και η ποιότητα της ανταλλαγής πληροφοριών παραμένει περιορισμένη, 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 χρηματοπιστωτικού τομέα. ***Ως εκ τούτου, είναι σημαντικό να ενισχυθούν οι εν λόγω δίαυλοι επικοινωνίας και να υπάρξει συμβολή από μη εποπτικές αρχές, όταν είναι αναγκαίο και σκόπιμο, καθ' όλη τη διάρκεια του εποπτικού κύκλου.***

(32) ***Επίσης***, οι χρηματοπιστωτικές οντότητες θα πρέπει να ενθαρρύνονται 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. 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 τη χρηματοπιστωτική κοινότητα 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 χρηματοπιστωτικούς διαύλους. Οι εν λόγω μηχανισμοί θα πρέπει να εφαρμόζονται τηρουμένων πλήρως των ισχυόντων κανόνων του δικαίου του ανταγωνισμού της Ένωσης[11], καθώς και κατά τρόπο που να εγγυάται την πλήρη τήρηση των κανόνων της Ένωσης για την προστασία των δεδομένων, κυρίως του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[12], ιδίως στο πλαίσιο

[11] Ανακοίνωση της Επιτροπής – Κατευθυντήριες γραμμές για την εφαρμογή του άρθρου 101 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης στις συμφωνίες οριζόντιας συνεργασίας (ΕΕ C 11 της 14.1.2011, σ. 1).

[12] 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

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.

(33) Παρά την ευρεία κάλυψη που επιδιώκεται με τον παρόντα κανονισμό, η εφαρμογή των κανόνων για την ψηφιακή επιχειρησιακή ανθεκτικότητα***, συμπεριλαμβανομένων των απαιτήσεων του πλαισίου διαχείρισης κινδύνων,*** θα πρέπει να λαμβάνει υπόψη τις σημαντικές διαφορές μεταξύ των χρηματοπιστωτικών οντοτήτων όσον αφορά το μέγεθος, ***τη φύση, την πολυπλοκότητα και το προφίλ κινδύνου***. Ως γενική αρχή, κατά τη διοχέτευση πόρων και ικανοτήτων στην εφαρμογή του πλαισίου διαχείρισης κινδύνων ΤΠΕ, οι χρηματοπιστωτικές οντότητες θα πρέπει να εξισορροπούν δεόντως τις σχετικές με τις ΤΠΕ ανάγκες τους με το μέγεθος***, τη φύση, την πολυπλοκότητα,*** το επιχειρηματικό προφίλ τους ***και το προφίλ σχετικού κινδύνου που διατρέχουν***, ενώ οι αρμόδιες αρχές θα πρέπει να συνεχίσουν να αξιολογούν και να επανεξετάζουν την προσέγγιση της εν λόγω κατανομής.

(34) Δεδομένου ότι οι μεγαλύτερες χρηματοπιστωτικές οντότητες ενδέχεται να διαθέτουν ευρύτερους πόρους και να μπορούν να κινητοποιούν άμεσα κεφάλαια για την ανάπτυξη δομών διακυβέρνησης και τη χάραξη διαφόρων εταιρικών στρατηγικών, μόνο οι χρηματοπιστωτικές 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 τους τρεις άξονες του μοντέλου άμυνας ή για την έκδοση εγγράφου ανθρώπινων πόρων, στο οποίο επεξηγούνται διεξοδικά οι πολιτικές σχετικά με τα δικαιώματα πρόσβασης.

Στο ίδιο πνεύμα, μόνο οι εν λόγω χρηματοπιστωτικές οντότητες θα πρέπει να καλούνται να διενεργούν εις βάθος αξιολογήσεις μετά από σημαντικές αλλαγές στις υποδομές και στις διαδικασίες των συστημάτων δικτύου και πληροφοριών, να προβαίνουν ανά τακτά χρονικά διαστήματα σε αναλύσεις κινδύνου για τα ήδη υφιστάμενα συστήματα ΤΠΕ ή να επεκτείνουν τις δοκιμές αδιάλειπτης λειτουργίας και τα σχέδια αντιμετώπισης και αποκατάστασης, ώστε να σχεδιάζουν σενάρια μετάβασης μεταξύ της κύριας υποδομής ΤΠΕ και των εφεδρικών εγκαταστάσεων.

(35) Επιπλέον, δεδομένου ότι μόνο οι χρηματοπιστωτικές οντότητες που χαρακτηρίζονται ως σημαντικές για τους σκοπούς των προηγμένων δοκιμών ψηφιακής ανθεκτικότητας θα πρέπει να υποχρεούνται να διενεργούν δοκιμές διείσδυσης βάσει απειλών, οι διοικητικές διαδικασίες και το οικονομικό κόστος που συνεπάγεται η διενέργεια των δοκιμών αυτών θα πρέπει να βαρύνουν μικρό ποσοστό των χρηματοπιστωτικών οντοτήτων. Τέλος, για τους σκοπούς της μείωσης των κανονιστικών επιβαρύνσεων, θα πρέπει να ζητείται από τις χρηματοπιστωτικές οντότητες, εκτός των πολύ μικρών επιχειρήσεων, να υποβάλλουν τακτικά στις αρμόδιες αρχές τα στοιχεία όλων των ***εκτιμώμενων*** δαπανών και ζημιών που προκαλούνται από ***σημαντικές*** διαταραχές των ΤΠΕ***, σημαντικά συμβάντα που σχετίζονται με τις ΤΠΕ*** καθώς και τα αποτελέσματα επανεξέτασης μετά από συμβάντα που επέρχονται λόγω ***παρόμοιων*** διαταραχών των

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).

ΤΠΕ.

(36) Για τους σκοπούς της διασφάλισης της πλήρους ευθυγράμμισης και της συνολικής συνοχής μεταξύ των επιχειρηματικών στρατηγικών των χρηματοπιστωτικών οντοτήτων, αφενός, και της άσκησης της διαχείρισης κινδύνων ΤΠΕ, αφετέρου, το διοικητικό όργανο θα πρέπει να υποχρεούται να επιτελεί καίριο και ενεργό ρόλο στον προσανατολισμό και στην προσαρμογή του πλαισίου διαχείρισης κινδύνων ΤΠΕ, καθώς και της συνολικής στρατηγικής για την ψηφιακή ανθεκτικότητα. Η προσέγγιση που πρέπει να υιοθετεί το διοικητικό όργανο 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 χρηματοπιστωτικής οντότητας θα πρέπει να αποτελεί γενική αρχή αυτής της ολοκληρωμένης προσέγγισης, η οποία θα μετουσιώνεται περαιτέρω στη διαρκή συμμετοχή του διοικητικού οργάνου στον έλεγχο της παρακολούθησης της διαχείρισης κινδύνων ΤΠΕ.

(37) Επιπλέον, η πλήρης λογοδοσία του διοικητικού οργάνου συμβαδίζει με την εξασφάλιση ενός επιπέδου επενδύσεων ΤΠΕ, καθώς και του συνολικού προϋπολογισμού, ώστε η χρηματοπιστωτική οντότητα να είναι σε θέση να επιτύχει τον βασικό στόχο της ως προς την ψηφιακή επιχειρησιακή ανθεκτικότητα.

(38) Βάσει σχετικών διεθνών, εθνικών και κλαδικών προτύπων, κατευθυντήριων γραμμών, συστάσεων ή προσεγγίσεων για τη διαχείριση των κινδύνων στον κυβερνοχώρο[13], ο παρών κανονισμός προάγει μια σειρά λειτουργιών που διευκολύνουν τη συνολική διάρθρωση της διαχείρισης κινδύνων ΤΠΕ. Στον βαθμό που οι κύριες ικανότητες που διαθέτουν οι χρηματοπιστωτικές οντότητες ανταποκρίνονται στις ανάγκες των προβλεπόμενων στόχων στο πλαίσιο των λειτουργιών (προσδιορισμός, προστασία και πρόληψη, εντοπισμός, αντιμετώπιση και αποκατάσταση, μάθηση και εξέλιξη και επικοινωνία) που καθορίζονται στον παρόντα κανονισμό, οι χρηματοπιστωτικές οντότητες εξακολουθούν να έχουν τη διακριτική ευχέρεια να χρησιμοποιούν μοντέλα διαχείρισης κινδύνων ΤΠΕ τα οποία πλαισιώνονται ή κατηγοριοποιούνται με διαφορετικό τρόπο.

(39) Προκειμένου να συμβαδίζουν με το εξελισσόμενο τοπίο των κυβερνοαπειλών, οι χρηματοπιστωτικές οντότητες θα πρέπει να διατηρούν επικαιροποιημένα συστήματα ΤΠΕ, τα οποία είναι αξιόπιστα και διαθέτουν επαρκή χωρητικότητα, για να

---

13 CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures* (Οδηγίες για την κυβερνοανθεκτικότητα των υποδομών χρηματοπιστωτικών αγορών), https://www.bis.org/cpmi/publ/d146.pdf G7, *Fundamental Elements of Cybersecurity for the Financial Sector* (Θεμελιώδη στοιχεία της κυβερνοασφάλειας για τον χρηματοπιστωτικό τομέα), https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf· NIST Cybersecurity Framework, https://www.nist.gov/cyberframework· FSB *CIRR toolkit*, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document

εξασφαλιστεί όχι μόνο η επεξεργασία δεδομένων που είναι απαραίτητη για την εκτέλεση των υπηρεσιών τους, αλλά και η τεχνολογική ανθεκτικότητα που επιτρέπει στις χρηματοπιστωτικές οντότητες να ανταποκρίνονται δεόντως στις πρόσθετες ανάγκες επεξεργασίας που ενδέχεται να προκληθούν από ακραίες συνθήκες της αγοράς ή άλλες αντίξοες καταστάσεις. Μολονότι ο παρών κανονισμός δεν συνεπάγεται τυποποίηση συγκεκριμένων συστημάτων, εργαλείων ή τεχνολογιών ΤΠΕ, βασίζεται στην κατάλληλη χρήση, εκ μέρους των χρηματοπιστωτικών οντοτήτων, ευρωπαϊκών και διεθνώς αναγνωρισμένων τεχνικών προτύπων (π.χ. ISO) ή βέλτιστων πρακτικών του κλάδου, υπό την προϋπόθεση ότι η χρήση αυτή συμμορφώνεται πλήρως με συγκεκριμένες εποπτικές οδηγίες σχετικά με τη χρήση και την ενσωμάτωση διεθνών προτύπων.

(40) Απαιτούνται αποτελεσματικά σχέδια αδιάλειπτης λειτουργίας και αποκατάστασης λειτουργίας ώστε οι χρηματοπιστωτικές 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 αποκατάστασης***, συνεκτιμώντας εάν πρόκειται για κρίσιμη ή σημαντική λειτουργία***. Ωστόσο, τα συστήματα εφεδρείας θα πρέπει να ξεκινούν την επεξεργασία χωρίς αδικαιολόγητη καθυστέρηση, ενώ η έναρξη της επεξεργασίας αυτού του είδους δεν θα πρέπει σε καμία περίπτωση να θέτει σε κίνδυνο την ακεραιότητα και την ασφάλεια των συστημάτων δικτύου και πληροφοριών ή τον εμπιστευτικό χαρακτήρα των δεδομένων.

(41) Μολονότι ο παρών κανονισμός παρέχει στις χρηματοπιστωτικές οντότητες τη δυνατότητα να καθορίζουν στόχους για τον χρόνο αποκατάστασης με ευέλικτο τρόπο και, κατ' επέκταση, να θέτουν τέτοιους στόχους λαμβάνοντας πλήρως υπόψη τη φύση και την κρισιμότητα της σχετικής λειτουργίας, καθώς και τυχόν ειδικών επιχειρηματικών αναγκών, θα πρέπει κατά τον καθορισμό των εν λόγω στόχων να απαιτείται επίσης αξιολόγηση των συνολικών δυνητικών επιπτώσεων στην αποτελεσματικότητα της αγοράς.

(42) Οι σημαντικές συνέπειες των κυβερνοεπιθέσεων αυξάνονται όταν συμβαίνουν στον χρηματοπιστωτικό τομέα, έναν τομέα που κινδυνεύει πολύ περισσότερο να αποτελέσει στόχο κακόβουλων χρηστών που επιδιώκουν οικονομικά οφέλη απευθείας στην πηγή. Για τον μετριασμό των κινδύνων αυτών και για να προληφθεί η απώλεια της ακεραιότητας ή της διαθεσιμότητας των συστημάτων ΤΠΕ ή η παραβίαση εμπιστευτικών δεδομένων ή η πρόκληση βλάβης στην υποδομή ΤΠΕ, η αναφορά σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ από τις χρηματοπιστωτικές οντότητες θα πρέπει να βελτιωθεί σημαντικά.

Η αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ θα πρέπει να εναρμονιστεί για όλες τις χρηματοπιστωτικές οντότητες, με την επιβολή της υποχρέωσης στις χρηματοπιστωτικές οντότητες να αναφέρουν συμβάντα μόνο στις οικείες αρμόδιες αρχές. Παρότι όλες οι χρηματοπιστωτικές οντότητες θα υπόκεινται σε αυτή την υποχρέωση αναφοράς συμβάντων, δεν θα πρέπει να επηρεάζονται όλες με τον ίδιο τρόπο, δεδομένου ότι τα σχετικά κατώτατα όρια σημαντικότητας και χρονοδιαγράμματα θα πρέπει να διαμορφώνονται καταλλήλως ώστε να αποτυπώνουν μόνο σημαντικά συμβάντα που σχετίζονται με τις ΤΠΕ. Η άμεση αναφορά συμβάντων θα παρέχει στις αρχές χρηματοπιστωτικής εποπτείας τη δυνατότητα πρόσβασης σε

πληροφορίες για συμβάντα που σχετίζονται με τις ΤΠΕ. Ωστόσο, οι αρχές χρηματοπιστωτικής εποπτείας θα πρέπει να διαβιβάζουν τις πληροφορίες αυτές σε μη χρηματοπιστωτικές δημόσιες αρχές (αρμόδιες αρχές NIS, εθνικές αρχές προστασίας δεδομένων και αρχές επιβολής του νόμου για συμβάντα ποινικού χαρακτήρα). Η διοχέτευση πληροφοριών για συμβάντα που σχετίζονται με τις ΤΠΕ θα πρέπει να είναι αμοιβαία: οι αρχές χρηματοπιστωτικής εποπτείας θα πρέπει να παρέχουν στη χρηματοπιστωτική οντότητα κάθε αναγκαία ανατροφοδότηση ή καθοδήγηση, ενώ οι ΕΕΑ θα πρέπει να ανταλλάσσουν ανωνυμοποιημένα δεδομένα σχετικά με απειλές και ευπάθειες που σχετίζονται με ένα γεγονός, με σκοπό την ενίσχυση της ευρύτερης συλλογικής άμυνας.

(43) Θα πρέπει να διερευνηθεί περαιτέρω η δυνατότητα συγκέντρωσης των αναφορών συμβάντων που σχετίζονται με τις ΤΠΕ, μέσω ενός ενιαίου κεντρικού κόμβου της ΕΕ ***για την αναφορά σημαντικών 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 εκθέσεων που διαβιβάζονται από τις εθνικές αρμόδιες αρχές και την άσκηση συντονιστικού ρόλου. Θα πρέπει να ζητηθεί από τις ΕΕΑ να εκπονήσουν, σε διαβούλευση με την ΕΚΤ και τον ENISA, και εντός καθορισμένης προθεσμίας, κοινή έκθεση στην οποία θα διερευνάται η σκοπιμότητα της δημιουργίας ενός τέτοιου κεντρικού κόμβου της ΕΕ.

(44) Για τους σκοπούς της διασφάλισης ισχυρής ψηφιακής επιχειρησιακής ανθεκτικότητας, και σύμφωνα με τα διεθνή πρότυπα (π.χ. τα θεμελιώδη στοιχεία της G7 για τις δοκιμές διείσδυσης βάσει απειλών), οι χρηματοπιστωτικές οντότητες***, πλην των πολύ μικρών επιχειρήσεων,*** θα πρέπει να υποβάλλουν τακτικά σε δοκιμή τα οικεία συστήματα ΤΠΕ και το προσωπικό τους ως προς την αποτελεσματικότητα των ικανοτήτων τους όσον αφορά την πρόληψη, τον εντοπισμό, την αντιμετώπιση και την αποκατάσταση, ώστε να αποκαλύπτουν και να αντιμετωπίζουν πιθανές ευπάθειες των ΤΠΕ. Για την αντιμετώπιση των διαφορών τόσο μεταξύ όσο και εντός των χρηματοπιστωτικών υποτομέων όσον αφορά την ετοιμότητα των χρηματοπιστωτικών 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 φυσικής ασφάλειας, λύσεις λογισμικού ερωτηματολογίων και σάρωσης, επανεξετάσεις κωδίκων πηγής, όπου αυτό είναι εφικτό, δοκιμές βάσει σεναρίων, δοκιμές συμβατότητας, δοκιμές επιδόσεων ή διατερματικές δοκιμές) έως πιο προηγμένες δοκιμές (π.χ. δοκιμές διείσδυσης βάσει απειλών για τις χρηματοπιστωτικές οντότητες που παρουσιάζουν επαρκή βαθμό ωριμότητας από πλευράς ΤΠΕ ώστε να είναι σε θέση να διεξάγουν δοκιμές αυτού του είδους). Συνεπώς, οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας θα πρέπει να είναι πιο απαιτητικές για σημαντικές χρηματοπιστωτικές οντότητες (όπως μεγάλα πιστωτικά ιδρύματα, χρηματιστήρια, κεντρικά αποθετήρια τίτλων, κεντρικοί αντισυμβαλλόμενοι κ.λπ.). Από την άλλη πλευρά, οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας θα πρέπει να είναι επίσης περισσότερο σημαντικές για ορισμένους υποτομείς που διαδραματίζουν βασικό συστημικό ρόλο (π.χ. πληρωμές, τράπεζες, εκκαθάριση και διακανονισμός) και λιγότερο σημαντικές για άλλους υποτομείς (π.χ. διαχειριστές περιουσιακών στοιχείων, οργανισμοί αξιολόγησης της πιστοληπτικής ικανότητας κ.λπ.). Οι διασυνοριακές χρηματοπιστωτικές οντότητες που ασκούν το δικαίωμα ελεύθερης εγκατάστασης ή παροχής υπηρεσιών εντός της Ένωσης θα πρέπει

να συμμορφώνονται με ένα ενιαίο σύνολο απαιτήσεων προηγμένων δοκιμών (π.χ. δοκιμή διείσδυσης βάσει απειλών) στο κράτος μέλος προέλευσής τους, και η σχετική δοκιμή θα πρέπει να περιλαμβάνει τις υποδομές ΤΠΕ σε όλες τις δικαιοδοσίες στις οποίες δραστηριοποιείται ο διασυνοριακός όμιλος εντός της Ένωσης, ώστε να διασφαλίζεται ότι οι διασυνοριακοί όμιλοι επιβαρύνονται με το κόστος δοκιμών μόνο σε μία δικαιοδοσία. ***Επιπλέον, προκειμένου να ενισχυθεί η συνεργασία με αξιόπιστες τρίτες χώρες στον τομέα της ανθεκτικότητας των χρηματοπιστωτικών οντοτήτων, η Επιτροπή και οι αρμόδιες αρχές θα πρέπει να επιδιώξουν να δημιουργήσουν ένα πλαίσιο για την αμοιβαία αναγνώριση των αποτελεσμάτων των δοκιμών διείσδυσης βάσει απειλών (TLPT).***

Τα κράτη μέλη θα πρέπει να ορίσουν μια ενιαία δημόσια αρχή υπεύθυνη για τις TLPT στον χρηματοπιστωτικό τομέα σε εθνικό επίπεδο. Η ενιαία δημόσια αρχή θα μπορούσε, μεταξύ άλλων, να είναι εθνική αρμόδια αρχή ή δημόσια αρχή που ορίζεται σύμφωνα με το άρθρο 8 της οδηγίας (ΕΕ) 2016/1148 (ΑΔΠ). Η ενιαία δημόσια αρχή θα πρέπει να είναι υπεύθυνη για την έκδοση βεβαιώσεων ότι η TLPT πραγματοποιήθηκε σύμφωνα με τις απαιτήσεις. Οι βεβαιώσεις αυτές θα πρέπει να διευκολύνουν την αμοιβαία αναγνώριση των δοκιμών μεταξύ των αρμόδιων αρχών.

Ορισμένες χρηματοπιστωτικές οντότητες έχουν την ικανότητα να διενεργούν εσωτερικές προηγμένες δοκιμές, ενώ άλλες θα συνάπτουν συμβάσεις με εξωτερικούς φορείς δοκιμών από το εσωτερικό της Ένωσης ή από τρίτη χώρα. Ως εκ τούτου, είναι σημαντικό όλοι οι φορείς δοκιμών να υπόκεινται στις ίδιες σαφείς απαιτήσεις. Προκειμένου να διασφαλιστεί η ανεξαρτησία των εσωτερικών φορέων δοκιμών, η χρήση τους θα πρέπει να υπόκειται στην έγκριση της αρμόδιας αρχής.

Η μεθοδολογία για την TLPT δεν θα πρέπει να είναι υποχρεωτική, αλλά η χρήση του υφιστάμενου πλαισίου TIBER-EU θα πρέπει να θεωρείται ότι συμμορφώνεται με τις απαιτήσεις της TLPT στον παρόντα κανονισμό.

Μέχρι την έναρξη ισχύος του παρόντος κανονισμού, και την εκπόνηση και έγκριση, από τις ΕΕΑ, των ανατεθέντων ρυθμιστικών τεχνικών προτύπων όσον αφορά την TLPT, οι χρηματοπιστωτικές οντότητες θα πρέπει να ακολουθούν τις σχετικές κατευθυντήριες γραμμές και τα πλαίσια στην Ένωση που ισχύουν για τις δοκιμές διείσδυσης βάσει στοιχείων, όπως αυτά θα συνεχίσουν να ισχύουν όταν τεθεί σε ισχύ ο παρών κανονισμός.

(44α) Η ευθύνη για τη διεξαγωγή της TLPT – και για τη διαχείριση της κυβερνοασφάλειας εν γένει και την πρόληψη κυβερνοεπιθέσεων – θα πρέπει να παραμείνει πλήρως στη χρηματοπιστωτική οντότητα, οι δε βεβαιώσεις που παρέχονται από τις αρχές θα πρέπει να αποσκοπούν αποκλειστικά στον σκοπό της αμοιβαίας αναγνώρισης και δεν θα πρέπει να αποκλείουν τυχόν επακόλουθες ενέργειες στο επίπεδο του κινδύνου ΤΠΕ στον οποίο είναι εκτεθειμένη η χρηματοπιστωτική οντότητα, ούτε να θεωρούνται ως έγκριση των ικανοτήτων της όσον αφορά τη διαχείριση και τον μετριασμό των κινδύνων ΤΠΕ.

(45) Για τους σκοπούς της διασφάλισης της ορθής παρακολούθησης του κινδύνου τρίτων παρόχων ΤΠΕ, είναι απαραίτητη η θέσπιση ενός συνόλου κανόνων βάσει αρχών, ώστε να παρέχεται στις χρηματοπιστωτικές οντότητες καθοδήγηση σχετικά με την

παρακολούθηση του κινδύνου που προκύπτει στο πλαίσιο των λειτουργιών που αποτελούν αντικείμενο εξωτερικής ανάθεσης σε τρίτους παρόχους υπηρεσιών ΤΠΕ***, ιδίως όσον αφορά την παροχή κρίσιμων ή σημαντικών λειτουργιών από τρίτους παρόχους υπηρεσιών ΤΠΕ*** και, γενικότερα, στο πλαίσιο των εξαρτήσεων από τρίτους παρόχους ΤΠΕ.

(46) Οι χρηματοπιστωτικές οντότητες θα πρέπει να φέρουν ανά πάσα στιγμή την πλήρη ευθύνη για τη συμμόρφωση με τις υποχρεώσεις που απορρέουν από τον παρόντα κανονισμό. Είναι σκόπιμο να οργανωθεί η αναλογική παρακολούθηση του κινδύνου που προκύπτει σε επίπεδο τρίτου παρόχου υπηρεσιών ΤΠΕ, λαμβανομένης δεόντως υπόψη ***της φύσης,*** της κλίμακας, της πολυπλοκότητας και της σημασίας των εξαρτήσεων 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 χρηματοπιστωτικών υπηρεσιών σε μεμονωμένο επίπεδο και σε επίπεδο ομίλου, ανάλογα με την περίπτωση***, καθώς και κατά πόσον οι υπηρεσίες ΤΠΕ παρέχονται από ενδοομιλικό ή από τρίτο πάροχο υπηρεσιών***.

(47) Για την άσκηση καθηκόντων παρακολούθησης αυτού του είδους θα πρέπει να ακολουθείται μια στρατηγική προσέγγιση ως προς τον κίνδυνο τρίτων παρόχων ΤΠΕ, η οποία θα επισημοποιείται μέσω της υιοθέτησης, από το διοικητικό όργανο της χρηματοοικονομικής οντότητας, ειδικής στρατηγικής που θα βασίζεται στον διαρκή έλεγχο όλων αυτών 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 του πλαισίου εποπτείας που θεσπίζεται με τον παρόντα κανονισμό, οι αρχές χρηματοπιστωτικής εποπτείας θα πρέπει να λαμβάνουν τακτικά σημαντικές πληροφορίες από τα μητρώα και θα πρέπει να είναι σε θέση να ζητούν αποσπάσματα από τα μητρώα αυτά σε ad hoc βάση.

(48) Η διενέργεια εμπεριστατωμένης προσυμβασιακής ανάλυσης θα πρέπει να στηρίζει την επίσημη σύναψη συμβατικών ρυθμίσεων και να προηγείται αυτής, ενώ ***θα πρέπει να λαμβάνονται διορθωτικά μέτρα και μέτρα αποκατάστασης, τα οποία μπορεί να περιλαμβάνουν μερική ή ολική*** καταγγελία των συμβάσεων ***στην περίπτωση τουλάχιστον ενός συνόλου*** περιστάσεων που καταδεικνύουν ελλείψεις στον τρίτο πάροχο υπηρεσιών ΤΠΕ.

(49) Για την αντιμετώπιση των συστημικών επιπτώσεων του κινδύνου συγκέντρωσης τρίτων παρόχων ΤΠΕ, θα πρέπει να προαχθεί μια ισορροπημένη λύση μέσω της υιοθέτησης ευέλικτης και σταδιακής προσέγγισης, δεδομένου ότι τα αυστηρά ανώτατα όρια ή οι αυστηροί περιορισμοί ενδέχεται να προβάλλουν προσκόμματα στην επιχειρηματική συμπεριφορά και στη συμβατική ελευθερία. Οι χρηματοπιστωτικές οντότητες θα πρέπει να αξιολογούν ενδελεχώς τις συμβατικές ρυθμίσεις για τον προσδιορισμό της πιθανότητας εμφάνισης κινδύνου αυτού του είδους, μεταξύ άλλων μέσω εμπεριστατωμένων αναλύσεων των ρυθμίσεων υπεργολαβίας ▌. Στο παρόν στάδιο, και για τους σκοπούς της επίτευξης δίκαιης ισορροπίας μεταξύ της επιτακτικής ανάγκης διατήρησης της συμβατικής ελευθερίας και της ανάγκης διασφάλισης της χρηματοπιστωτικής σταθερότητας, δεν κρίνεται σκόπιμο να προβλεφθούν αυστηρά ανώτατα όρια και περιορισμοί όσον αφορά την έκθεση σε κινδύνους τρίτων παρόχων ΤΠΕ. ***Το όργανο κοινής εποπτείας που ασκεί*** την εποπτεία για κάθε κρίσιμο τρίτο

πάροχο ΤΠΕ ***και η ΕΕΑ που έχει οριστεί να ασκεί καθημερινή εποπτεία*** (στο εξής: κύριος εποπτικός φορέας) θα πρέπει να δίνει ιδιαίτερη προσοχή, κατά την άσκηση των καθηκόντων εποπτείας, στην πλήρη κατανόηση της έκτασης των αλληλεξαρτήσεων και 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 χρηματοπιστωτικού συστήματος της Ένωσης, ενώ θα πρέπει να προβλέπει, αντιθέτως, τη διεξαγωγή διαλόγου με κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ όταν εντοπίζεται ο κίνδυνος αυτός[14].

(50) Προκειμένου να είναι δυνατή η αξιολόγηση και η παρακολούθηση σε τακτική βάση της ικανότητας του τρίτου παρόχου υπηρεσιών ΤΠΕ να παρέχει με ασφάλεια υπηρεσίες στη χρηματοπιστωτική οντότητα, χωρίς αρνητικές επιπτώσεις στην ανθεκτικότητα της οντότητας, θα πρέπει να διασφαλίζεται η εναρμόνιση των βασικών συμβατικών στοιχείων καθ' όλη τη διάρκεια της εκτέλεσης των συμβάσεων με τρίτους παρόχους ΤΠΕ. Τα στοιχεία αυτά καλύπτουν μόνο τις ελάχιστες συμβατικές πτυχές που θεωρούνται καίριας σημασίας για την εξασφάλιση της δυνατότητας στήριξης της πλήρους παρακολούθησης εκ μέρους της χρηματοπιστωτικής οντότητας, από την άποψη της διασφάλισης της ψηφιακής ανθεκτικότητάς της, στη σταθερότητα και στην ασφάλεια της υπηρεσίας ΤΠΕ.

(51) 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 υποβάλλονται σε επεξεργασία, καθώς και πλήρη περιγραφή του επιπέδου εξυπηρέτησης, συνοδευόμενη από ποσοτικούς και ποιοτικούς στόχους επιδόσεων εντός των συμφωνηθέντων επιπέδων εξυπηρέτησης, ώστε να εξασφαλίζεται η δυνατότητα αποτελεσματικής παρακολούθησης εκ μέρους της χρηματοπιστωτικής οντότητας. Στο ίδιο πνεύμα, οι διατάξεις σχετικά με την προσβασιμότητα, τη διαθεσιμότητα, την ακεραιότητα, την ασφάλεια και την προστασία των δεδομένων προσωπικού χαρακτήρα, καθώς και οι εγγυήσεις για την πρόσβαση, την ανάκτηση και την επιστροφή σε περίπτωση αφερεγγυότητας, εξυγίανσης, διακοπής των επιχειρηματικών δραστηριοτήτων του τρίτου παρόχου υπηρεσιών ΤΠΕ ***ή τερματισμού των συμβατικών ρυθμίσεων*** θα πρέπει επίσης να θεωρούνται ουσιώδη στοιχεία για την ικανότητα μιας χρηματοοικονομικής οντότητας να διασφαλίζει την παρακολούθηση του κινδύνου τρίτων.

(52) Προκειμένου να διασφαλιστεί ότι οι χρηματοπιστωτικές οντότητες διατηρούν τον πλήρη έλεγχο όλων των εξελίξεων που ενδέχεται να υπονομεύσουν την ασφάλεια των οικείων ΤΠΕ, θα πρέπει να καθοριστούν περίοδοι προειδοποίησης και υποχρεώσεις υποβολής εκθέσεων για τον τρίτο πάροχο υπηρεσιών ΤΠΕ σε περίπτωση εξελίξεων με δυνητικές σημαντικές επιπτώσεις στην ικανότητα του τρίτου παρόχου υπηρεσιών ΤΠΕ να εκτελεί με αποτελεσματικό τρόπο κρίσιμες ή σημαντικές λειτουργίες, συμπεριλαμβανομένης της παροχής συνδρομής εκ μέρους του σε περίπτωση συμβάντος που σχετίζεται με τις ΤΠΕ ***αναφορικά με τις υπηρεσίες που παρέχονται από τον τρίτο πάροχο υπηρεσιών ΤΠΕ στη χρηματοπιστωτική οντότητα στα συμφωνημένα***

[14] Επιπλέον, σε περίπτωση που προκύψει κίνδυνος κατάχρησης από τρίτο πάροχο υπηρεσιών ΤΠΕ που θεωρείται ότι κατέχει δεσπόζουσα θέση, οι χρηματοπιστωτικές οντότητες θα πρέπει να έχουν επίσης τη δυνατότητα υποβολής είτε επίσημης είτε ανεπίσημης καταγγελίας στην Ευρωπαϊκή Επιτροπή ή στις εθνικές αρχές που είναι αρμόδιες για το δίκαιο του ανταγωνισμού.

επίπεδα εξυπηρέτησης χωρίς πρόσθετο κόστος ή με κόστος που καθορίζεται εκ των προτέρων. ***Οι δευτερεύουσες υπηρεσίες ΤΠΕ από τις οποίες οι χρηματοοικονομικές οντότητες δεν εξαρτώνται λειτουργικά δεν καλύπτονται από τον παρόντα κανονισμό***.

Επιπλέον, ο ορισμός της «κρίσιμης ή σημαντικής λειτουργίας» που προβλέπεται στον παρόντα κανονισμό θα πρέπει να 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, της 15ης Μαΐου 2014*[15]. Ως εκ τούτου, λειτουργίες που είναι κρίσιμες λειτουργίες σύμφωνα με την οδηγία (ΕΕ) 2014/59 θα πρέπει να είναι κρίσιμες ή σημαντικές λειτουργίες κατά την έννοια του παρόντος κανονισμού.***

(53) ***Σε περίπτωση συμβατικών ρυθμίσεων για κρίσιμες ή σημαντικές λειτουργίες,*** τα δικαιώματα πρόσβασης, επιθεώρησης και ελέγχου από τη χρηματοπιστωτική οντότητα ή διορισμένο τρίτο αποτελούν μέσα καίριας σημασίας για τη συνεχή παρακολούθηση των επιδόσεων του τρίτου παρόχου υπηρεσιών ΤΠΕ από τις χρηματοπιστωτικές οντότητες, σε συνδυασμό με την πλήρη συνεργασία του τελευταίου κατά τη διάρκεια των επιθεωρήσεων. Στο ίδιο πνεύμα, ***το όργανο κοινής εποπτείας και ο κύριος εποπτικός φορέας*** της χρηματοπιστωτικής οντότητας θα πρέπει να έχουν τη δυνατότητα να ασκούν, βάσει προειδοποιήσεων, τα εν λόγω δικαιώματα επιθεώρησης και ελέγχου του τρίτου παρόχου υπηρεσιών ΤΠΕ, με την επιφύλαξη της τήρησης του απορρήτου ***και επιδεικνύοντας παράλληλα προσοχή ώστε να μην διαταράσσονται οι υπηρεσίες που παρέχονται σε άλλους πελάτες του τρίτου παρόχου υπηρεσιών ΤΠΕ***. ***Η χρηματοπιστωτική οντότητα και ο τρίτος πάροχος υπηρεσιών ΤΠΕ θα πρέπει να είναι σε θέση να συμφωνήσουν ότι τα δικαιώματα πρόσβασης, επιθεώρησης και ελέγχου μπορούν να ανατεθούν σε ανεξάρτητο τρίτο***.

(54) Οι συμβατικές ρυθμίσεις θα πρέπει να προβλέπουν σαφή δικαιώματα καταγγελίας και σχετικές ελάχιστες κοινοποιήσεις, καθώς και ειδικές στρατηγικές εξόδου που θα παρέχουν, ιδίως, τη δυνατότητα καθορισμού υποχρεωτικών μεταβατικών περιόδων, κατά τη διάρκεια των οποίων οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ θα πρέπει να εξακολουθούν να παρέχουν τις σχετικές λειτουργίες με στόχο τη μείωση του κινδύνου διαταραχών στο επίπεδο της χρηματοπιστωτικής οντότητας ή την εξασφάλιση της δυνατότητας της χρηματοπιστωτικής οντότητας να αλλάξει τρίτο πάροχο υπηρεσιών ΤΠΕ ή να καταφύγει, εναλλακτικά, στη χρήση λύσεων εντός ***της επιχείρησης***, ανάλογα με την πολυπλοκότητα της παρεχόμενης υπηρεσίας. ***Επιπλέον, τα πιστωτικά ιδρύματα θα πρέπει να διασφαλίζουν ότι οι σχετικές συμβάσεις ΤΠΕ είναι ισχυρές και πλήρως εκτελεστές σε περίπτωση εξυγίανσης του πιστωτικού ιδρύματος. Σύμφωνα με τις προσδοκίες των αρχών εξυγίανσης, τα πιστωτικά ιδρύματα θα πρέπει να διασφαλίζουν ότι οι σχετικές συμβάσεις για υπηρεσίες ΤΠΕ είναι ανθεκτικές στην εξυγίανση. Όσο συνεχίζουν να εκτελούνται κρίσιμες ή σημαντικές λειτουργίες ΤΠΕ,***

---

15 ***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).***

οι εν λόγω χρηματοπιστωτικές οντότητες θα πρέπει να διασφαλίζουν ότι οι συμβάσεις περιέχουν, μεταξύ άλλων απαιτήσεων, ρήτρες μη καταγγελίας, αναστολής και τροποποίησης για λόγους αναδιάρθρωσης ή εξυγίανσης.

(55) Επιπλέον, η προαιρετική χρήση τυποποιημένων συμβατικών ρητρών που έχει αναπτύξει η Επιτροπή για τις υπηρεσίες υπολογιστικού νέφους μπορεί να εξυπηρετεί ακόμη περισσότερο τις χρηματοπιστωτικές οντότητες και τους οικείους τρίτους παρόχους υπηρεσιών ΤΠΕ, με την ενίσχυση του επιπέδου ασφάλειας δικαίου όσον αφορά τη χρήση υπηρεσιών υπολογιστικού νέφους από τον χρηματοπιστωτικό τομέα, σε πλήρη εναρμόνιση με τις απαιτήσεις και τις προσδοκίες που προβλέπονται στον κανονισμό για τις χρηματοπιστωτικές υπηρεσίες. Οι εργασίες αυτές 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 χρηματοπιστωτικές οντότητες, με βάση τις διατομεακές προσπάθειες των ενδιαφερόμενων στον τομέα του υπολογιστικού νέφους που έχουν ήδη διευκολυνθεί από την Επιτροπή με την εξασφάλιση της συμμετοχής του χρηματοπιστωτικού τομέα.

(55α) Οι ΕΕΑ θα πρέπει να έχουν την εντολή να καταρτίζουν εκτελεστικά τεχνικά και ρυθμιστικά πρότυπα που να διευκρινίζουν τις προσδοκίες πολιτικής όσον αφορά τη διαχείριση του κινδύνου τρίτων παρόχων ΤΠΕ και τις συμβατικές απαιτήσεις. Μέχρι την έναρξη ισχύος των εν λόγω προτύπων, οι χρηματοπιστωτικές οντότητες θα πρέπει να ακολουθούν τις σχετικές κατευθυντήριες γραμμές και άλλα μέτρα που εκδίδουν οι ΕΕΑ και οι αρμόδιες αρχές.

(56) Για τους σκοπούς της προώθησης της σύγκλισης και της αποτελεσματικότητας σε σχέση με τις εποπτικές προσεγγίσεις όσον αφορά τον κίνδυνο τρίτων παρόχων ΤΠΕ για τον χρηματοπιστωτικό τομέα, την ενίσχυση της ψηφιακής επιχειρησιακής ανθεκτικότητας των χρηματοπιστωτικών οντοτήτων που βασίζονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ για την εκτέλεση επιχειρησιακών λειτουργιών και, κατ' επέκταση, τη συμβολή στη διατήρηση της σταθερότητας του χρηματοπιστωτικού συστήματος της Ένωσης και της ακεραιότητας της ενιαίας αγοράς χρηματοπιστωτικών υπηρεσιών, οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ θα πρέπει να υπόκεινται σε ενωσιακό πλαίσιο εποπτείας.

(57) Δεδομένου ότι η ειδική μεταχείριση δικαιολογείται μόνο για κρίσιμους τρίτους παρόχους υπηρεσιών, θα πρέπει να θεσπιστεί μηχανισμός ορισμού για τους σκοπούς της εφαρμογής του πλαισίου εποπτείας της Ένωσης, ώστε να λαμβάνεται υπόψη η διάσταση και ο χαρακτήρας της εξάρτησης του χρηματοπιστωτικού τομέα από τους εν λόγω τρίτους παρόχους υπηρεσιών ΤΠΕ, ο οποίος θα περιλαμβάνει ένα σύνολο ποσοτικών και ποιοτικών κριτηρίων που θα καθορίζουν τις παραμέτρους κρισιμότητας ως βάση για την υπαγωγή τους στο πλαίσιο εποπτείας. Οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που δεν ορίζονται αυτομάτως δυνάμει της εφαρμογής των προαναφερόμενων κριτηρίων θα πρέπει να έχουν τη δυνατότητα προαιρετικής συμμετοχής στο πλαίσιο εποπτείας, ενώ οι τρίτοι πάροχοι ΤΠΕ που υπόκεινται ήδη σε πλαίσια μηχανισμών εποπτείας που ***στηρίζουν την εκπλήρωση των καθηκόντων*** σε επίπεδο Ευρωσυστήματος ***όπως*** αναφέρονται στο άρθρο 127 παράγραφος 2 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης θα πρέπει, συνεπώς, να

εξαιρούνται. ***Ομοίως, οι επιχειρήσεις που ανήκουν σε χρηματοπιστωτικό όμιλο και παρέχουν υπηρεσίες ΤΠΕ αποκλειστικά σε χρηματοπιστωτικές οντότητες εντός του ίδιου χρηματοπιστωτικού ομίλου δεν θα πρέπει να υπόκεινται στον μηχανισμό προκειμένου να οριστούν ως κρίσιμες.***

(58) Η απαίτηση νομικής ενσωμάτωσης στην Ένωση τρίτων παρόχων υπηρεσιών ΤΠΕ που έχουν οριστεί ως κρίσιμοι δεν ισοδυναμεί με γεωγραφικό περιορισμό δεδομένων, διότι ο παρών κανονισμός δεν συνεπάγεται τη θέσπιση περαιτέρω απαιτήσεων σχετικά με την αποθήκευση ή την επεξεργασία δεδομένων στην Ένωση. ***Η απαίτηση ύπαρξης επιχείρησης, όπως μια θυγατρική που έχει συσταθεί στην Ένωση δυνάμει του δικαίου κράτους μέλους, έχει ως στόχο να εξασφαλίσει ότι θα υπάρχει ένα σημείο επαφής μεταξύ του τρίτου παρόχου υπηρεσιών ΤΠΕ, αφενός, και του κύριου εποπτικού φορέα και του οργάνου κοινής εποπτείας, αφετέρου, και να εξασφαλίσουν ότι ο κύριος εποπτικός φορέας και το όργανο κοινής εποπτείας θα είναι σε θέση να εκτελούν τα καθήκοντά τους και να ασκούν τις εξουσίες εποπτείας και επιβολής που προβλέπονται στον παρόντα κανονισμό***. ***Οι συμβατικές υπηρεσίες του τρίτου παρόχου υπηρεσιών ΤΠΕ δεν χρειάζεται να παρέχονται από την οντότητά του στην Ένωση.***

(58α) Λόγω του σημαντικού αντίκτυπου που θα μπορούσε να έχει στους τρίτους παρόχους υπηρεσιών ΤΠΕ ο ορισμός τους ως κρίσιμων, θα πρέπει να θεσπιστούν δικαιώματα προηγούμενης ακρόασης ως υποχρέωση που επιβάλλεται στις ΕΕΑ και στο όργανο κοινής εποπτείας να λαμβάνουν δεόντως υπόψη τυχόν πρόσθετες πληροφορίες που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ κατά τη διάρκεια της διαδικασίας ορισμού.

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

(60) Για την αξιοποίηση της υφιστάμενης πολυεπίπεδης θεσμικής αρχιτεκτονικής στον τομέα των χρηματοπιστωτικών υπηρεσιών, η μεικτή επιτροπή των ΕΕΑ θα πρέπει να συνεχίσει να διασφαλίζει τον συνολικό διατομεακό συντονισμό σε σχέση με όλα τα θέματα που αφορούν τον κίνδυνο ΤΠΕ, σύμφωνα με τα καθήκοντά της για την κυβερνοασφάλεια, ***μέσω του νεοσυσταθέντος οργάνου κοινής εποπτείας εκδίδοντας*** τόσο ▌μεμονωμένες αποφάσεις που απευθύνονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ όσο και ▌συλλογικές συστάσεις, ιδίως όσον αφορά τη συγκριτική αξιολόγηση των προγραμμάτων εποπτείας κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ και τον προσδιορισμό βέλτιστων πρακτικών για την αντιμετώπιση ζητημάτων συγκέντρωσης ΤΠΕ.

(61) Προκειμένου να διασφαλιστεί ότι οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που διαδραματίζουν κρίσιμο ρόλο στη λειτουργία του χρηματοπιστωτικού τομέα τελούν υπό αναλογική εποπτεία σε ενωσιακή κλίμακα, ***πρέπει να συσταθεί το όργανο κοινής εποπτείας προκειμένου να ασκεί άμεση εποπτεία των κρίσιμων τρίτων παρόχων*** υπηρεσιών ΤΠΕ. ***Επιπλέον,*** μία από τις ΕΕΑ θα πρέπει να οριστεί ως κύριος εποπτικός φορέας για κάθε κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ ***για τη διεξαγωγή και τον συντονισμό της καθημερινής εποπτείας και του ερευνητικού έργου, προκειμένου να***

ενεργεί ως ενιαίο σημείο επαφής και να διασφαλίζει τη συνέχεια. Το όργανο κοινής εποπτείας και ο κύριος εποπτικός φορέας θα πρέπει να εργάζονται απρόσκοπτα για να εξασφαλίζουν αποτελεσματική καθημερινή εποπτεία, καθώς και ολιστική προσέγγιση όσον αφορά τη λήψη αποφάσεων και τις συστάσεις.

(62) Οι κύριοι εποπτικοί φορείς θα πρέπει να διαθέτουν τις απαραίτητες εξουσίες για τη διεξαγωγή ερευνών, επιτόπιων επιθεωρήσεων σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, την πρόσβαση σε όλες τις σχετικές εγκαταστάσεις και τοποθεσίες και την απόκτηση πλήρων και επικαιροποιημένων πληροφοριών, ώστε να τους παρέχεται η δυνατότητα να διαμορφώνουν πραγματική εικόνα ως προς το είδος, τη διάσταση και τον αντίκτυπο του κινδύνου τρίτων παρόχων ΤΠΕ για τις χρηματοπιστωτικές οντότητες και, εντέλει, για το χρηματοπιστωτικό σύστημα της Ένωσης.

(62α) Η ανάθεση της ***άμεσης*** εποπτείας ***στον κύριο εποπτικό φορέα*** συνιστά προϋπόθεση για την κατανόηση και την αντιμετώπιση της συστημικής διάστασης του κινδύνου ΤΠΕ στον χρηματοοικονομικό τομέα. Το ενωσιακό αποτύπωμα των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ και τα δυνητικά ζητήματα του κινδύνου συγκέντρωσης ΤΠΕ που συνδέονται με αυτό απαιτούν την υιοθέτηση συλλογικής προσέγγισης σε επίπεδο Ένωσης. Η άσκηση πολλαπλών δικαιωμάτων ελέγχου και πρόσβασης από πολλές αρμόδιες αρχές χωριστά, με ελάχιστο ή μηδενικό συντονισμό, δεν θα οδηγούσε σε πλήρη επισκόπηση του κινδύνου τρίτων παρόχων ΤΠΕ, ενώ θα δημιουργούσε παράλληλα περιττούς πλεονασμούς, επιβαρύνσεις και πολυπλοκότητα στο επίπεδο των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ που βρίσκονται αντιμέτωποι με τόσο μεγάλο αριθμό αιτημάτων.

(63) ***Ο κύριος εποπτικός φορέας*** θα πρέπει να είναι σε θέση να ***εκδίδει*** συστάσεις σχετικά με θέματα κινδύνων ΤΠΕ και κατάλληλα διορθωτικά μέτρα, μεταξύ άλλων να ***εναντιώνεται*** σε ορισμένες συμβατικές ρυθμίσεις που έχουν εντέλει αντίκτυπο στη σταθερότητα της χρηματοπιστωτικής οντότητας ή του χρηματοπιστωτικού συστήματος. Η συμμόρφωση με τέτοιου είδους ουσιαστικές συστάσεις που διατυπώνονται από ***τον κύριο εποπτικό φορέα*** θα πρέπει να λαμβάνεται δεόντως υπόψη από τις εθνικές αρμόδιες αρχές στο πλαίσιο των καθηκόντων τους που αφορούν την προληπτική εποπτεία των χρηματοπιστωτικών οντοτήτων. ***Πριν από την οριστικοποίηση των εν λόγω συστάσεων, οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ θα πρέπει να έχουν την ευκαιρία να παρέχουν πληροφορίες οι οποίες πιστεύουν εύλογα ότι θα πρέπει να ληφθούν υπόψη πριν από την οριστικοποίηση και την έκδοση της σύστασης.***

(63α) Προκειμένου να αποφευχθούν αλληλεπικαλύψεις και αντιφάσεις σε σχέση με τα τεχνικά και οργανωσιακά μέτρα που ενδέχεται να ισχύουν για κρίσιμους τρίτους παρόχους υπηρεσιών, οι κύριοι εποπτικοί φορείς και το όργανο κοινής εποπτείας θα πρέπει να λαμβάνουν δεόντως υπόψη το πλαίσιο που θεσπίστηκε με την οδηγία (ΕΕ) 2016/1148 κατά την άσκηση των εξουσιών τους σύμφωνα με στο πλαίσιο εποπτείας του παρόντος κανονισμού. Πριν ασκήσουν τις εν λόγω εξουσίες, το όργανο κοινής εποπτείας και ο κύριος εποπτικός φορέας θα πρέπει να διαβουλεύονται με τις αρμόδιες αρχές που έχουν δικαιοδοσία βάσει της οδηγίας (ΕΕ) 2016/1148.

(64) Το πλαίσιο εποπτείας δεν αντικαθιστά ούτε υποκαθιστά καθ' οιονδήποτε τρόπο και για κανένα μέρος τη διαχείριση, εκ μέρους των χρηματοπιστωτικών οντοτήτων, του

κινδύνου που συνεπάγεται η χρήση τρίτων παρόχων υπηρεσιών ΤΠΕ, συμπεριλαμβανομένης της υποχρέωσης συνεχούς παρακολούθησης των συμβατικών τους ρυθμίσεων που συνάπτονται με κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, ούτε επηρεάζει την πλήρη ευθύνη των χρηματοπιστωτικών οντοτήτων όσον αφορά τη συμμόρφωσή τους με όλες τις απαιτήσεις που περιλαμβάνονται στον παρόντα κανονισμό και στη σχετική νομοθεσία για τις χρηματοπιστωτικές υπηρεσίες, καθώς και την εκπλήρωση αυτών. Για την πρόληψη 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. Κάθε τέτοιο μέτρο θα πρέπει προηγουμένως να αποτελεί αντικείμενο συντονισμού και συμφωνίας βάσει του πλαισίου εποπτείας.

(65) Για την προώθηση της σύγκλισης σε διεθνές επίπεδο όσον αφορά τις βέλτιστες πρακτικές που πρέπει να χρησιμοποιούνται κατά την επανεξέταση της διαχείρισης ψηφιακού κινδύνου των τρίτων παρόχων υπηρεσιών ΤΠΕ, οι ΕΕΑ θα πρέπει να ενθαρρύνονται να συνάπτουν συμφωνίες συνεργασίας με τις σχετικές εποπτικές και ρυθμιστικές αρμόδιες αρχές των τρίτων χωρών, ώστε να διευκολύνεται η ανάπτυξη βέλτιστων πρακτικών για την αντιμετώπιση του κινδύνου τρίτων παρόχων ΤΠΕ.

(66) Για την αξιοποίηση της τεχνικής εμπειρογνωσίας των εμπειρογνωμόνων των αρμόδιων αρχών στη διαχείριση λειτουργικών κινδύνων και κινδύνων ΤΠΕ, οι κύριοι εποπτικοί φορείς***, όταν διενεργούν γενικές έρευνες ή επιτόπιες επιθεωρήσεις,*** θα πρέπει να αξιοποιούν την εθνική εποπτική εμπειρία και να συγκροτούν ειδικές εξεταστικές ομάδες για κάθε επιμέρους κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ, συγκεντρώνοντας διεπιστημονικές ομάδες για την υποστήριξη τόσο της προετοιμασίας όσο και της πραγματικής εκτέλεσης των δραστηριοτήτων εποπτείας, συμπεριλαμβανομένων των επιτόπιων επιθεωρήσεων κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ, καθώς και της απαιτούμενης παρακολούθησής τους.

(67) Οι αρμόδιες αρχές θα πρέπει να διαθέτουν όλες τις εξουσίες εποπτείας, έρευνας και επιβολής κυρώσεων που είναι απαραίτητες για τη διασφάλιση της εφαρμογής του παρόντος κανονισμού. Οι διοικητικές κυρώσεις θα πρέπει, καταρχήν, να δημοσιεύονται. Δεδομένου ότι οι χρηματοπιστωτικές οντότητες και οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ μπορούν να είναι εγκατεστημένοι σε διαφορετικά κράτη μέλη και να τελούν υπό την εποπτεία διαφορετικών αρμόδιων τομεακών αρχών, η 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[16], και η διαβούλευση με τις ΕΕΑ θα πρέπει να διασφαλίζονται μέσω της αμοιβαίας ανταλλαγής πληροφοριών και της παροχής συνδρομής στο πλαίσιο των εποπτικών δραστηριοτήτων. ***Το Ενιαίο Συμβούλιο Εξυγίανσης, μολονότι δεν είναι αρμόδια αρχή για τους σκοπούς του παρόντος κανονισμού, θα πρέπει, ωστόσο, να συμμετέχει στους μηχανισμούς αμοιβαίας ανταλλαγής πληροφοριών για τις οντότητες που εμπίπτουν στο πεδίο εφαρμογής του***

[16] 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).

κανονισμού (ΕΕ) αριθ. 806/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[17].

(68) Για τους σκοπούς του περαιτέρω ποσοτικού και ποιοτικού προσδιορισμού των κριτηρίων για τον ορισμό των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ, καθώς και για τους σκοπούς της εναρμόνισης των τελών εποπτείας, θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία να εκδίδει πράξεις, σύμφωνα με το άρθρο 290 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, όσον αφορά τα εξής: για τον περαιτέρω προσδιορισμό των συστημικών επιπτώσεων που θα μπορούσε να έχει η αθέτηση υποχρεώσεων εκ μέρους τρίτου παρόχου ΤΠΕ στις χρηματοπιστωτικές οντότητες που εξυπηρετεί, στον αριθμό των παγκόσμιων συστημικώς σημαντικών ιδρυμάτων (G-SII) ή άλλων συστημικώς σημαντικών ιδρυμάτων (O-SII) που βασίζονται στον αντίστοιχο τρίτο πάροχο υπηρεσιών ΤΠΕ, στον αριθμό των τρίτων παρόχων υπηρεσιών ΤΠΕ που δραστηριοποιούνται σε συγκεκριμένη αγορά, στο κόστος μετάβασης σε άλλον τρίτο πάροχο υπηρεσιών ΤΠΕ, στον αριθμό των κρατών μελών στα οποία ο αντίστοιχος τρίτος πάροχος υπηρεσιών ΤΠΕ παρέχει υπηρεσίες και στον τρόπο λειτουργίας των χρηματοπιστωτικών οντοτήτων που χρησιμοποιούν τον αντίστοιχο τρίτο πάροχο υπηρεσιών ΤΠΕ, καθώς και στο ύψος των τελών εποπτείας και στον 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[18]. Πιο συγκεκριμένα, προκειμένου να διασφαλιστεί η ίση συμμετοχή στην προετοιμασία των κατ' εξουσιοδότηση πράξεων, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο λαμβάνουν όλα τα έγγραφα κατά τον ίδιο χρόνο με τους εμπειρογνώμονες των κρατών μελών, και οι εμπειρογνώμονές τους έχουν συστηματικά πρόσβαση στις συνεδριάσεις των ομάδων εμπειρογνωμόνων της Επιτροπής που ασχολούνται με την προετοιμασία κατ' εξουσιοδότηση πράξεων.

(69) Δεδομένου ότι ο παρών κανονισμός, σε συνδυασμό με την οδηγία (ΕΕ) 20xx/xx του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[19], συνεπάγεται την ενοποίηση των διατάξεων διαχείρισης κινδύνων ΤΠΕ που περιλαμβάνονται σε μεγάλο αριθμό κανονισμών και οδηγιών του κεκτημένου της Ένωσης στον τομέα των χρηματοπιστωτικών υπηρεσιών, συμπεριλαμβανομένων των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και (ΕΕ) αριθ. 909/2014, και για τους σκοπούς της διασφάλισης πλήρους διαφάνειας, οι εν λόγω κανονισμοί θα πρέπει να τροποποιηθούν ώστε να αποσαφηνιστεί ότι οι συναφείς διατάξεις που σχετίζονται με τους κινδύνους ΤΠΕ καθορίζονται στον παρόντα κανονισμό.

Οι σχετικές κατευθυντήριες γραμμές που εκδίδονται ή που βρίσκονται επί του

---

17 ***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).***

18 ΕΕ L 123 της 12.5.2016, σ. 1.

19 [*Να προστεθεί πλήρης παραπομπή*]

παρόντος υπό επεξεργασία από τις ΕΕΑ για την εφαρμογή αυτών των κανονισμών και οδηγιών θα πρέπει να επανεξεταστούν και να αναθεωρηθούν ως μέρος της διαδικασίας ενοποίησης, έτσι ώστε η νομική βάση για τις απαιτήσεις όσον αφορά τους κινδύνους ΤΠΕ στο δίκαιο της Ένωσης να απορρέει αποκλειστικά από τον παρόντα κανονισμό, τις εκτελεστικές πράξεις και τις αποφάσεις του και τις συστάσεις που εκδίδονται σύμφωνα με αυτές, σχετικά με οντότητες που εμπίπτουν στο πεδίο εφαρμογής του.

(69α) Η συνεκτική εναρμόνιση των απαιτήσεων που καθορίζονται στον παρόντα κανονισμό θα πρέπει να διασφαλίζεται με τεχνικά πρότυπα. Θα πρέπει να ανατεθεί στις ΕΕΑ, ως φορείς υψηλού επιπέδου εξειδικευμένης πείρας, η εντολή 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, των δοκιμών και των βασικών απαιτήσεων για την ορθή παρακολούθηση των κινδύνων τρίτων παρόχων ΤΠΕ. ***Κατά την ανάπτυξη σχεδίων ρυθμιστικών τεχνικών προτύπων, οι ΕΕΑ θα πρέπει να λαμβάνουν δεόντως υπόψη την εντολή τους σε σχέση με τις πτυχές της αναλογικότητας και να ζητούν συμβουλές από τις αντίστοιχες συμβουλευτικές επιτροπές τους για την αναλογικότητα, ιδίως σε σχέση με την εφαρμογή του παρόντος κανονισμού σε ΜΜΕ και εταιρείες μεσαίας κεφαλαιοποίησης.***

(70) Είναι ιδιαίτερα σημαντικό η Επιτροπή να διεξαγάγει κατάλληλες διαβουλεύσεις στο πλαίσιο των προπαρασκευαστικών της εργασιών, τις μεταξύ άλλων σε επίπεδο εμπειρογνωμόνων. Η Επιτροπή και οι ΕΕΑ θα πρέπει να διασφαλίζουν ότι τα εν λόγω πρότυπα και απαιτήσεις μπορούν να εφαρμόζονται από όλες τις χρηματοπιστωτικές οντότητες κατά τρόπο ανάλογο προς τη φύση, το μέγεθος και την πολυπλοκότητα των οντοτήτων αυτών και των δραστηριοτήτων τους.

(71) Προκειμένου να διευκολυνθεί η συγκρισιμότητα των αναφορών σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ και να διασφαλιστεί η διαφάνεια των συμβατικών ρυθμίσεων για τη χρήση των υπηρεσιών ΤΠΕ που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ, θα πρέπει να ανατεθεί στις ΕΕΑ η εντολή να αναπτύσσουν σχέδια εκτελεστικών τεχνικών προτύπων για την κατάρτιση τυποποιημένων υποδειγμάτων, εντύπων και διαδικασιών, ώστε οι χρηματοπιστωτικές οντότητες να είναι σε θέση να αναφέρουν σημαντικά συμβάντα που σχετίζονται με τις ΤΠΕ, καθώς και για την κατάρτιση τυποποιημένων υποδειγμάτων για το μητρώο πληροφοριών. Κατά την ανάπτυξη των προτύπων αυτών, οι ΕΕΑ θα πρέπει να λαμβάνουν υπόψη ***τη φύση,*** το μέγεθος, την πολυπλοκότητα ***και το επιχειρηματικό προφίλ*** των χρηματοπιστωτικών οντοτήτων, καθώς και τη φύση και το επίπεδο κινδύνου των δραστηριοτήτων τους. Θα πρέπει επίσης να ανατεθεί στην Επιτροπή η εξουσία να εγκρίνει τα εν λόγω εκτελεστικά τεχνικά πρότυπα μέσω εκτελεστικών πράξεων δυνάμει του άρθρου 291 της ΣΛΕΕ και του άρθρου 15 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) 1094/2010 και (ΕΕ) αριθ. 1095/2010, αντίστοιχα. 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, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και (ΕΕ) αριθ. 909/2014, αντίστοιχα, 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.

(72) Για τη διαδικασία αυτή θα απαιτηθεί η μεταγενέστερη τροποποίηση των υφιστάμενων κατ' εξουσιοδότηση και εκτελεστικών πράξεων που έχουν εκδοθεί σε διάφορους τομείς της νομοθεσίας για τις χρηματοπιστωτικές υπηρεσίες. Το πεδίο εφαρμογής των άρθρων σχετικά με τον λειτουργικό κίνδυνο, βάσει των οποίων ασκήθηκαν οι εξουσιοδοτήσεις που περιλαμβάνονταν στις εν λόγω πράξεις για την ανάθεση της εντολής έκδοσης κατ' εξουσιοδότηση και εκτελεστικών πράξεων, θα πρέπει να τροποποιηθεί ενόψει της μεταφοράς στον παρόντα κανονισμό όλων των διατάξεων που καλύπτουν την ψηφιακή επιχειρησιακή ανθεκτικότητα και αποτελούν επί του παρόντος μέρος των εν λόγω κανονισμών.

(73) Δεδομένου ότι οι στόχοι του παρόντος κανονισμού, και συγκεκριμένα η διασφάλιση υψηλού επιπέδου ψηφιακής επιχειρησιακής ανθεκτικότητας που θα ισχύει για όλες τις χρηματοπιστωτικές οντότητες, δεν μπορούν να επιτευχθούν επαρκώς από τα κράτη μέλη διότι προϋποθέτουν την εναρμόνιση μεγάλου αριθμού διαφορετικών κανόνων, οι οποίοι περιλαμβάνονται επί του παρόντος είτε σε ορισμένες πράξεις της Ένωσης είτε στα νομικά συστήματα των διαφόρων κρατών μελών, αλλά μπορούν να επιτευχθούν 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, η οποία προβλέπεται στο εν λόγω άρθρο, ο παρών κανονισμός δεν βαίνει πέραν των αναγκαίων ορίων για την επίτευξη του επιδιωκόμενου στόχου.

ΕΞΕΔΩΣΑΝ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

ΚΕΦΑΛΑΙΟ I

ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1

Αντικείμενο

1. Ο παρών κανονισμός καθορίζει τις ακόλουθες ενιαίες απαιτήσεις όσον αφορά την ασφάλεια των συστημάτων δικτύου και πληροφοριών, τα οποία υποστηρίζουν τις επιχειρησιακές διαδικασίες των χρηματοπιστωτικών οντοτήτων, για τη διασφάλιση υψηλού κοινού επιπέδου ψηφιακής επιχειρησιακής ανθεκτικότητας, ως εξής:

α) απαιτήσεις που ισχύουν για τις χρηματοπιστωτικές οντότητες όσον αφορά:

– τη διαχείριση κινδύνων των τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ),

– την αναφορά σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ στις αρμόδιες αρχές,

– ***την αναφορά σημαντικών επιχειρησιακών ή σχετικών με τις πληρωμές συμβάντων ασφαλείας στις αρμόδιες αρχές από τις χρηματοπιστωτικές οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 στοιχεία α) έως γ)·***

– τις δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας·

– την ανταλλαγή πληροφοριών και στοιχείων σχετικά με κυβερνοαπειλές και ευπάθειες·

– τα μέτρα για τη χρηστή διαχείριση ***του κινδύνου τρίτων παρόχων ΤΠΕ*** από τις χρηματοπιστωτικές οντότητες·

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

γ) το πλαίσιο εποπτείας για κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ κατά την παροχή υπηρεσιών σε χρηματοπιστωτικές 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 χρηματοπιστωτικές οντότητες που προσδιορίζονται ως φορείς εκμετάλλευσης βασικών υπηρεσιών σύμφωνα με τους εθνικούς κανόνες για τη μεταφορά του άρθρου 5 της οδηγίας (ΕΕ) 2016/1148 στο εθνικό δίκαιο, ο παρών κανονισμός θεωρείται τομεακή νομική πράξη της Ένωσης για τους σκοπούς του άρθρου 1 παράγραφος 7 της εν λόγω οδηγίας.

2α. Ο παρών κανονισμός δεν θίγει τις αρμοδιότητες των κρατών μελών όσον αφορά τη διατήρηση της δημόσιας ασφάλειας, της άμυνας και της εθνικής ασφάλειας.

Άρθρο 2

Προσωπικό πεδίο εφαρμογής

1. Ο παρών κανονισμός εφαρμόζεται στις ακόλουθες οντότητες:

α) πιστωτικά ιδρύματα,

β) ιδρύματα πληρωμών,

γ) ιδρύματα ηλεκτρονικού χρήματος,

δ) επιχειρήσεις επενδύσεων,

ε) παρόχους υπηρεσιών κρυπτοστοιχείων, εκδότες ***και προσφέροντες*** κρυπτοστοιχείων, εκδότες ***και προσφέροντες*** ψηφιακών κερμάτων με εγγύηση περιουσιακών στοιχείων και εκδότες σημαντικών ψηφιακών κερμάτων με εγγύηση περιουσιακών στοιχείων,

στ) κεντρικά αποθετήρια τίτλων ***και διαχειριστές συστημάτων διακανονισμού τίτλων***,

ζ) κεντρικούς αντισυμβαλλομένους,

η) τόπους διαπραγμάτευσης,

θ) αρχεία καταγραφής συναλλαγών,

ι) διαχειριστές οργανισμών εναλλακτικών επενδύσεων,

ια) εταιρείες διαχείρισης,

ιβ) παρόχους υπηρεσιών αναφοράς δεδομένων,

ιγ) ασφαλιστικές και αντασφαλιστικές επιχειρήσεις,

ιδ) ασφαλιστικούς διαμεσολαβητές, αντασφαλιστικούς διαμεσολαβητές και ασφαλιστικούς διαμεσολαβητές που ασκούν ως δευτερεύουσα δραστηριότητα την ασφαλιστική διαμεσολάβηση***, εκτός εάν είναι πολύ μικρές, μικρές ή μεσαίες επιχειρήσεις που βασίζονται αποκλειστικά σε οργανωμένα αυτοματοποιημένα συστήματα πωλήσεων***,

ιε) ιδρύματα ***για παροχή*** επαγγελματικών ***συντάξεων (IORPs) που δεν εφαρμόζουν συνταξιοδοτικά συστήματα τα οποία από κοινού έχουν λιγότερα από 15 μέλη***,

ιστ) οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας,

ιζ) νόμιμους ελεγκτές και ελεγκτικά γραφεία ***που δεν είναι πολύ μικρές, μικρές ή μεσαίες επιχειρήσεις, εκτός εάν οι εν λόγω πολύ μικρές, μικρές ή μεσαίες επιχειρήσεις παρέχουν ελεγκτικές υπηρεσίες σε οντότητες που απαριθμούνται στο παρόν άρθρο, με εξαίρεση τις πολύ μικρές, μικρές ή μεσαίες επιχειρήσεις που είναι μη κερδοσκοπικές ελεγκτικές οντότητες σύμφωνα με το άρθρο 2 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 537/2014, εκτός εάν η αρμόδια αρχή αποφασίσει ότι η εξαίρεση δεν είναι έγκυρη***,

ιη) διαχειριστές δεικτών αναφοράς κρίσιμης σημασίας,

ιθ) παρόχους υπηρεσιών πληθοχρηματοδότησης,

κ) αρχεία καταγραφής τιτλοποιήσεων,

κα) τρίτους παρόχους υπηρεσιών ΤΠΕ.

1α. Ο παρών κανονισμός, με εξαίρεση το τμήμα ΙΙ του κεφαλαίου V, εφαρμόζεται επίσης σε ενδοομιλικούς παρόχους υπηρεσιών ΤΠΕ.

2. Για τους σκοπούς του παρόντος κανονισμού, οι οντότητες που αναφέρονται στα στοιχεία α) έως κ) αναφέρονται συλλογικά ως «χρηματοπιστωτικές οντότητες».

2α. Για τους σκοπούς του παρόντος κανονισμού, με εξαίρεση το κεφάλαιο V τμήμα II, οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ και οι ενδοομιλικοί πάροχοι υπηρεσιών ΤΠΕ αναφέρονται συλλογικά ως «τρίτοι πάροχοι υπηρεσιών ΤΠΕ».

Άρθρο 3

Ορισμοί

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

(1) «ψηφιακή επιχειρησιακή ανθεκτικότητα»: η ικανότητα μιας χρηματοπιστωτικής οντότητας να διαμορφώνει, να εξασφαλίζει και να επανεξετάζει την επιχειρησιακή της ακεραιότητα ▌διασφαλίζοντας, άμεσα ή έμμεσα, μέσω της χρήσης υπηρεσιών από τρίτους παρόχους ΤΠΕ, ▌ τη συνεχή παροχή χρηματοπιστωτικών υπηρεσιών και την ποιότητά τους ***σε περίπτωση λειτουργικών διαταραχών που επηρεάζουν τις δυνατότητες ΤΠΕ της***·

(2) «σύστημα δικτύου και πληροφοριών»: το σύστημα δικτύου και πληροφοριών όπως ορίζεται στο άρθρο 4 σημείο 1 της οδηγίας (ΕΕ) 2016/1148·

(3) «ασφάλεια συστημάτων δικτύου και πληροφοριών»: η ασφάλεια των συστημάτων δικτύου και πληροφοριών όπως ορίζεται στο άρθρο 4 σημείο 2 της οδηγίας (ΕΕ) 2016/1148·

(4) «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 ***τις ΤΠΕ***, της λειτουργίας και της διεξαγωγής διαδικασιών ή της παροχής υπηρεσιών ▌·

(5) «πληροφοριακοί πόροι»: συλλογή πληροφοριών, ενσώματων ή άυλων, που αξίζουν να προστατευτούν·

(6) «συμβάν που σχετίζεται με τις ΤΠΕ»: απρόβλεπτο ***συμβάν ή σειρά συνδεδεμένων συμβάντων*** που διαπιστώνεται ▌, το οποίο ▌θέτει σε κίνδυνο την ασφάλεια των συστημάτων δικτύου και πληροφοριών, ▌ ή έχει δυσμενείς επιπτώσεις στη διαθεσιμότητα, τον απόρρητο χαρακτήρα, τη συνέχεια***, την ακεραιότητα*** ή τη γνησιότητα των χρηματοπιστωτικών υπηρεσιών που παρέχει η χρηματοπιστωτική οντότητα·

(6α) «επιχειρησιακό συμβάν που σχετίζεται με την ασφάλεια των πληρωμών»: συμβάν ή σειρά συνδεδεμένων περιστατικών που δεν έχουν προβλεφθεί από τις χρηματοπιστωτικές οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 στοιχεία α) έως γ), τα οποία έχουν ή ενδέχεται να έχουν δυσμενείς επιπτώσεις στην ακεραιότητα, τη διαθεσιμότητα, τον απόρρητο χαρακτήρα, την αυθεντικότητα ή τη συνέχεια υπηρεσιών που σχετίζονται με πληρωμές·

(7) «σημαντικό συμβάν που σχετίζεται με τις ΤΠΕ»: συμβάν που σχετίζεται με τις ΤΠΕ που ***έχει ή*** μπορεί να έχει εξαιρετικά δυσμενείς επιπτώσεις στα συστήματα δικτύου και πληροφοριών τα οποία υποστηρίζουν κρίσιμες λειτουργίες της χρηματοπιστωτικής οντότητας·

(7α) «σημαντικό επιχειρησιακό συμβάν ή σχετικό με τις πληρωμές συμβάν ασφαλείας:

επιχειρησιακό συμβάν ή σχετικό με τις πληρωμές συμβάν ασφαλείας, το οποίο πληροί τα κριτήρια που ορίζονται στο άρθρο 16·

(8) «κυβερνοαπειλή»: η κυβερνοαπειλή όπως ορίζεται στο άρθρο 2 σημείο 8 του κανονισμού (ΕΕ) αριθ. 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[20]·

(8α) «σημαντική κυβερνοαπειλή»: κυβερνοαπειλή της οποίας τα χαρακτηριστικά δείχνουν σαφώς ότι είναι πιθανό να οδηγήσει σε σημαντικό συμβάν που σχετίζεται με τις ΤΠΕ·

(9) «κυβερνοεπίθεση»: κακόβουλο συμβάν που σχετίζεται με τις ΤΠΕ μέσω απόπειρας καταστροφής, έκθεσης, μεταβολής, απενεργοποίησης, υποκλοπής ή απόκτησης μη εξουσιοδοτημένης πρόσβασης ή μη εξουσιοδοτημένης χρήσης περιουσιακού στοιχείου, η οποία τελείται από οποιονδήποτε παράγοντα απειλής·

(10) «πληροφορίες για απειλές»: πληροφορίες που έχουν συγκεντρωθεί, μετατραπεί, αναλυθεί, ερμηνευτεί ή εμπλουτιστεί με σκοπό την παροχή του απαραίτητου πλαισίου για τη λήψη αποφάσεων και οι οποίες οδηγούν σε 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·

(11) «άμυνα σε βάθος»: στρατηγική που σχετίζεται με τις ΤΠΕ και περιλαμβάνει άτομα, διαδικασίες και τεχνολογία με σκοπό τη δημιουργία ποικίλων φραγμών σε πολλαπλά επίπεδα και διαστάσεις της οντότητας·

(12) «ευπάθεια»: αδυναμία, ευαισθησία ή ελάττωμα περιουσιακού στοιχείου, συστήματος, διαδικασίας ή ελέγχου που μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης από μια ***κυβερνοαπειλή***·

(13) «δοκιμή διείσδυσης βάσει απειλών»: 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 ζωντανής παραγωγής της οντότητας·

(14) «κίνδυνος τρίτων παρόχων ΤΠΕ»: κίνδυνος ΤΠΕ που μπορεί να προκύψει για χρηματοπιστωτική οντότητα σε σχέση με τη χρήση υπηρεσιών ΤΠΕ που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ ή από άλλους υπεργολάβους των παρόχων αυτών·

(15) «τρίτος πάροχος υπηρεσιών ΤΠΕ»: επιχείρηση που παρέχει ▌υπηρεσίες ***ΤΠΕ***, ***συμπεριλαμβανομένης μιας χρηματοπιστωτικής οντότητας που παρέχει υπηρεσίες ΤΠΕ η οποία αποτελεί μέρος επιχείρησης που παρέχει ευρύτερο φάσμα προϊόντων ή υπηρεσιών***, εξαιρουμένων, ωστόσο, των παρόχων στοιχείων υλισμικού και των επιχειρήσεων που διαθέτουν άδεια λειτουργίας σύμφωνα με το ενωσιακό δίκαιο και παρέχουν υπηρεσίες ηλεκτρονικών επικοινωνιών, όπως ορίζονται στο άρθρο 2 σημείο

[20] 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).

4 της οδηγίας (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[21]·

(15α) «ενδοομιλικός πάροχος υπηρεσιών ΤΠΕ»: επιχείρηση που αποτελεί μέρος χρηματοπιστωτικού ομίλου και παρέχει υπηρεσίες ΤΠΕ αποκλειστικά σε χρηματοπιστωτικές οντότητες του ίδιου ομίλου ή σε χρηματοπιστωτικές 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·

(16) «υπηρεσίες ΤΠΕ»: ψηφιακές υπηρεσίες και υπηρεσίες δεδομένων που παρέχονται μέσω των συστημάτων ΤΠΕ σε έναν ή περισσότερους εσωτερικούς ή εξωτερικούς χρήστες ***σε συνεχή βάση, εξαιρουμένων των συμβάσεων τηλεπικοινωνίας***·

(17) «κρίσιμη ή σημαντική λειτουργία»: ***δραστηριότητα ή υπηρεσία που είναι απαραίτητη για τη λειτουργία μιας χρηματοπιστωτικής οντότητας, η διαταραχή της οποίας θα έβλαπτε ουσιωδώς την αξιοπιστία ή τη συνέχεια των υπηρεσιών και δραστηριοτήτων της χρηματοπιστωτικής οντότητας ή*** της οποίας η ασυνεχής, πλημμελής ή αποτυχημένη εκτέλεση θα έβλαπτε ουσιωδώς τη συνεχή συμμόρφωση μιας χρηματοπιστωτικής οντότητας με τους όρους και τις υποχρεώσεις της άδειας λειτουργίας της, ή με άλλες υποχρεώσεις της βάσει της ισχύουσας νομοθεσίας για τις χρηματοπιστωτικές υπηρεσίες, ***συμπεριλαμβανομένων των «κρίσιμων λειτουργιών» όπως ορίζονται στο άρθρο 2, παράγραφος 1, σημείο 35 της οδηγίας 2014/59/ΕΕ***·

(18) «κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ»: τρίτος πάροχος υπηρεσιών ΤΠΕ που ορίζεται σύμφωνα με το άρθρο ***28*** και υπόκειται στο πλαίσιο εποπτείας που αναφέρεται στα άρθρα ***29*** έως 37·

(19) «τρίτος πάροχος υπηρεσιών ΤΠΕ εγκατεστημένος σε τρίτη χώρα»: τρίτος πάροχος υπηρεσιών ΤΠΕ ο οποίος είναι νομικό πρόσωπο εγκατεστημένο σε τρίτη χώρα ▌ και έχει συνάψει συμβατικές ρυθμίσεις με χρηματοπιστωτική οντότητα για την παροχή υπηρεσιών ΤΠΕ·

(20) «υπεργολάβος ΤΠΕ εγκατεστημένος σε τρίτη χώρα»: υπεργολάβος ΤΠΕ ο οποίος είναι νομικό πρόσωπο εγκατεστημένο σε τρίτη χώρα, ▌ και έχει συνάψει συμβατικές ρυθμίσεις με τρίτο πάροχο υπηρεσιών ΤΠΕ ή με τρίτο πάροχο υπηρεσιών ΤΠΕ εγκατεστημένο σε τρίτη χώρα·

(21) «κίνδυνος συγκέντρωσης ΤΠΕ»: έκθεση σε μεμονωμένους ή πολλαπλούς σχετικούς κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ που δημιουργεί βαθμό εξάρτησης από τους εν λόγω παρόχους κατά τέτοιον τρόπο ώστε η μη διαθεσιμότητα, η αθέτηση υποχρεώσεων ή άλλου είδους αδυναμία εκ μέρους των εν λόγω παρόχων να μπορεί δυνητικά να θέσει σε κίνδυνο ***τη χρηματοπιστωτική σταθερότητα της Ένωσης συνολικά ή*** την ικανότητα της χρηματοπιστωτικής οντότητας ▌ να παρέχει κρίσιμες ή σημαντικές λειτουργίες, ή να έχει άλλες μορφές δυσμενών επιπτώσεων, προκαλώντας, μεταξύ άλλων, μεγάλων ζημιών·

(22) «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, στο άρθρο 2 παράγραφος 1 σημείο 45 του κανονισμού (ΕΕ) αριθ. 909/2014, στο

[21] Οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (Αναδιατύπωση) (ΕΕ L 321 της 17.12.2018, σ. 36).

άρθρο 3 παράγραφος 1 σημείο 20 του κανονισμού (ΕΕ) 2016/1011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[22], στο άρθρο 3 παράγραφος 1 ***σημείο 18*** του κανονισμού (ΕΕ) 20xx/xx του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[23] [κανονισμός για τις αγορές κρυπτοστοιχείων (MICA)] ή τα ισοδύναμα πρόσωπα που διευθύνουν πράγματι την οντότητα ή ασκούν βασικά καθήκοντα σύμφωνα με τη σχετική ενωσιακή ή εθνική νομοθεσία·

(23) «πιστωτικό ίδρυμα»: πιστωτικό ίδρυμα κατά την έννοια του άρθρου 4 παράγραφος 1 σημείο 1) του κανονισμού (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[24]·

(23α) «πιστωτικό ίδρυμα που εξαιρείται από την οδηγία 2013/36/ΕΕ»: πιστωτικό ίδρυμα που τυγχάνει εξαίρεσης σύμφωνα με το άρθρο 2 παράγραφος 5, σημεία 4 έως 23 της οδηγίας 2013/36/ΕΕ·

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

(24α) «μικρή και μη διασυνδεδεμένη επιχείρηση επενδύσεων»: επιχείρηση επενδύσεων που πληροί τους όρους που ορίζονται στο άρθρο 12 παράγραφος 1 του κανονισμού (ΕΕ) 2019/2033·

(25) «ίδρυμα πληρωμών»: ίδρυμα πληρωμών όπως ορίζεται στο άρθρο 1 παράγραφος 1 στοιχείο δ) της οδηγίας (ΕΕ) 2015/2366·

(25α) «ίδρυμα πληρωμών που εξαιρείται από την οδηγία (ΕΕ)2015/2366»: ίδρυμα πληρωμών που τυγχάνει απαλλαγής σύμφωνα με το άρθρο 32 παράγραφος 1 της οδηγίας (ΕΕ)2015/2366·

(26) «ίδρυμα ηλεκτρονικού χρήματος»: ίδρυμα ηλεκτρονικού χρήματος όπως ορίζεται στο άρθρο 2 σημείο 1 της οδηγίας 2009/110/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[25]·

(26α) «ίδρυμα ηλεκτρονικού χρήματος που εξαιρείται από την οδηγία 2009/110/ΕΚ»: ίδρυμα ηλεκτρονικού χρήματος που τυγχάνει απαλλαγής σύμφωνα με το άρθρο 9 της οδηγίας 2009/110/ΕΚ·

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

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

---

22 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).

23 [*Να συμπληρωθεί ο πλήρης τίτλος και τα στοιχεία ΕΕ*]

24 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 επιχειρήσεις επενδύσεων και την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 (ΕΕ L 176 της 27.6.2013, σ. 1).

25 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).

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

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

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

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

(33) «πάροχος υπηρεσιών αναφοράς δεδομένων»: πάροχος υπηρεσιών αναφοράς δεδομένων όπως ορίζεται στο άρθρο 4 παράγραφος 1 σημείο 63 της οδηγίας 2014/65/ΕΕ·

(34) «ασφαλιστική επιχείρηση»: ασφαλιστική επιχείρηση όπως ορίζεται στο άρθρο 13 σημείο 1 της οδηγίας 2009/138/ΕΚ·

(35) «αντασφαλιστική επιχείρηση»: αντασφαλιστική επιχείρηση όπως ορίζεται στο άρθρο 13 σημείο 4 της οδηγίας 2009/138/ΕΚ·

(36) «ασφαλιστικός διαμεσολαβητής»: ασφαλιστικός διαμεσολαβητής όπως ορίζεται στο άρθρο 2 ***παράγραφος 1*** σημείο 3 της οδηγίας (ΕΕ) 2016/97·

(37) «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·

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

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

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

(41) «νόμιμος ελεγκτής»: νόμιμος ελεγκτής όπως ορίζεται στο άρθρο 2 σημείο 2 της οδηγίας 2006/43/ΕΚ·

(42) «ελεγκτικό γραφείο»: ελεγκτικό γραφείο όπως ορίζεται στο άρθρο 2 σημείο 3 της οδηγίας 2006/43/ΕΚ·

(43) «πάροχος υπηρεσιών κρυπτοστοιχείων»: πάροχος υπηρεσιών κρυπτοστοιχείων, όπως ορίζεται στο άρθρο 3 παράγραφος 1 στοιχείο ιδ) του κανονισμού (ΕΕ) 202x/xx [Υπηρεσία Εκδόσεων: Να συμπληρωθεί παραπομπή στον κανονισμό MICA]·

(44) «εκδότης κρυπτοστοιχείων»: εκδότης κρυπτοστοιχείων όπως ορίζεται στο άρθρο 3 παράγραφος 1 στοιχείο η) του [ΕΕ: Να συμπληρωθεί παραπομπή στον κανονισμό MICA]·

(44α) «προσφέρων»: ο προσφέρων όπως ορίζεται στο άρθρο 3 παράγραφος 1 στοιχείο ΧΧ) της [ΕΕ: Να συμπληρωθεί παραπομπή στον κανονισμό MICA]·

(44β) «προσφέρων κρυπτοστοιχείων»: προσφέρων «κρυπτοστοιχείων» όπως ορίζεται στο άρθρο 3 παράγραφος 1 στοιχείο XX) της [ΕΕ: Να συμπληρωθεί παραπομπή στον κανονισμό MICA]·

(45) «εκδότης ψηφιακών κερμάτων με εγγύηση περιουσιακών στοιχείων»: «εκδότης ψηφιακών κερμάτων πληρωμών με εγγύηση περιουσιακών στοιχείων» όπως ορίζεται στο άρθρο 3 παράγραφος 1 στοιχείο θ) του [ΕΕ: Να συμπληρωθεί παραπομπή στον κανονισμό MICA]·

(45α) «προσφέρων ψηφιακών κερμάτων με εγγύηση περιουσιακών στοιχείων»: προσφέρων ψηφιακών κερμάτων με εγγύηση περιουσιακών στοιχείων όπως ορίζεται στο άρθρο 3 παράγραφος 1 στοιχείο [(XX)] [ΕΕ: Να συμπληρωθεί παραπομπή στον κανονισμό MICA]·

(46) «εκδότης σημαντικών ψηφιακών κερμάτων με εγγύηση περιουσιακών στοιχείων»: εκδότης σημαντικών ψηφιακών κερμάτων πληρωμών με εγγύηση περιουσιακών στοιχείων όπως ορίζεται στο άρθρο 3 παράγραφος 1 στοιχείο (***XX***) του [ΕΕ: Να συμπληρωθεί παραπομπή στον κανονισμό MICA]·

(47) «διαχειριστής δεικτών αναφοράς κρίσιμης σημασίας»: διαχειριστής «δεικτών αναφοράς κρίσιμης σημασίας» όπως ορίζεται στο άρθρο ***3*** στοιχείο ***25***) του κανονισμού ***2016/1011*** [ΕΕ: Να συμπληρωθεί παραπομπή στον κανονισμό για τους δείκτες αναφοράς]·

(48) «πάροχος υπηρεσιών πληθοχρηματοδότησης»: πάροχος υπηρεσιών πληθοχρηματοδότησης όπως ορίζεται στο άρθρο ***2 παράγραφος 1*** στοιχείο ε) του κανονισμού (ΕΕ) ***2020/1503*** [Υπηρεσία Εκδόσεων: Να συμπληρωθεί παραπομπή στον κανονισμό για την πληθοχρηματοδότηση]·

(49) «αρχείο καταγραφής τιτλοποιήσεων»: αρχείο καταγραφής τιτλοποιήσεων όπως ορίζεται στο άρθρο 2 σημείο 23 του κανονισμού (ΕΕ) 2017/2402·

(50) «πολύ μικρή***, μικρή και μεσαία*** επιχείρηση»: χρηματοπιστωτική οντότητα όπως ορίζεται στο άρθρο 2 του παραρτήματος της σύστασης 2003/361/ΕΚ.

(50α) «αρχή εξυγίανσης»: αρχή που ορίζεται από κράτος μέλος, σύμφωνα με το άρθρο 3 της οδηγίας 2014/59/ΕΕ, ή από το ενιαίο συμβούλιο εξυγίανσης, που έχει συσταθεί σύμφωνα με το άρθρο 42 του κανονισμού 806/2014.

Άρθρο 3α

Αρχή της αναλογικότητας

1. Οι χρηματοπιστωτικές οντότητες εφαρμόζουν τους κανόνες που θεσπίζονται στα κεφάλαια ΙΙ, ΙΙΙ και IV, σύμφωνα με την αρχή της αναλογικότητας, λαμβάνοντας υπόψη το μέγεθός τους, τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, δραστηριοτήτων και λειτουργιών τους και το συνολικό προφίλ κινδύνου τους.

2. Σύμφωνα με την αρχή της αναλογικότητας, τα άρθρα 4 έως 14 του παρόντος κανονισμού δεν εφαρμόζονται:

α) σε μικρές και μη διασυνδεδεμένες επιχειρήσεις επενδύσεων ή ιδρύματα πληρωμών που εξαιρούνται από την οδηγία (ΕΕ) 2015/2366·

β) σε πιστωτικά ιδρύματα που εξαιρούνται από την οδηγία 2013/36/ΕΕ·

γ) σε ιδρύματα ηλεκτρονικού χρήματος που εξαιρούνται από την οδηγία 2009/110/ΕΚ· ή

δ) σε μικρά ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών.

3. Με βάση την ετήσια έκθεση σχετικά με την επανεξέταση του πλαισίου διαχείρισης κινδύνων ΤΠΕ, που αναφέρεται στο άρθρο 5 παράγραφος 6 και στο άρθρο 14α παράγραφος 2, οι σχετικές αρμόδιες αρχές επανεξετάζουν και αξιολογούν την εφαρμογή της αναλογικότητας από μια χρηματοπιστωτική οντότητα και προσδιορίζουν κατά πόσον το πλαίσιο διαχείρισης κινδύνων ΤΠΕ της χρηματοπιστωτικής οντότητας διασφαλίζει τη χρηστή διαχείριση, την ψηφιακή επιχειρησιακή ανθεκτικότητα και την κάλυψη του κινδύνου ΤΠΕ. Στο πλαίσιο αυτό, οι αρμόδιες αρχές λαμβάνουν υπόψη το μέγεθος της χρηματοπιστωτικής οντότητας, τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της, καθώς και το συνολικό προφίλ κινδύνου της.

4. Σε περίπτωση που η σχετική αρμόδια αρχή κρίνει ότι το πλαίσιο διαχείρισης κινδύνων ΤΠΕ της χρηματοπιστωτικής οντότητας είναι ανεπαρκές και δυσανάλογο, αρχίζει διάλογο με τη χρηματοπιστωτική οντότητα για να διορθωθούν οι ελλείψεις και να διασφαλιστεί η πλήρης συμμόρφωση με το κεφάλαιο ΙΙ.

5. Οι ΕΕΑ εκπονούν σχέδια ρυθμιστικών τεχνικών προτύπων σε σχέση με τα εξής:

α) τον προσδιορισμό του βαθμού στον οποίο οι υποχρεώσεις διαχείρισης κινδύνων ΤΠΕ εφαρμόζονται σε καθεμία από τις χρηματοπιστωτικές οντότητες που αναφέρονται στην παράγραφο 1·

β) τον περαιτέρω προσδιορισμό του περιεχομένου και της μορφής της ετήσιας έκθεσης σχετικά με την επανεξέταση του πλαισίου διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στην παράγραφο 3·

γ) τον περαιτέρω καθορισμό των κανόνων και των διαδικασιών που πρέπει να ακολουθούν οι αρμόδιες αρχές και οι χρηματοπιστωτικές οντότητες στο πλαίσιο του διαλόγου που αναφέρεται στην παράγραφο 4.

6. Οι ΕΕΑ υποβάλλουν τα σχέδια ρυθμιστικών τεχνικών προτύπων που αναφέρονται στην παράγραφο 5 στην Επιτροπή μέχρι τις 3 [ΕΕ: Να συμπληρωθεί ημερομηνία 1 έτος μετά την ημερομηνία έναρξης ισχύος].

Ανατίθεται στην Επιτροπή η εξουσία έκδοσης των ρυθμιστικών τεχνικών προτύπων που αναφέρονται στην παράγραφο 10 του παρόντος άρθρου, σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010 αντιστοίχως.

ΚΕΦΑΛΑΙΟ ΙΙ

ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΤΠΕ

ΤΜΗΜΑ Ι

Άρθρο 4

Διακυβέρνηση και οργάνωση

1. Οι χρηματοπιστωτικές οντότητες εφαρμόζουν ***εσωτερική διακυβέρνηση*** και ***πλαίσιο*** ελέγχου το οποίο διασφαλίζει την αποτελεσματική και συνετή διαχείριση όλων των κινδύνων ΤΠΕ, ***με σκοπό την επίτευξη υψηλού επιπέδου ψηφιακής επιχειρησιακής ανθεκτικότητας***.

2. Το διοικητικό όργανο της χρηματοπιστωτικής οντότητας καθορίζει, εγκρίνει, εποπτεύει και λογοδοτεί για την εφαρμογή όλων των ρυθμίσεων σχετικά με το πλαίσιο διαχείρισης κινδύνων ΤΠΕ το οποίο αναφέρεται στο άρθρο 5 παράγραφος 1:

   Για τους σκοπούς του πρώτου εδαφίου, το διοικητικό όργανο:

   α) φέρει την τελική ευθύνη για τη διαχείριση κινδύνων ΤΠΕ της χρηματοπιστωτικής οντότητας·

   αα) εφαρμόζει διαδικασίες και πολιτικές που στοχεύουν στη διασφάλιση της διατήρησης υψηλών προτύπων ασφάλειας, εμπιστευτικότητας και ακεραιότητας των δεδομένων·

   β) καθορίζει σαφείς ρόλους και αρμοδιότητες για όλες τις λειτουργίες που σχετίζονται με τις ΤΠΕ·

   γ) προσδιορίζει το κατάλληλο επίπεδο ανοχής κινδύνου για τον κίνδυνο ΤΠΕ της χρηματοπιστωτικής οντότητας, όπως αναφέρεται στο άρθρο 5 παράγραφος 9 στοιχείο β)·

   δ) εγκρίνει, εποπτεύει και επανεξετάζει περιοδικά την εφαρμογή, εκ μέρους της χρηματοπιστωτικής οντότητας, της πολιτικής αδιάλειπτης λειτουργίας των ΤΠΕ και του σχεδίου αποκατάστασης λειτουργίας των ΤΠΕ***, τα οποία μπορεί να εγκριθούν ως ειδική διακριτή πολιτική και ως αναπόσπαστο μέρος της ευρύτερης πολιτικής αδιάλειπτης λειτουργίας της χρηματοπιστωτικής οντότητας και του σχεδίου αποκατάστασης λειτουργίας έπειτα από καταστροφή,*** που αναφέρονται στο άρθρο 10 παράγραφοι 1 και 3 αντίστοιχα·

   ε) εγκρίνει και επανεξετάζει περιοδικά τα σχέδια ελέγχου ΤΠΕ, τους ελέγχους ΤΠΕ, καθώς και τις σημαντικές μεταβολές τους·

   στ) διαθέτει κατάλληλο προϋπολογισμό και τον επανεξετάζει τακτικά ώστε να καλύπτονται οι ανάγκες ψηφιακής επιχειρησιακής ανθεκτικότητας της χρηματοπιστωτικής οντότητας όσον αφορά όλα τα είδη των πόρων, μεταξύ των

οποίων η ***σχετική*** κατάρτιση όλων των μελών του προσωπικού σχετικά με κινδύνους και δεξιότητες ΤΠΕ ·

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

η) τηρείται δεόντως ενήμερο για όλες τις ρυθμίσεις που συνάπτονται με τρίτους παρόχους υπηρεσιών ΤΠΕ και αφορούν τη χρήση υπηρεσιών ΤΠΕ, κάθε σχετική προγραμματισμένη σημαντική μεταβολή σε σχέση με τους τρίτους παρόχους υπηρεσιών ΤΠΕ και τις πιθανές επιπτώσεις των μεταβολών αυτών στις κρίσιμες ή σημαντικές λειτουργίες που υπόκεινται στις εν λόγω ρυθμίσεις, συμπεριλαμβανομένης της παραλαβής συνοπτικής παρουσίασης της ανάλυσης κινδύνων για την εκτίμηση των επιπτώσεων των μεταβολών αυτών·

θ) τηρείται ***τακτικά*** ενήμερο ***τουλάχιστον*** για ***σημαντικά*** συμβάντα που σχετίζονται με τις ΤΠΕ και τις επιπτώσεις τους, καθώς και για τα μέτρα αντιμετώπισης, αποκατάστασης και επανόρθωσης.

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

4. Τα μέλη του διοικητικού οργάνου ***της χρηματοπιστωτικής οντότητας επικαιροποιούν ενεργά*** επαρκείς γνώσεις και δεξιότητες ▌ώστε να κατανοούν και να αξιολογούν τους κινδύνους ΤΠΕ και τις επιπτώσεις τους στις δραστηριότητες της χρηματοπιστωτικής οντότητας***, μεταξύ άλλων παρακολουθώντας ειδική κατάρτιση σε τακτική βάση, ανάλογη προς τους κινδύνους ΤΠΕ που τελούν υπό διαχείριση.***

ΤΜΗΜΑ ΙΙ

Άρθρο 5

Πλαίσιο διαχείρισης κινδύνων ΤΠΕ

1. Οι χρηματοπιστωτικές οντότητες πρέπει να διαθέτουν ισχυρό, ολοκληρωμένο και άρτια τεκμηριωμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ, που να 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 που αναφέρεται στην παράγραφο 1 περιλαμβάνει στρατηγικές, πολιτικές, διαδικασίες, πρωτόκολλα και εργαλεία ΤΠΕ που είναι απαραίτητα για την κατάλληλη και αποτελεσματική προστασία όλων των σχετικών υλικών συνιστωσών και υποδομών, συμπεριλαμβανομένου του υλισμικού, των διακομιστών, καθώς και όλων των σχετικών εγκαταστάσεων, κέντρων δεδομένων και ευαίσθητων οριοθετημένων χώρων, ώστε να διασφαλίζεται ότι όλα αυτά τα υλικά στοιχεία προστατεύονται επαρκώς από κινδύνους, συμπεριλαμβανομένης τυχόν βλάβης

και μη εξουσιοδοτημένης πρόσβασης ή χρήσης.

3. Οι χρηματοπιστωτικές οντότητες ελαχιστοποιούν τις επιπτώσεις των κινδύνων ΤΠΕ με την ανάπτυξη κατάλληλων στρατηγικών, πολιτικών, διαδικασιών, πρωτοκόλλων και εργαλείων, όπως προσδιορίζονται στο πλαίσιο διαχείρισης κινδύνων ΤΠΕ. Παρέχουν πλήρεις και επικαιροποιημένες πληροφορίες σχετικά με τους κινδύνους ΤΠΕ ***και σχετικά με το πλαίσιό τους για τη διαχείριση κινδύνων ΤΠΕ***, όπως απαιτείται από τις αρμόδιες αρχές.

4. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στην παράγραφο 1, οι χρηματοπιστωτικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, εφαρμόζουν σύστημα διαχείρισης της ασφάλειας των πληροφοριών βάσει αναγνωρισμένων διεθνών προτύπων και σύμφωνα με τις εποπτικές κατευθυντήριες γραμμές, ***εφόσον ήδη είναι διαθέσιμες και κατάλληλες, συμπεριλαμβανομένης της καθοδήγησης που εκτίθεται στις σχετικές κατευθυντήριες γραμμές που θεσπίζονται από τις ΕΕΑ***, το οποίο επανεξετάζουν τακτικά.

5. Οι χρηματοπιστωτικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, ***εκχωρούν την ευθύνη για τη διαχείριση και την εποπτεία των κινδύνων ΤΠΕ σε μια λειτουργία ελέγχου και διασφαλίζουν την ανεξαρτησία της εν λόγω λειτουργίας ελέγχου προκειμένου να αποφεύγεται η σύγκρουση συμφερόντων***. ***Οι χρηματοπιστωτικές οντότητες*** διασφαλίζουν ***την κατάλληλη ανεξαρτησία*** των λειτουργιών διαχείρισης ΤΠΕ, των λειτουργιών ελέγχου και των λειτουργιών εσωτερικού ελέγχου, σύμφωνα με το μοντέλο τριών γραμμών άμυνας ή ένα εσωτερικό μοντέλο διαχείρισης κινδύνων και ελέγχου.

6. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στην παράγραφο 1 τεκμηριώνεται και επανεξετάζεται τουλάχιστον μία φορά ετησίως, καθώς και κατά την επέλευση σημαντικών 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 σε ετήσια βάση.

7. ***Όσον αφορά τις χρηματοπιστωτικές οντότητες πλην των πολύ μικρών επιχειρήσεων,*** το πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στην παράγραφο 1 ελέγχεται τακτικά από ελεγκτές ΤΠΕ που διαθέτουν επαρκείς γνώσεις, δεξιότητες και εμπειρογνωσία σε θέματα κινδύνων ΤΠΕ. Η συχνότητα και η εστίαση των ελέγχων ΤΠΕ είναι ανάλογες προς τους κινδύνους ΤΠΕ που αντιμετωπίζει η χρηματοπιστωτική οντότητα.

8. Θεσπίζεται επίσημη διαδικασία παρακολούθησης, που περιλαμβάνει κανόνες για την έγκαιρη επαλήθευση και επανόρθωση κρίσιμων ευρημάτων ελέγχου ΤΠΕ, λαμβανομένων υπόψη των συμπερασμάτων από την επανεξέταση του ελέγχου. ▌

9. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στην παράγραφο 1 περιλαμβάνει στρατηγική ψηφιακής ***επιχειρησιακής*** ανθεκτικότητας για τον καθορισμό του τρόπου εφαρμογής του πλαισίου. Για τον σκοπό αυτόν, 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 χρηματοπιστωτικής οντότητας·

β) θεσπίζοντας το επίπεδο ανοχής κινδύνου για τον κίνδυνο ΤΠΕ, σύμφωνα με τη διάθεση ανάληψης κινδύνων της χρηματοπιστωτικής οντότητας, και αναλύοντας την ανοχή στις επιπτώσεις των διαταραχών των ΤΠΕ·

γ) καθορίζοντας σαφείς στόχους ασφάλειας των πληροφοριών·

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

ε) περιγράφοντας τους διάφορους μηχανισμούς που εφαρμόζονται για τον εντοπισμό, την προστασία και την αποτροπή των επιπτώσεων των συμβάντων που σχετίζονται με τις ΤΠΕ·

στ) τεκμηριώνοντας τον αριθμό των αναφερόμενων σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ και την αποτελεσματικότητα των προληπτικών μέτρων·

ζ) ***προσδιορίζοντας*** βασικές εξαρτήσεις από τρίτους παρόχους υπηρεσιών ΤΠΕ και ***εκθέτοντας λεπτομερώς στρατηγικές εξόδου σε σχέση με τέτοιες βασικές εξαρτήσεις***·

η) εφαρμόζοντας δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας***, σύμφωνα με το κεφάλαιο IV του παρόντος κανονισμού***·

θ) περιγράφοντας μια στρατηγική επικοινωνίας σε περίπτωση συμβάντων που σχετίζονται με τις ΤΠΕ ***τα οποία απαιτείται να γνωστοποιούνται σύμφωνα με το άρθρο 13***.

10. Κατόπιν έγκρισης από τις αρμόδιες αρχές, οι χρηματοπιστωτικές οντότητες δύνανται να ***αναθέτουν*** τα καθήκοντα επαλήθευσης της συμμόρφωσης με τις απαιτήσεις διαχείρισης κινδύνων ΤΠΕ σε ▌ εξωτερικές επιχειρήσεις.

Κατόπιν κοινοποίησης στις αρμόδιες αρχές, οι χρηματοπιστωτικές οντότητες δύνανται να αναθέτουν το καθήκον επαλήθευσης της συμμόρφωσης με τις απαιτήσεις διαχείρισης κινδύνων ΤΠΕ σε ενδοομιλικές επιχειρήσεις.

Σε περίπτωση που πραγματοποιείται η ανάθεση που αναφέρεται στο δεύτερο εδάφιο, η χρηματοπιστωτική οντότητα θα παραμένει πλήρως υπόλογη για την επαλήθευση της συμμόρφωσης με τις απαιτήσεις διαχείρισης κινδύνων ΤΠΕ.

Άρθρο 6

Συστήματα, πρωτόκολλα και εργαλεία ΤΠΕ

1. Οι χρηματοπιστωτικές οντότητες χρησιμοποιούν και διατηρούν επικαιροποιημένα συστήματα, πρωτόκολλα και εργαλεία ΤΠΕ, ***προκειμένου να αντιμετωπίζουν και να διαχειρίζονται τον κίνδυνο ΤΠΕ,*** τα οποία πληρούν τις ακόλουθες προϋποθέσεις:

α) τα συστήματα και τα εργαλεία είναι κατάλληλα για ▌το μέγεθος των εργασιών που υποστηρίζουν τη διεξαγωγή των δραστηριοτήτων τους·

β) είναι αξιόπιστα·

γ) διαθέτουν επαρκή χωρητικότητα ώστε να επεξεργάζονται με ακρίβεια τα δεδομένα που είναι αναγκαία για την έγκαιρη εκτέλεση δραστηριοτήτων και 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.

2. Σε περίπτωση που οι χρηματοπιστωτικές οντότητες χρησιμοποιούν διεθνώς αναγνωρισμένα τεχνικά πρότυπα και πρωτοπόρες πρακτικές του κλάδου όσον αφορά την ασφάλεια των πληροφοριών και τους εσωτερικούς ελέγχους ΤΠΕ, χρησιμοποιούν τα εν λόγω πρότυπα και τις πρακτικές σύμφωνα με τυχόν σχετικές εποπτικές συστάσεις για την ενσωμάτωσή τους.

Άρθρο 7

Προσδιορισμός

1. Στο πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 5 παράγραφος 1, οι χρηματοπιστωτικές οντότητες προσδιορίζουν, ταξινομούν και τεκμηριώνουν επαρκώς όλες τις ***κρίσιμες ή σημαντικές*** επιχειρηματικές λειτουργίες που σχετίζονται με τις ΤΠΕ, τα πληροφοριακά περιουσιακά στοιχεία που υποστηρίζουν τις λειτουργίες αυτές, καθώς και τη διαμόρφωση των συστημάτων ΤΠΕ και τη διασύνδεσή τους με εσωτερικά και εξωτερικά συστήματα ΤΠΕ. Οι χρηματοπιστωτικές οντότητες επανεξετάζουν, όταν κρίνεται αναγκαίο, και τουλάχιστον σε ετήσια βάση, ***την κρισιμότητα ή τη σπουδαιότητα των επιχειρηματικών λειτουργιών που σχετίζονται με τις ΤΠΕ καθώς και*** την επάρκεια της ταξινόμησης των πληροφοριακών πόρων και τυχόν συναφών εγγράφων τεκμηρίωσης.

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

3. Οι χρηματοπιστωτικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, προβαίνουν***, όπου αρμόζει,*** σε αξιολόγηση κινδύνων έπειτα από κάθε σημαντική αλλαγή της υποδομής των συστημάτων δικτύου και πληροφοριών, των διαδικασιών ή των διεργασιών που επηρεάζουν τις λειτουργίες, τις υποστηρικτικές διαδικασίες ή τους πληροφοριακούς πόρους τους.

4. Οι χρηματοπιστωτικές οντότητες προσδιορίζουν όλους τους λογαριασμούς

συστημάτων ΤΠΕ, συμπεριλαμβανομένων εκείνων που βρίσκονται σε απομακρυσμένες τοποθεσίες, τους πόρους δικτύου και τον εξοπλισμό υλισμικού και καταγράφουν τον υλικό εξοπλισμό που θεωρείται ζωτικής σημασίας. Καταγράφουν τις παραμέτρους των ***κρίσιμων ή σημαντικών*** πόρων ΤΠΕ, ***λαμβάνοντας υπόψη τον σκοπό τους*** καθώς και τις συνδέσεις και τις αλληλεξαρτήσεις μεταξύ των ***εν λόγω*** διαφόρων πόρων ΤΠΕ.

5. Οι χρηματοπιστωτικές οντότητες προσδιορίζουν και τεκμηριώνουν όλες τις ***κρίσιμες ή σημαντικές*** διαδικασίες που εξαρτώνται από τρίτους παρόχους υπηρεσιών ΤΠΕ και προσδιορίζουν τις διασυνδέσεις με τρίτους παρόχους υπηρεσιών ΤΠΕ ***που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες***.

6. Για τους σκοπούς των παραγράφων 1, 4 και 5, οι χρηματοπιστωτικές οντότητες τηρούν και επικαιροποιούν τακτικά τους σχετικούς καταλόγους.

7. Οι χρηματοπιστωτικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, διενεργούν τακτικά, και τουλάχιστον σε ετήσια βάση, ειδική αξιολόγηση κινδύνων ΤΠΕ σε όλα τα ήδη υφιστάμενα συστήματα ΤΠΕ***, συμπεριλαμβανομένων συστημάτων τα οποία βρίσκονται ακόμη σε χρήση και επιτελούν τις λειτουργίες τους, αλλά τα οποία:***

α) είναι παλαιά ή βρίσκονται στο τέλος της ζωής τους, στην περίπτωση υλισμικού·

β) δεν είναι πλέον σε θέση να λαμβάνουν υποστήριξη ή συντήρηση από τον προμηθευτή τους· ή

γ) είναι αδύνατο ή ασύμφορο να επικαιροποιηθούν. Ετήσιες εκτιμήσεις κινδύνων ΤΠΕ διενεργούνται σε κληροδοτημένα συστήματα ΤΠΕ, ιδίως πριν και μετά τη σύνδεση ▌τεχνολογιών, εφαρμογών ή συστημάτων.

Άρθρο 8

Προστασία και πρόληψη

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

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

3. Για την επίτευξη των στόχων που αναφέρονται στην παράγραφο 2, οι χρηματοπιστωτικές οντότητες χρησιμοποιούν ▌τεχνολογίες και διαδικασίες ΤΠΕ οι οποίες:

α) ***μεγιστοποιούν*** την ασφάλεια των μέσων διαβίβασης των πληροφοριών·

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

γ) αποτρέπουν τη διαρροή πληροφοριών·

δ) διασφαλίζουν ότι τα δεδομένα προστατεύονται από ***εσωτερικούς*** κινδύνους ***ΤΠΕ, συμπεριλαμβανομένων των κινδύνων*** πλημμελούς διοίκησης***, των κινδύνων*** που σχετίζονται με την επεξεργασία ***και του ανθρώπινου σφάλματος***.

4. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 5 παράγραφος 1***, σύμφωνα με το προφίλ κινδύνου τους,*** οι χρηματοπιστωτικές οντότητες:

α) καταρτίζουν και τεκμηριώνουν μια πολιτική ασφάλειας των πληροφοριών, η οποία ορίζει κανόνες για την προστασία του απορρήτου, της ακεραιότητας και της διαθεσιμότητας των πόρων ΤΠΕ, ***των δεδομένων και των πληροφοριακών πόρων*** που χρησιμοποιούν οι ίδιες ***ενώ διασφαλίζουν την πλήρη προστασία των πόρων ΤΠΕ,*** των δεδομένων και των πληροφοριακών πόρων ***που χρησιμοποιούν*** οι πελάτες τους ***όταν αποτελούν μέρος των συστημάτων ΤΠΕ των χρηματοπιστωτικών οντοτήτων·***

β) ακολουθώντας μια προσέγγιση βάσει κινδύνων, θεσπίζουν ορθή διαχείριση δικτύων και υποδομών χρησιμοποιώντας κατάλληλες τεχνικές, μεθόδους και πρωτόκολλα, ***τα οποία μπορεί να περιλαμβάνουν την εφαρμογή*** ▌ μηχανισμών για την απομόνωση των πληροφοριακών πόρων που επηρεάζονται σε περίπτωση κυβερνοεπιθέσεων·

γ) εφαρμόζουν πολιτικές***, διαδικασίες και ελέγχους*** που περιορίζουν την υλική και εικονική πρόσβαση σε πόρους και δεδομένα του συστήματος ΤΠΕ στην πρόσβαση που είναι απολύτως αναγκαία για τις νόμιμες και εγκεκριμένες λειτουργίες και δραστηριότητες ▌·

δ) εφαρμόζουν πολιτικές και πρωτόκολλα για ισχυρούς μηχανισμούς επαλήθευσης της ταυτότητας, ***και προστασία με κλειδιά κρυπτογράφησης,*** βάσει σχετικών προτύπων και ειδικών συστημάτων ελέγχου ▌·

ε) εφαρμόζουν πολιτικές, διαδικασίες και ελέγχους για τη διαχείριση αλλαγών στις ΤΠΕ, συμπεριλαμβανομένων αλλαγών σε λογισμικό, υλισμικό, στοιχεία υλικολογισμικού, αλλαγές συστήματος ή ασφάλειας, που βασίζονται σε μια προσέγγιση αξιολόγησης κινδύνου και αποτελούν αναπόσπαστο μέρος της συνολικής διαδικασίας διαχείρισης αλλαγών της χρηματοπιστωτικής 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 πολιτικές σχετικά με τις ενημερώσεις κώδικα και τις επικαιροποιήσεις.

Για τους σκοπούς του στοιχείου β), οι χρηματοπιστωτικές οντότητες σχεδιάζουν την υποδομή σύνδεσης δικτύου κατά τρόπο ώστε να μπορεί να διακοπεί το ταχύτερο δυνατόν και διασφαλίζουν τη διαμερισματοποίηση και τον κατακερματισμό της προκειμένου να ελαχιστοποιείται και να αποτρέπεται η μετάδοση, ιδίως όσον αφορά τις διασυνδεδεμένες χρηματοπιστωτικές διαδικασίες.

Για τους σκοπούς του στοιχείου ε), η διαδικασία διαχείρισης αλλαγών ΤΠΕ εγκρίνεται από κατάλληλες ιεραρχικές δομές και έχει ενεργοποιήσει ειδικά πρωτόκολλα για αλλαγές έκτακτης ανάγκης.

Άρθρο 9

Εντοπισμός

1. Οι χρηματοπιστωτικές οντότητες διαθέτουν μηχανισμούς για τον άμεσο εντοπισμό αντικανονικών δραστηριοτήτων, σύμφωνα με το άρθρο 15, συμπεριλαμβανομένων ζητημάτων που αφορούν τις επιδόσεις του δικτύου ΤΠΕ και συμβάντων που σχετίζονται με τις ΤΠΕ, καθώς και***, όπου είναι τεχνολογικά εφικτό,*** για τον προσδιορισμό ***και την παρακολούθηση*** όλων των δυνητικά σημαντικών μοναδικών σημείων αποτυχίας.

   Όλοι οι μηχανισμοί εντοπισμού που αναφέρονται στο πρώτο εδάφιο υποβάλλονται τακτικά σε δοκιμές σύμφωνα με το άρθρο 22.

2. Οι μηχανισμοί εντοπισμού που αναφέρονται στην παράγραφο 1 ***ενεργοποιούν διαδικασίες*** εντοπισμού και 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 χρηματοπιστωτικές οντότητες διαθέτουν επαρκείς πόρους και δυνατότητες, ▌ώστε να παρακολουθούν τη δραστηριότητα των χρηστών, την εμφάνιση αντικανονικών δραστηριοτήτων ΤΠΕ και συμβάντων που σχετίζονται με τις ΤΠΕ, ιδίως όσον αφορά κυβερνοεπιθέσεις.

3α. Οι χρηματοπιστωτικές οντότητες καταγράφουν όλα τα συμβάντα που σχετίζονται με τις ΤΠΕ και έχουν αντίκτυπο στη σταθερότητα, τη συνέχεια ή την ποιότητα των χρηματοπιστωτικών υπηρεσιών, συμπεριλαμβανομένων των περιπτώσεων στις οποίες το συμβάν είχε ή είναι πιθανό να έχει αντίκτυπο σε παρόμοιες υπηρεσίες.

4. Οι χρηματοπιστωτικές οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 στοιχείο ιβ) 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 τυχόν εσφαλμένων αναφορών.

Άρθρο 10

Αντιμετώπιση και αποκατάσταση

1. Στο πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 5 παράγραφος 1 και βάσει των απαιτήσεων προσδιορισμού που προβλέπονται στο άρθρο 7, οι χρηματοπιστωτικές οντότητες θέτουν σε εφαρμογή ▌ολοκληρωμένη πολιτική αδιάλειπτης λειτουργίας των ΤΠΕ***, η οποία μπορεί να εγκριθεί ως ειδική και διακριτή πολιτική και*** ως αναπόσπαστο μέρος της ***ευρύτερης*** πολιτικής αδιάλειπτης επιχειρησιακής λειτουργίας της χρηματοπιστωτικής οντότητας ***σε κλίμακα επιχείρησης***.

   Η πολιτική αδιάλειπτης λειτουργίας ΤΠΕ αποσκοπεί στη διαχείριση και τον μετριασμό των κινδύνων που θα μπορούσαν να έχουν επιβλαβείς επιπτώσεις στα συστήματα ΤΠΕ και στις υπηρεσίες ΤΠΕ των χρηματοπιστωτικών οντοτήτων, καθώς και στη διευκόλυνση της ταχείας ανάκαμψής τους, εάν χρειαστεί. Κατά την

κατάρτιση της πολιτικής αδιάλειπτης λειτουργίας ΤΠΕ, οι χρηματοπιστωτικές οντότητες εξετάζουν συγκεκριμένα τους κινδύνους που θα μπορούσαν να έχουν επιβλαβείς επιπτώσεις στις υπηρεσίες ΤΠΕ και στα συστήματα ΤΠΕ.

2. Οι χρηματοπιστωτικές οντότητες εφαρμόζουν την πολιτική αδιάλειπτης λειτουργίας των ΤΠΕ που αναφέρεται στην παράγραφο 1 μέσω ειδικών, κατάλληλων και τεκμηριωμένων ρυθμίσεων, σχεδίων, διαδικασιών και μηχανισμών, με στόχο:

β) τη διασφάλιση της συνέχειας των κρίσιμων λειτουργιών της χρηματοπιστωτικής οντότητας·

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

δ) 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 αποκατάστασης, οι οποίες θεσπίζονται σύμφωνα με το άρθρο 11·

ε) την προκαταρκτική εκτίμηση επιπτώσεων, βλαβών και ζημιών·

στ) τον καθορισμό δράσεων επικοινωνίας και διαχείρισης κρίσεων, οι οποίες διασφαλίζουν τη διαβίβαση επικαιροποιημένων πληροφοριών σε όλα τα μέλη του αρμόδιου εσωτερικού προσωπικού και τα εξωτερικά ενδιαφερόμενα μέρη, σύμφωνα με το άρθρο 13, και αναφέρονται στις αρμόδιες αρχές σύμφωνα με το άρθρο 17.

3. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 5 παράγραφος 1, οι χρηματοπιστωτικές οντότητες εφαρμόζουν σχετικό σχέδιο αποκατάστασης λειτουργίας των ΤΠΕ μετά από καταστροφή, το οποίο υπόκειται, στην περίπτωση των χρηματοπιστωτικών οντοτήτων πλην των πολύ μικρών επιχειρήσεων, σε επανεξέταση από ανεξάρτητους ελεγκτές.

4. Οι χρηματοπιστωτικές οντότητες θεσπίζουν, διατηρούν και υποβάλλουν περιοδικά σε δοκιμή κατάλληλα σχέδια αδιάλειπτης λειτουργίας 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 ολοκληρωμένης διαχείρισης κινδύνων ΤΠΕ, οι χρηματοπιστωτικές οντότητες:

α) υποβάλλουν σε δοκιμή την πολιτική αδιάλειπτης λειτουργίας των ΤΠΕ και το σχέδιο αποκατάστασης λειτουργίας των ΤΠΕ μετά από καταστροφή τουλάχιστον ετησίως και μετά από σημαντικές αλλαγές ***σε κρίσιμα ή σημαντικά*** συστήματα ΤΠΕ·

β) υποβάλλουν σε δοκιμή τα σχέδια επικοινωνίας σε καταστάσεις κρίσης που καταρτίζονται σύμφωνα με το άρθρο 13.

Για τους σκοπούς του στοιχείου α), οι χρηματοπιστωτικές οντότητες, πλην των πολύ

μικρών επιχειρήσεων, περιλαμβάνουν στα σχέδια δοκιμών σενάρια κυβερνοεπιθέσεων και μετάβασης μεταξύ της κύριας υποδομής ΤΠΕ και της πλεονάζουσας χωρητικότητας, αντίγραφα ασφαλείας και εφεδρικές εγκαταστάσεις που απαιτούνται για την εκπλήρωση των υποχρεώσεων που προβλέπονται στο άρθρο 11.

Οι χρηματοπιστωτικές οντότητες επανεξετάζουν ανά τακτά χρονικά διαστήματα την πολιτική αδιάλειπτης λειτουργίας των ΤΠΕ και το σχέδιο αποκατάστασης λειτουργίας των ΤΠΕ μετά από καταστροφή, λαμβάνοντας υπόψη τα αποτελέσματα των δοκιμών που διενεργούνται σύμφωνα με το πρώτο εδάφιο και τις συστάσεις που προκύπτουν από ελέγχους ή εποπτικές αξιολογήσεις.

6. Οι χρηματοπιστωτικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, διαθέτουν λειτουργία διαχείρισης κρίσεων, ***είτε ως ειδική λειτουργία είτε ως μέρος των λειτουργιών με αρμοδιότητες για την αντιμετώπιση και τη διαχείριση συμβάντων. Η λειτουργία διαχείρισης κρίσεων,*** σε περίπτωση ενεργοποίησης της πολιτικής αδιάλειπτης λειτουργίας των ΤΠΕ ή του σχεδίου αποκατάστασης λειτουργίας των ΤΠΕ μετά από καταστροφή, καθορίζει σαφείς διαδικασίες για τη διαχείριση της εσωτερικής και εξωτερικής επικοινωνίας σε καταστάσεις κρίσης σύμφωνα με το άρθρο 13.

7. Οι χρηματοπιστωτικές οντότητες τηρούν αρχεία ***σχετικών*** δραστηριοτήτων πριν από γεγονότα διαταραχής, καθώς και κατά τη διάρκεια αυτών, όταν ενεργοποιείται η πολιτική αδιάλειπτης λειτουργίας των ΤΠΕ ή το σχέδιο αποκατάστασης λειτουργίας των ΤΠΕ μετά από καταστροφή. Τα αρχεία αυτά καθίστανται άμεσα διαθέσιμα.

8. Οι χρηματοπιστωτικές οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 στοιχείο στ) παρέχουν στις αρμόδιες αρχές αντίγραφα των αποτελεσμάτων των δοκιμών αδιάλειπτης λειτουργίας των ΤΠΕ ή παρόμοιων ασκήσεων που πραγματοποιήθηκαν κατά την υπό εξέταση περίοδο.

9. Οι χρηματοπιστωτικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, υποβάλλουν στις αρμόδιες αρχές έκθεση σχετικά με το σύνολο του ***εκτιμώμενου οικονομικού*** κόστους και των ζημιών που προκλήθηκαν από ***σημαντικές*** διαταραχές των ΤΠΕ και ***μείζονα*** συμβάντα που σχετίζονται με τις ΤΠΕ.

9α. Οι ΕΕΑ, μέσω της Μικτής Επιτροπής, καταρτίζουν κοινές κατευθυντήριες γραμμές σχετικά με τη μεθοδολογία για τον υπολογισμό του κόστους και τον ποσοτικό προσδιορισμό των ζημιών, που αναφέρονται στην παράγραφο 9.

Άρθρο 11

Πολιτικές δημιουργίας αντιγράφων ασφαλείας και μέθοδοι αποκατάστασης

1. Για τους σκοπούς της διασφάλισης της αποκατάστασης των συστημάτων ΤΠΕ με ελάχιστο χρόνο διακοπής και με περιορισμό της διαταραχής, στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ, οι χρηματοπιστωτικές οντότητες αναπτύσσουν:

   α) πολιτική δημιουργίας αντιγράφων ασφαλείας στην οποία προσδιορίζεται το εύρος των δεδομένων που υπόκεινται σε αντίγραφα ασφαλείας και η ελάχιστη συχνότητα δημιουργίας αντιγράφων ασφαλείας, βάσει της κρισιμότητας των πληροφοριών ή της ευαισθησίας των δεδομένων·

   β) μεθόδους αποκατάστασης της λειτουργίας.

2. ***Σύμφωνα με την πολιτική αντιγράφων ασφαλείας που προσδιορίζεται στο στοιχείο***

α) της παραγράφου 1, τα συστήματα δημιουργίας αντιγράφων ασφαλείας αρχίζουν την επεξεργασία χωρίς αδικαιολόγητη καθυστέρηση, εκτός εάν μια τέτοια εκκίνηση θέτει σε κίνδυνο την ασφάλεια των συστημάτων δικτύου και πληροφοριών ή την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων.

3. Κατά την επαναφορά των δεδομένων των αντιγράφων ασφαλείας με χρήση ιδίων συστημάτων, οι χρηματοπιστωτικές οντότητες χρησιμοποιούν συστήματα ΤΠΕ ***τα οποία είναι διαχωρισμένα, είτε φυσικά είτε λογικά,*** από το κύριο σύστημα ΤΠΕ ***τους, τα οποία προστατεύονται*** με ασφάλεια από κάθε μη εξουσιοδοτημένη πρόσβαση ή φθορά των ΤΠΕ.

Για τις χρηματοπιστωτικές οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 στοιχείο ζ), 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.

4. Οι χρηματοπιστωτικές οντότητες ***εκτιμούν την ανάγκη να*** διατηρούν πλεονάζουσες χωρητικότητες ΤΠΕ εξοπλισμένες με επαρκείς και κατάλληλους πόρους, δυνατότητες και λειτουργίες για την κάλυψη των επιχειρηματικών αναγκών ***και την ικανοποίηση των απαιτήσεων ψηφιακής επιχειρησιακής ανθεκτικότητας που εκτίθενται στον παρόντα κανονισμό***.

5. Οι χρηματοπιστωτικές οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 στοιχείο στ) διατηρούν, ή μεριμνούν ώστε να διατηρούν οι τρίτοι πάροχοι ΤΠΕ με τους οποίους συνεργάζονται, τουλάχιστον έναν δευτερεύοντα τόπο επεξεργασίας με επαρκείς και κατάλληλους 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 υπηρεσιών κατά πανομοιότυπο τρόπο με τον κύριο τόπο ή να παρέχει το απαιτούμενο επίπεδο υπηρεσιών ώστε να διασφαλίζεται ότι η χρηματοπιστωτική οντότητα εκτελεί τις κρίσιμες δραστηριότητές της στο πλαίσιο των στόχων αποκατάστασης·

γ) είναι ▌προσβάσιμος από το προσωπικό της χρηματοπιστωτικής 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 χρηματοπιστωτικές οντότητες λαμβάνουν υπόψη ***εάν 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 χρηματοπιστωτικές οντότητες ***διασφαλίζουν ότι η ακεραιότητα των δεδομένων***

βρίσκεται στο ανώτατο επίπεδο, για παράδειγμα μέσω της διενέργειας πολλαπλών ελέγχων, μεταξύ άλλων της συμφωνίας μεταξύ των στοιχείων. ***Παρόμοιοι*** έλεγχοι ▌ διενεργούνται επίσης κατά την ανακατασκευή δεδομένων από εξωτερικά ενδιαφερόμενα μέρη, ώστε να διασφαλίζεται ότι όλα η συνεκτικότητα των δεδομένων μεταξύ των συστημάτων.

Άρθρο 12

Εκπαίδευση και εξέλιξη

1. Οι χρηματοπιστωτικές οντότητες πρέπει να 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 χρηματοπιστωτικές οντότητες προβαίνουν σε ελέγχους μετά από ***μείζονα*** συμβάντα που σχετίζονται με τις ΤΠΕ έπειτα από σημαντικές διαταραχές των ΤΠΕ στο πλαίσιο των βασικών τους δραστηριοτήτων, αναλύοντας τα αίτια της διαταραχής και προσδιορίζοντας τις βελτιώσεις που απαιτούνται στις λειτουργίες των ΤΠΕ ή στο πλαίσιο της πολιτικής αδιάλειπτης λειτουργίας των ΤΠΕ, όπως αναφέρεται στο άρθρο 10.

   Σε περίπτωση υλοποίησης αλλαγών***, που συνδέονται με την αντιμετώπιση κινδύνων ΤΠΕ οι οποίοι έχουν εντοπισθεί ως αποτέλεσμα ελέγχων μετά από μείζονα συμβάντα που σχετίζονται με τις ΤΠΕ,*** οι χρηματοπιστωτικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, κοινοποιούν ***όλες*** τις ***σημαντικές*** αλλαγές ▌ στις αρμόδιες αρχές***, αναφέροντας λεπτομερώς τις απαιτούμενες βελτιώσεις και τον τρόπο με τον οποίο αυτές αποσκοπούν στην πρόληψη ή τον μετριασμό των διαταραχών στο μέλλον. Η κοινοποίηση των αλλαγών στις αρμόδιες αρχές μπορεί να προηγείται ή να έπεται της εφαρμογής των αλλαγών.***

   Οι έλεγχοι μετά από συμβάντα 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 προειδοποιήσεις ασφάλειας και προσδιορισμού των επιπτώσεων και της σοβαρότητας των συμβάντων που σχετίζονται με τις ΤΠΕ·

   β) την ποιότητα και την ταχύτητα στη διενέργεια εγκληματολογικής ανάλυσης·

   γ) την αποτελεσματικότητα της παραπομπής του συμβάντος στο κατάλληλο επίπεδο εντός της χρηματοπιστωτικής 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 23 και 24 όσο και από πραγματικά συμβάντα που σχετίζονται με τις ΤΠΕ, ιδίως κυβερνοεπιθέσεις, μαζί με τις προκλήσεις που αντιμετωπίστηκαν κατά την ενεργοποίηση του σχεδίου αδιάλειπτης λειτουργίας ή του σχεδίου αποκατάστασης λειτουργίας, 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 πορίσματα αυτά τροφοδοτούν τη δέουσα επανεξέταση των συναφών συνιστωσών του πλαισίου διαχείρισης κινδύνων ΤΠΕ, όπως αναφέρεται στο άρθρο 5 παράγραφος 1.

4. Οι χρηματοπιστωτικές οντότητες παρακολουθούν την αποτελεσματικότητα της εφαρμογής της στρατηγικής τους για την ψηφιακή ανθεκτικότητα που καθορίζεται στο άρθρο 5 παράγραφος 9. Χαρτογραφούν την εξέλιξη των κινδύνων ΤΠΕ με την πάροδο του χρόνου, ***συμπεριλαμβανομένης της εγγύτητας των εν λόγω κινδύνων σε κρίσιμες ή σημαντικές λειτουργίες,*** 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 και να ενισχύσουν τα επίπεδα ωριμότητας και ετοιμότητας της χρηματοπιστωτικής οντότητας στον κυβερνοχώρο.

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

6. Οι χρηματοπιστωτικές 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 προγράμματα ευαισθητοποίησης σε θέματα ασφάλειας ΤΠΕ εφαρμόζονται σε όλο το προσωπικό. Η κατάρτιση στην ψηφιακή επιχειρησιακή ανθεκτικότητα ισχύει*** για όλους τους υπαλλήλους ***που έχουν δικαίωμα άμεσης πρόσβασης στα συστήματα ΤΠΕ*** και για τα ανώτερα διοικητικά στελέχη. ***Η πολυπλοκότητα των ενοτήτων κατάρτισης είναι ανάλογη προς το επίπεδο άμεσης πρόσβασης του υπαλλήλου στα συστήματα ΤΠΕ και, ειδικότερα, λαμβάνει υπόψη την πρόσβασή του σε κρίσιμες ή σημαντικές λειτουργίες.***

Οι χρηματοπιστωτικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, παρακολουθούν τις σχετικές τεχνολογικές εξελίξεις σε διαρκή βάση, με σκοπό επίσης την κατανόηση των πιθανών επιπτώσεων της επέκτασης 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 αντιμετωπίζονται αποτελεσματικά οι τρέχουσες ή νέες μορφές κυβερνοεπιθέσεων.

Άρθρο 13

Επικοινωνία

1. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 5 παράγραφος 1, οι χρηματοπιστωτικές οντότητες διαθέτουν σχέδια επικοινωνίας που καθιστούν δυνατή την υπεύθυνη γνωστοποίηση ***τουλάχιστον των σημαντικών*** συμβάντων που σχετίζονται με τις ΤΠΕ ή σημαντικών ευπαθειών σε πελάτες και αντισυμβαλλομένους, καθώς και στο κοινό, ανάλογα με την περίπτωση.

Τα σχέδια επικοινωνίας που αναφέρονται στο πρώτο εδάφιο διασφαλίζουν επίσης τη γνωστοποίηση στους πελάτες και τους αντισυμβαλλομένους, σε ετήσια βάση, σύνοψης όλων των συμβάντων που σχετίζονται με τις ΤΠΕ. Η γνωστοποίηση αυτή σέβεται πλήρως το επιχειρηματικό απόρρητο της χρηματοπιστωτικής οντότητας και

των πελατών και των αντισυμβαλλομένων της και δεν θέτει σε κίνδυνο το πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 5 παράγραφος 1.

2. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 5 παράγραφος 1, οι χρηματοπιστωτικές οντότητες εφαρμόζουν πολιτικές επικοινωνίας που απευθύνονται στο προσωπικό και σε εξωτερικά ενδιαφερόμενα μέρη. Στις πολιτικές επικοινωνίας για το προσωπικό λαμβάνεται υπόψη η ανάγκη διαχωρισμού μεταξύ, αφενός, του προσωπικού που συμμετέχει στη διαχείριση κινδύνων ΤΠΕ, ιδίως όσον αφορά την αντιμετώπιση και την αποκατάσταση, και, αφετέρου, του προσωπικού που πρέπει να ενημερωθεί.

3. Η αρμοδιότητα της εφαρμογής της στρατηγικής επικοινωνίας για ***τουλάχιστον τα σημαντικά*** συμβάντα που σχετίζονται με τις ΤΠΕ ανατίθεται τουλάχιστον σε ένα πρόσωπο της οντότητας, το οποίο θα λειτουργεί ως εκπρόσωπος Τύπου για τον σκοπό αυτόν.

Άρθρο 14

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

Η Ευρωπαϊκή Αρχή Τραπεζών (ΕΒΑ), η Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών (ESMA) και η Ευρωπαϊκή Αρχή Ασφαλίσεων και Επαγγελματικών Συντάξεων (EIOPA), σε συνεννόηση με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), καταρτίζουν σχέδια ρυθμιστικών τεχνικών προτύπων για τους ακόλουθους σκοπούς:

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 8 παράγραφος 2, ώστε να διασφαλίζεται η ασφάλεια των δικτύων, να παρέχεται η δυνατότητα επαρκών διασφαλίσεων έναντι εισβολών και κατάχρησης δεδομένων, να διατηρείται η γνησιότητα και η ακεραιότητα των δεδομένων, συμπεριλαμβανομένων των τεχνικών κρυπτογράφησης, και να εξασφαλίζεται η ακριβής και έγκαιρη διαβίβαση δεδομένων χωρίς σημαντικές διαταραχές ***και περιττές καθυστερήσεις***·

δ) να αναπτύξουν περαιτέρω συνιστώσες των ελέγχων διαχείρισης δικαιωμάτων πρόσβασης, που αναφέρονται στο άρθρο 8 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 αντικανονικών 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·

ε) να αναπτύξουν περαιτέρω τα στοιχεία που προσδιορίζονται στο άρθρο 9 παράγραφος 1, παρέχοντας τη δυνατότητα έγκαιρου εντοπισμού αντικανονικών δραστηριοτήτων, και τα κριτήρια που αναφέρονται στο άρθρο 9 παράγραφος 2 και ενεργοποιώντας διαδικασίες εντοπισμού και αντιμετώπισης συμβάντων που σχετίζονται με τις ΤΠΕ·

στ) να προσδιορίσουν περαιτέρω τις συνιστώσες της πολιτικής αδιάλειπτης λειτουργίας των ΤΠΕ που αναφέρεται στο άρθρο 10 παράγραφος 1·

ζ) να προσδιορίσουν περαιτέρω τις δοκιμές των σχεδίων αδιάλειπτης λειτουργίας των ΤΠΕ που αναφέρονται στο άρθρο 10 παράγραφος 5, με σκοπό να διασφαλίζεται ότι 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·

η) να προσδιορίσουν περαιτέρω τις συνιστώσες του σχεδίου αποκατάστασης λειτουργίας των ΤΠΕ μετά από καταστροφή που αναφέρεται στο άρθρο 10 παράγραφος 3.

Η ΕΒΑ, η ESMA και η ΕΙΟΡΑ υποβάλλουν στην Επιτροπή τα εν λόγω σχέδια ρυθμιστικών τεχνικών προτύπων έως τις [ΕΕ: Να συμπληρωθεί ημερομηνία 1 έτος μετά την ημερομηνία έναρξης ισχύος].

Ανατίθεται στην Επιτροπή η εξουσία να εγκρίνει 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, αντίστοιχα.

Άρθρο 14α

Πλαίσιο διαχείρισης κινδύνων ΤΠΕ για μικρές, μη διασυνδεδεμένες και εξαιρούμενες οντότητες

1. Σύμφωνα με το άρθρο 3α, οι μικρές και μη διασυνδεδεμένες επιχειρήσεις επενδύσεων, τα ιδρύματα πληρωμών που εξαιρούνται από την οδηγία (ΕΕ) 2015/2366, τα πιστωτικά ιδρύματα που εξαιρούνται από την οδηγία 2013/36/ΕΕ, τα ιδρύματα ηλεκτρονικού χρήματος που εξαιρούνται από την οδηγία 2009/110/ΕΚ και τα μικρά ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών δημιουργούν και διατηρούν ένα υγιές και τεκμηριωμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ, το οποίο:

α) περιγράφει λεπτομερώς τους μηχανισμούς και τα μέτρα που αποσκοπούν στη γρήγορη, αποτελεσματική και ολοκληρωμένη διαχείριση όλων των κινδύνων ΤΠΕ, συμπεριλαμβανομένης της προστασίας των σχετικών υλικών συνιστωσών και υποδομών·

β) παρακολουθεί συνεχώς την ασφάλεια και τη λειτουργία όλων των συστημάτων ΤΠΕ·

γ) ελαχιστοποιεί τον αντίκτυπο των κινδύνων ΤΠΕ μέσω της χρήσης υγιών, ανθεκτικών και επικαιροποιημένων συστημάτων, πρωτοκόλλων και εργαλείων ΤΠΕ που είναι κατάλληλα για την υποστήριξη της απόδοσης των δραστηριοτήτων τους και της παροχής υπηρεσιών·

δ) προστατεύει επαρκώς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δικτυακών και πληροφοριακών συστημάτων δεδομένων·

ε) επιτρέπει τον άμεσο εντοπισμό και την ανίχνευση πηγών κινδύνου και ανωμαλιών στα δικτυακά και πληροφοριακά συστήματα και τον γρήγορο χειρισμό συμβάντων ΤΠΕ.

2. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στην παράγραφο 1

τεκμηριώνεται και επανεξετάζεται τουλάχιστον μία φορά ετησίως, καθώς και κατά την επέλευση σημαντικών 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 σε ετήσια βάση.

ΚΕΦΑΛΑΙΟ III

ΣΥΜΒΑΝΤΑ ΠΟΥ ΣΧΕΤΙΖΟΝΤΑΙ ΜΕ ΤΙΣ ΤΠΕ

ΔΙΑΧΕΙΡΙΣΗ, ΤΑΞΙΝΟΜΗΣΗ ΚΑΙ ΑΝΑΦΟΡΑ

Άρθρο 15

Διαδικασία διαχείρισης συμβάντων που σχετίζονται με τις ΤΠΕ

1. Οι χρηματοπιστωτικές οντότητες 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 και καθορίζουν δείκτες έγκαιρης προειδοποίησης που λειτουργούν ως συναγερμικές ειδοποιήσεις.

2. Οι χρηματοπιστωτικές 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 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) καθιερώνει διαδικασίες για τον προσδιορισμό, την ανίχνευση, την καταγραφή, την κατηγοριοποίηση και την ταξινόμηση συμβάντων που σχετίζονται με τις ΤΠΕ ανάλογα με την προτεραιότητά τους και τη σοβαρότητα και την κρισιμότητα των υπηρεσιών που επηρεάζονται, σύμφωνα με τα κριτήρια που αναφέρονται στο άρθρο 16 παράγραφος 1·

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

   γ) καθορίζει σχέδια για την επικοινωνία με το προσωπικό, τα εξωτερικά ενδιαφερόμενα μέρη και τα μέσα ενημέρωσης, σύμφωνα με το άρθρο 13, 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 χρηματοπιστωτικές οντότητες που ενεργούν ως αντισυμβαλλόμενοι, ανάλογα με την περίπτωση·

   δ) διασφαλίζει ότι ***τουλάχιστον*** τα σημαντικά συμβάντα που σχετίζονται με τις ΤΠΕ αναφέρονται στα αρμόδια ανώτερα διοικητικά στελέχη και ότι το διοικητικό όργανο τηρείται ενήμερο για τα εν λόγω σημαντικά συμβάντα, επεξηγώντας τις επιπτώσεις, την αντιμετώπιση και τους πρόσθετους ελέγχους που πρέπει να καθοριστούν ως αποτέλεσμα των σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ·

   ε) 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 16

Ταξινόμηση συμβάντων που σχετίζονται με τις ΤΠΕ

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

   α) τον αριθμό των χρηστών ή των χρηματοπιστωτικών αντισυμβαλλομένων οι οποίοι επηρεάζονται από τη διαταραχή που προκλήθηκε από το συμβάν που σχετίζεται με τις ΤΠΕ ▌·

   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, όπως απώλεια της ακεραιότητας, απώλεια της εμπιστευτικότητας ή απώλεια της διαθεσιμότητας·

   ε) τη σοβαρότητα των επιπτώσεων του συμβάντος που σχετίζεται με τις ΤΠΕ στα συστήματα ΤΠΕ της χρηματοπιστωτικής οντότητας·

   στ) την κρισιμότητα των επηρεαζόμενων υπηρεσιών, συμπεριλαμβανομένων των συναλλαγών και των δραστηριοτήτων της χρηματοπιστωτικής οντότητας·

   ζ) τις οικονομικές επιπτώσεις του συμβάντος που σχετίζεται με τις ΤΠΕ σε απόλυτους και σχετικούς όρους.

2. Οι ΕΕΑ, μέσω της μεικτής επιτροπής των ΕΕΑ (στο εξής: μεικτή επιτροπή) και ***σε συντονισμό*** με την Ευρωπαϊκή Κεντρική Τράπεζα (ΕΚΤ) και τον ENISA, αναπτύσσουν 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 σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ, τα οποία υπόκεινται στην υποχρέωση αναφοράς που προβλέπεται στο άρθρο 17 παράγραφος 1·

   β) τα κριτήρια που πρέπει να εφαρμόζουν οι αρμόδιες αρχές για την αξιολόγηση της συνάφειας των σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ με τις δικαιοδοσίες άλλων κρατών μελών, καθώς και τα στοιχεία των αναφορών ***σημαντικών*** συμβάντων που σχετίζονται με τις ΤΠΕ τα οποία πρέπει να κοινοποιούνται σε άλλες αρμόδιες αρχές σύμφωνα με τα σημεία 5) και 6) του άρθρου 17.

3. Κατά την κατάρτιση των κοινών σχεδίων ρυθμιστικών τεχνικών προτύπων που αναφέρονται στην παράγραφο 2, οι ΕΕΑ λαμβάνουν υπόψη τα διεθνή πρότυπα, καθώς και τις προδιαγραφές που αναπτύσσει και δημοσιεύει ο ENISA, συμπεριλαμβανομένων, κατά περίπτωση, των προδιαγραφών που ισχύουν για άλλους οικονομικούς τομείς. ***Οι ΕΕΑ λαμβάνουν επίσης υπόψη ότι η έγκαιρη και αποτελεσματική διαχείριση ενός συμβάντος από μικρές και πολύ μικρές επιχειρήσεις δεν περιορίζεται από την ανάγκη τήρησης των απαιτήσεων ταξινόμησης που ορίζονται στο παρόν άρθρο. Οι ΕΕΑ λαμβάνουν υπόψη το μέγεθος των***

χρηματοπιστωτικών οντοτήτων, τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών τους, καθώς και το συνολικό προφίλ κινδύνου τους.

Οι ΕΕΑ υποβάλλουν στην Επιτροπή τα εν λόγω κοινά σχέδια ρυθμιστικών τεχνικών προτύπων έως τη(ν) [Υπηρεσία Εκδόσεων: Να συμπληρωθεί ημερομηνία ***2 έτη*** μετά την ημερομηνία έναρξης ισχύος].

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στην παράγραφο 2, σύμφωνα με τα άρθρα 10 έως 14 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010, αντίστοιχα.

Άρθρο 17

Αναφορά σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ

1. Οι χρηματοπιστωτικές οντότητες αναφέρουν στην αρμόδια αρχή σημαντικά συμβάντα που σχετίζονται με τις ΤΠΕ, όπως ορίζεται στο άρθρο 41, εντός των προθεσμιών που προβλέπονται στην παράγραφο 3.

   Για τους σκοπούς του πρώτου εδαφίου, οι χρηματοπιστωτικές οντότητες, αφού συλλέξουν και αναλύσουν όλες τις σχετικές πληροφορίες, καταρτίζουν αναφορά συμβάντος, χρησιμοποιώντας το υπόδειγμα που αναφέρεται στο άρθρο 18, και την υποβάλλουν στην αρμόδια αρχή.

   Η αναφορά περιλαμβάνει όλες τις απαραίτητες πληροφορίες προκειμένου η αρμόδια αρχή να είναι σε θέση να προσδιορίσει τη σημασία του σημαντικού συμβάντος που σχετίζεται με τις ΤΠΕ και να προβεί σε εκτίμηση των πιθανών διασυνοριακών επιπτώσεων.

1α. Οι χρηματοπιστωτικές οντότητες μπορούν, σε εθελοντική βάση, να γνωστοποιούν σημαντικές κυβερνοαπειλές στη σχετική αρμόδια αρχή όταν θεωρούν ότι η απειλή είναι σημαντική για το χρηματοπιστωτικό σύστημα, τους χρήστες υπηρεσιών ή τους πελάτες. Η σχετική αρμόδια αρχή μπορεί να παρέχει τις πληροφορίες αυτές σε άλλες σχετικές αρχές σύμφωνα με την παράγραφο 5.

2. Όταν ***συμβαίνει*** ένα σημαντικό συμβάν που σχετίζεται με τις ΤΠΕ ***και*** έχει ***σημαντικές*** επιπτώσεις στα οικονομικά συμφέροντα των χρηστών και των πελατών της υπηρεσίας, οι χρηματοπιστωτικές οντότητες ενημερώνουν, χωρίς αδικαιολόγητη καθυστέρηση ***αφότου λαμβάνουν γνώστη του συμβάντος***, τους χρήστες και τους πελάτες της υπηρεσίας όσον αφορά το σημαντικό συμβάν που σχετίζεται με τις ΤΠΕ και τους ενημερώνουν ▌σχετικά με όλα τα ***βάσιμα*** μέτρα που έχουν ληφθεί για τον περιορισμό των αρνητικών επιπτώσεων του εν λόγω συμβάντος. ***Όταν δεν προκύπτει βλάβη στους χρήστες και τους πελάτες υπηρεσιών λόγω των αντιμέτρων που λαμβάνει η χρηματοπιστωτική οντότητα, δεν ισχύει η απαίτηση ενημέρωσης των χρηστών και των πελατών της υπηρεσίας.***

3. Οι χρηματοπιστωτικές οντότητες υποβάλλουν στην αρμόδια αρχή, όπως αναφέρεται στο άρθρο 41:

   α) αρχική κοινοποίηση ▌του σημαντικού συμβάντος που σχετίζεται με τις ΤΠΕ***, η οποία περιέχει τις πληροφορίες που έχει στη διάθεσή της η κοινοποιούσα***

οντότητα με τη μέγιστη δυνατή επιμέλεια, ως εξής:

i) όσον αφορά συμβάντα που διαταράσσουν σημαντικά τη διαθεσιμότητα των υπηρεσιών που παρέχει η χρηματοπιστωτική οντότητα, η αρμόδια αρχή ειδοποιείται χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που η οντότητα λαμβάνει γνώση του συμβάντος·

ii) όσον αφορά συμβάντα που έχουν σημαντικό αντίκτυπο στη χρηματοπιστωτική οντότητα πέραν της διαθεσιμότητας των υπηρεσιών που παρέχει η εν λόγω χρηματοπιστωτική οντότητα, η αρμόδια αρχή ενημερώνεται χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 72 ωρών από τη στιγμή που η οντότητα λαμβάνει γνώση του συμβάντος·

iii) αφορά συμβάντα που έχουν αντίκτυπο στην ακεραιότητα, την εμπιστευτικότητα ή την ασφάλεια των δεδομένων προσωπικού χαρακτήρα που διατηρεί η εν λόγω χρηματοπιστωτική οντότητα, η αρμόδια αρχή ειδοποιείται χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που η οντότητα λαμβάνει γνώση του συμβάντος·

β) ενδιάμεση έκθεση, ***αμέσως μόλις μεταβληθεί σημαντικά η κατάσταση του αρχικού συμβάντος ή όταν έλθουν στο φως νέες πληροφορίες που θα μπορούσαν να έχουν σημαντικό αντίκτυπο στον τρόπο με τον οποίο αντιμετωπίζεται από την αρμόδια αρχή το σχετίζεται με τις ΤΠΕ***, μετά την αρχική κοινοποίηση που αναφέρεται στο στοιχείο α), συνοδευόμενη, κατά περίπτωση, από επικαιροποιημένες κοινοποιήσεις κάθε φορά που διατίθεται σχετική επικαιροποίηση της κατάστασης, καθώς και κατόπιν συγκεκριμένου αιτήματος της αρμόδιας αρχής·

γ) τελική έκθεση, όταν ολοκληρωθεί η ανάλυση των βαθύτερων αιτίων, ανεξάρτητα από το αν έχουν ήδη εφαρμοστεί μέτρα μετριασμού ή όχι, και όταν είναι διαθέσιμα τα στοιχεία των πραγματικών επιπτώσεων προς αντικατάσταση των εκτιμήσεων, αλλά το αργότερο έναν μήνα από την ***ημερομηνία αποστολής*** της αρχικής έκθεσης·

γα) σε περίπτωση συμβάντος που εξακολουθεί να είναι σε εξέλιξη κατά τον χρόνο υποβολής της λεπτομερούς έκθεσης σύμφωνα με το στοιχείο γ), υποβάλλεται τελική έκθεση έναν μήνα μετά την επίλυση του συμβάντος.

Η σχετική αρμόδια αρχή που αναφέρεται στο άρθρο 41 προβλέπει ότι, σε δεόντως αιτιολογημένες περιπτώσεις, επιτρέπεται σε μια χρηματοπιστωτική οντότητα να παρεκκλίνει από τις προθεσμίες που ορίζονται στα στοιχεία α), β), γ) και γα) της παρούσας παραγράφου, λαμβάνοντας δεόντως υπόψη την ικανότητα των χρηματοπιστωτικών οντοτήτων να παρέχουν ακριβείς και ουσιαστικές πληροφορίες σε σχέση με σημαντικά συμβάντα που σχετίζονται με τις ΤΠΕ.

4. Οι χρηματοπιστωτικές οντότητες δύνανται να αναθέτουν σε τρίτους παρόχους υπηρεσιών τις υποχρεώσεις αναφοράς που προβλέπονται στο παρόν άρθρο μόνον κατόπιν έγκρισης από τη σχετική αρμόδια αρχή που αναφέρεται στο άρθρο 41. ***Στις περιπτώσεις παρόμοιας ανάθεσης, η χρηματοπιστωτική οντότητα θα παραμένει εξ ολοκλήρου υπεύθυνη για την εκπλήρωση των απαιτήσεων αναφοράς συμβάντων.***

5. Μετά την παραλαβή της έκθεσης που προβλέπεται στην παράγραφο 1, η αρμόδια αρχή παρέχει, χωρίς αδικαιολόγητη καθυστέρηση, τις λεπτομέρειες του ***σημαντικού*** συμβάντος ***που σχετίζεται με τις ΤΠΕ***:

α) στην ΕΒΑ, στην ESMA ή στην ΕΙΟΡΑ, ανάλογα με την περίπτωση·

β) στην ΕΚΤ, εάν κρίνεται σκόπιμο, στην περίπτωση χρηματοπιστωτικών οντοτήτων που αναφέρονται στα στοιχεία α), β) και γ) του άρθρου 2 παράγραφος 1· και

γ) στο ενιαίο κέντρο επαφής που ορίζεται σύμφωνα με το άρθρο 8 της οδηγίας (ΕΕ) 2016/1148 ***ή στις CSIRT που ορίζονται βάσει του άρθρου 9 της οδηγίας (ΕΕ) 2016/1149***·

γα) στην αρχή εξυγίανσης που είναι υπεύθυνη για τη σχετική χρηματοπιστωτική οντότητα. Στο Ενιαίο Συμβούλιο Εξυγίανσης (ΕΣΕ) όσον αφορά τις οντότητες που αναφέρονται στο άρθρο 7 παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 806/2014, και για τις οντότητες και τους ομίλους που αναφέρονται στο άρθρο 7 παράγραφος 4 στοιχείο β) και παράγραφος 5 του κανονισμού (ΕΕ) αριθ. 806/2014, εφόσον πληρούνται οι προϋποθέσεις για την εφαρμογή των εν λόγω παραγράφων·

γβ) Στις εθνικές αρχές εξυγίανσης όσον αφορά οντότητες και ομάδες που αναφέρονται στο άρθρο 7 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 806/2014. Οι εθνικές αρχές εξυγίανσης παρέχουν στο ΕΣΕ, σε τριμηνιαία βάση, σύνοψη των εκθέσεων που έχουν λάβει βάσει του παρόντος σημείου σε σχέση με τις οντότητες και τους ομίλους που αναφέρονται στο άρθρο 7 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 806/2014·

γγ) σε άλλες αρμόδιες δημόσιες αρχές, συμπεριλαμβανομένων των αρχών άλλων κρατών μελών.

6. Η ΕΒΑ, η ESMA ή η ΕΙΟΡΑ και η ΕΚΤ***, σε συνεργασία με τον ENISA,*** αξιολογούν τη συνάφεια του σημαντικού συμβάντος που σχετίζεται με τις ΤΠΕ με άλλες αρμόδιες δημόσιες αρχές και τις ενημερώνουν σχετικά το συντομότερο δυνατόν. 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 χρηματοπιστωτικού συστήματος.

Άρθρο 18

Εναρμόνιση του περιεχομένου και των υποδειγμάτων των αναφορών

1. Οι ΕΕΑ, μέσω της μεικτής επιτροπής και κατόπιν διαβούλευσης με τον ENISA και την ΕΚΤ, καταρτίζουν:

α) κοινά σχέδια ρυθμιστικών τεχνικών προτύπων προκειμένου:

(1) να καθορίσουν το περιεχόμενο των αναφορών για σημαντικά συμβάντα που σχετίζονται με τις ΤΠΕ·

(2) να διευκρινίσουν περαιτέρω τους όρους υπό τους οποίους οι

χρηματοπιστωτικές οντότητες δύνανται να αναθέτουν σε τρίτο πάροχο υπηρεσιών, κατόπιν πρότερης έγκρισης από την αρμόδια αρχή, τις υποχρεώσεις αναφοράς που προβλέπονται στο παρόν κεφάλαιο·

(3) να προσδιορίσουν περαιτέρω τα κριτήρια για τον προσδιορισμό του αντικτύπου σημαντικού συμβάντος που σχετίζεται με τις ΤΠΕ σε χρηματοπιστωτική οντότητα για τους σκοπούς του άρθρου 17 παράγραφος 3 στοιχείο α).

β) κοινά σχέδια εκτελεστικών τεχνικών προτύπων με σκοπό τη δημιουργία τυποποιημένων εντύπων, υποδειγμάτων και διαδικασιών για την αναφορά σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ από τις χρηματοπιστωτικές οντότητες.

Οι ΕΕΑ υποβάλλουν στην Επιτροπή τα κοινά σχέδια ρυθμιστικών τεχνικών προτύπων που αναφέρονται ***στο*** στοιχείο α) ***του πρώτου εδαφίου*** και τα κοινά σχέδια εκτελεστικών τεχνικών προτύπων που αναφέρονται ***στο*** στοιχείο β) ***του δεύτερου εδαφίου*** έως τον xx του 202x [Υπηρεσία Εκδόσεων: Να συμπληρωθεί ημερομηνία ***2*** έτη μετά την ημερομηνία έναρξης ισχύος].

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

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

2. Εν αναμονή του αποτελέσματος της έκθεσης σκοπιμότητας που αναφέρεται στο άρθρο 19 σχετικά με την περαιτέρω συγκέντρωση της αναφοράς συμβάντων, οι ΕΕΑ, μέσω της Μεικτής Επιτροπής και σε συνεργασία με τις αρμόδιες αρχές, την ΕΚΤ, το SRB και τον ENISA, καταρτίζουν κατευθυντήριες γραμμές για την ανταλλαγή πληροφοριών σχετικά με τις αναφορές σοβαρών συμβάντων που σχετίζονται με τις ΤΠΕ σύμφωνα με το άρθρο 17 παράγραφος 5.

Οι κατευθυντήριες γραμμές που αναφέρονται στο πρώτο εδάφιο εξετάζουν τουλάχιστον τα ακόλουθα:

α) τις αποτελεσματικότερες γραμμές επικοινωνίας·

β) τη διατήρηση της ασφάλειας, της εμπιστευτικότητας και της ακεραιότητας των ανταλλασσόμενων δεδομένων·

γ) την πιθανή συμμετοχή χρηματοπιστωτικών οντοτήτων για τη συμπλήρωση της ανταλλαγής πληροφοριών που αναφέρεται στο άρθρο 40.

Άρθρο 19

Κεντρική διαχείριση της αναφοράς σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ

1. Οι ΕΕΑ, μέσω της μεικτής επιτροπής και κατόπιν διαβούλευσης 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 σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ από τις χρηματοπιστωτικές οντότητες. Στην 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 έκθεση που αναφέρεται στην παράγραφο 1 περιλαμβάνονται τουλάχιστον τα εξής στοιχεία:

α) προϋποθέσεις για τη δημιουργία ***ενιαίου*** κόμβου της ΕΕ·

β) οφέλη, περιορισμοί και πιθανοί κίνδυνοι·

βα) ικανότητα καθιέρωσης της διαλειτουργικότητας και εκτίμησης της προστιθέμενης αξίας της σε σχέση με άλλα σχετικά συστήματα αναφοράς, συμπεριλαμβανομένης της οδηγίας (ΕΕ) 2016/1148.

γ) στοιχεία λειτουργικής διαχείρισης·

δ) όροι συμμετοχής·

ε) λεπτομέρειες όσον αφορά την πρόσβαση των χρηματοπιστωτικών οντοτήτων και των εθνικών αρμόδιων αρχών στον ***ενιαίο*** κόμβο της ΕΕ·

στ) προκαταρκτική αξιολόγηση του οικονομικού κόστους που συνεπάγεται η σύσταση της επιχειρησιακής πλατφόρμας για την υποστήριξη του ***ενιαίου*** κόμβου της ΕΕ, συμπεριλαμβανομένης της απαιτούμενης εμπειρογνωσίας.

3. Οι ΕΕΑ υποβάλλουν στην Επιτροπή, στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο την έκθεση που αναφέρεται στην παράγραφο 1 έως τον xx του 202x [ΕΕ: Να συμπληρωθεί ημερομηνία 3 έτη μετά την ημερομηνία έναρξης ισχύος].

Άρθρο 20

Σχόλια και παρατηρήσεις των εποπτικών αρχών

1. Με την παραλαβή της αναφοράς που προβλέπεται στο άρθρο 17 παράγραφος 1, η αρμόδια αρχή επιβεβαιώνει την παραλαβή της κοινοποίησης και παρέχει το συντομότερο δυνατόν στη χρηματοπιστωτική οντότητα όλα τα απαραίτητα σχόλια και παρατηρήσεις ή καθοδήγηση, ιδίως για να συζητηθούν διορθωτικά μέτρα στο επίπεδο της οντότητας ή τρόποι για την ελαχιστοποίηση των αρνητικών επιπτώσεων στους διάφορους τομείς ***και επίσης παρέχει κατάλληλα ανωνυμοποιημένα σχόλια και πληροφορίες σε όλες τις σχετικές χρηματοπιστωτικές οντότητες, όπου θα μπορούσε αυτό να είναι επωφελές, βάσει οποιωνδήποτε αναφορών σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ τα οποία λαμβάνουν***.

2. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, υποβάλλουν ετησίως έκθεση σε ανωνυμοποιημένη και συγκεντρωτική βάση σχετικά με τις κοινοποιήσεις ***αναφοράς σημαντικών*** συμβάντων που σχετίζονται με τις ΤΠΕ τις οποίες λαμβάνουν από τις αρμόδιες αρχές, αναφέροντας τουλάχιστον τον αριθμό των σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ, τη φύση τους, τις επιπτώσεις τους στις δραστηριότητες των χρηματοπιστωτικών οντοτήτων ή των πελατών, το ***εκτιμώμενο*** κόστος και τα διορθωτικά μέτρα που έχουν ληφθεί.

Οι ΕΕΑ εκδίδουν προειδοποιήσεις και παράγουν στατιστικά στοιχεία υψηλού επιπέδου

προς επίρρωση των αξιολογήσεων των απειλών και των ευπαθειών για τις ΤΠΕ.

Άρθρο 20α

Επιχειρησιακά συμβάντα ή συμβάντα ασφάλειας πληρωμών που αφορούν ορισμένες χρηματοπιστωτικές οντότητες

Οι απαιτήσεις που ορίζονται στο παρόν κεφάλαιο ισχύουν επίσης για επιχειρησιακά συμβάντα ή συμβάντα ασφαλείας που σχετίζονται με πληρωμές και για σημαντικά επιχειρησιακά συμβάντα ή συμβάντα ασφαλείας που σχετίζονται με πληρωμές, όταν αφορούν χρηματοπιστωτικές οντότητες που αναφέρονται στα στοιχεία α), β) και γ) του άρθρου 2 παράγραφος 1.

ΚΕΦΑΛΑΙΟ IV

ΔΟΚΙΜΕΣ ΨΗΦΙΑΚΗΣ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΑΝΘΕΚΤΙΚΟΤΗΤΑΣ

Άρθρο 21

Γενικές απαιτήσεις για τη διενέργεια δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας

1. Για τους σκοπούς της αξιολόγησης της ετοιμότητας όσον αφορά συμβάντα που σχετίζονται με τις ΤΠΕ, του εντοπισμού αδυναμιών, ελλείψεων ή κενών στην ψηφιακή επιχειρησιακή ανθεκτικότητα, καθώς και της άμεσης εφαρμογής διορθωτικών μέτρων, οι χρηματοπιστωτικές οντότητες***, πλην των πολύ μικρών επιχειρήσεων,*** 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 5.

2. Το πρόγραμμα δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας περιλαμβάνει σειρά αξιολογήσεων, δοκιμών, μεθοδολογιών, πρακτικών και εργαλείων που πρέπει να εφαρμόζονται σύμφωνα με τις διατάξεις των άρθρων 22 και 23.

3. Οι χρηματοπιστωτικές οντότητες εφαρμόζουν προσέγγιση βάσει κινδύνων κατά τη εκπόνηση του προγράμματος δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας που αναφέρεται στην παράγραφο 1, λαμβάνοντας υπόψη το εξελισσόμενο τοπίο των κινδύνων ΤΠΕ, τυχόν ειδικούς κινδύνους στους οποίους εκτίθεται ή ενδέχεται να εκτεθεί η χρηματοπιστωτική οντότητα, την κρισιμότητα των πληροφοριακών πόρων και των παρεχόμενων υπηρεσιών, καθώς και κάθε άλλο παράγοντα τον οποίο κρίνει κατάλληλο η χρηματοπιστωτική οντότητα.

4. Οι χρηματοπιστωτικές οντότητες διασφαλίζουν ότι οι δοκιμές πραγματοποιούνται από ανεξάρτητους φορείς, εσωτερικούς ή εξωτερικούς. ***Όταν διενεργούνται δοκιμές από εσωτερικό φορέα δοκιμών, οι χρηματοπιστωτικές οντότητες διαθέτουν επαρκείς πόρους και διασφαλίζουν την αποφυγή συγκρούσεων συμφερόντων καθ' όλη τη διάρκεια των φάσεων σχεδιασμού και εκτέλεσης της δοκιμής.***

5. Οι χρηματοπιστωτικές οντότητες θεσπίζουν διαδικασίες και πολιτικές για την ιεράρχηση, την ταξινόμηση και την ***αντιμετώπιση*** όλων των ζητημάτων που αναγνωρίζονται κατά τη διάρκεια της διενέργειας 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 χρηματοπιστωτικές οντότητες ***διασφαλίζουν ότι διενεργούνται κατάλληλες δοκιμές σε*** όλα τα κρίσιμα συστήματα και εφαρμογές ΤΠΕ, τουλάχιστον ετησίως.

Άρθρο 22

Δοκιμές των εργαλείων και συστημάτων ΤΠΕ

1. Το πρόγραμμα δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας που αναφέρεται στο άρθρο 21 προβλέπει τη διενέργεια πλήρους φάσματος κατάλληλων δοκιμών.

Οι εν λόγω δοκιμές μπορεί να περιλαμβάνουν αξιολογήσεις και ελέγχους ευπαθειών, αναλύσεις ανοικτού κώδικα, αξιολογήσεις ασφάλειας δικτύου, αναλύσεις ελλείψεων, ελέγχους φυσικής ασφάλειας, ερωτηματολόγια και λύσεις λογισμικού σάρωσης, ελέγχους πηγαίου κώδικα, εφόσον είναι εφικτό, δοκιμές βάσει σεναρίων, δοκιμές συμβατότητας, δοκιμές επιδόσεων, διατερματικές δοκιμές ή δοκιμές διείσδυσης.

2. Οι χρηματοπιστωτικές οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 στοιχεία στ) και ζ) διενεργούν αξιολογήσεις ευπαθειών πριν από την ανάπτυξη ή αναδιάταξη νέων ή υφιστάμενων υπηρεσιών που υποστηρίζουν κρίσιμες λειτουργίες, εφαρμογές και στοιχεία της υποδομής της χρηματοπιστωτικής οντότητας.

Άρθρο 23

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

1. Οι χρηματοπιστωτικές οντότητες που προσδιορίζονται ***στο δεύτερο εδάφιο της παραγράφου 3*** πραγματοποιούν τουλάχιστον ανά 3 έτη προηγμένες δοκιμές μέσω δοκιμών διείσδυσης βάσει απειλών.

2. Οι δοκιμές διείσδυσης βάσει απειλών καλύπτουν τουλάχιστον τις κρίσιμες ***ή σημαντικές*** λειτουργίες και υπηρεσίες μιας χρηματοπιστωτικής οντότητας και διενεργούνται σε συστήματα ζωντανής παραγωγής που υποστηρίζουν τις εν λόγω λειτουργίες***, εφόσον είναι δυνατόν, ή σε συστήματα προπαραγωγής με την ίδια διαμόρφωση όσον αφορά την ασφάλεια***. Το ακριβές εύρος των δοκιμών διείσδυσης βάσει απειλών προσδιορίζεται από τις χρηματοπιστωτικές οντότητες με βάση την αξιολόγηση κρίσιμων ***ή σημαντικών*** λειτουργιών και υπηρεσιών και επικυρώνεται από τις αρμόδιες αρχές. ***Δεν υπάρχει η απαίτηση μία δοκιμή διείσδυσης βάσει απειλών να καλύπτει όλες τις κρίσιμες ή σημαντικές λειτουργίες***.

Για τους σκοπούς του πρώτου εδαφίου, οι χρηματοπιστωτικές οντότητες προσδιορίζουν όλες τις σχετικές υποκείμενες διαδικασίες, συστήματα και τεχνολογίες ΤΠΕ που υποστηρίζουν κρίσιμες ***ή σημαντικές*** λειτουργίες και υπηρεσίες, συμπεριλαμβανομένων των ***κρίσιμων ή σημαντικών*** λειτουργιών και υπηρεσιών που αποτελούν αντικείμενο εξωτερικής ανάθεσης ή υπεργολαβίας μέσω ρυθμίσεων σε τρίτους παρόχους υπηρεσιών ΤΠΕ.

Σε περίπτωση που στο πλαίσιο διενέργειας δοκιμών διείσδυσης βάσει απειλών περιλαμβάνονται τρίτοι πάροχοι ***κρίσιμων*** υπηρεσιών ΤΠΕ, ***και, όπου είναι αναγκαίο, τρίτοι πάροχοι μη κρίσιμων υπηρεσιών ΤΠΕ,*** η χρηματοπιστωτική οντότητα λαμβάνει τα απαραίτητα μέτρα για την εξασφάλιση της συμμετοχής των εν λόγω παρόχων. ***Οι εν λόγω τρίτοι πάροχοι υπηρεσιών ΤΠΕ δεν υποχρεούνται να κοινοποιούν πληροφορίες ή να παρέχουν λεπτομέρειες σχετικά με στοιχεία που δεν σχετίζονται με τους ελέγχους διαχείρισης κινδύνων των σχετικών κρίσιμων ή σημαντικών λειτουργιών των σχετικών χρηματοπιστωτικών οντοτήτων. Οι εν λόγω δοκιμές δεν επηρεάζουν δυσμενώς άλλους πελάτες των τρίτων παρόχων υπηρεσιών ΤΠΕ.***

Σε περιπτώσεις όπου η συμμετοχή ενός τρίτου παρόχου υπηρεσιών ΤΠΕ στη δοκιμή διείσδυσης βάσει απειλών θα μπορούσε δυνητικά να έχει αντίκτυπο στην ποιότητα, την εμπιστευτικότητα ή την ασφάλεια των υπηρεσιών τρίτου παρόχου υπηρεσιών ΤΠΕ σε άλλους πελάτες που δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού ή στη συνολική ακεραιότητα των δραστηριοτήτων του τρίτου παρόχου υπηρεσιών ΤΠΕ, η χρηματοπιστωτική οντότητα και ο τρίτος πάροχος υπηρεσιών ΤΠΕ μπορούν να συμφωνήσουν με σύμβαση ότι επιτρέπεται στον τρίτο πάροχο υπηρεσιών ΤΠΕ να συνάψει απευθείας συμβατικές ρυθμίσεις με εξωτερικό φορέα δοκιμών. Οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ μπορούν να συνάπτουν αυτές τις ρυθμίσεις εξ ονόματος όλων των χρηστών υπηρεσιών των χρηματοπιστωτικών

οντοτήτων τους προκειμένου να διενεργούν ομαδικές δοκιμές.

Οι χρηματοπιστωτικές οντότητες εφαρμόζουν αποτελεσματικούς ελέγχους διαχείρισης κινδύνων με σκοπό τον ***μετριασμό*** των κινδύνων όσον αφορά τις πιθανές επιπτώσεις στα δεδομένα, την πρόκλησης ζημίας στα περιουσιακά στοιχεία και τη διαταραχή κρίσιμων ***ή σημαντικών λειτουργιών*** ή δραστηριοτήτων της ίδιας της χρηματοπιστωτικής οντότητας, των αντισυμβαλλομένων της ή του χρηματοπιστωτικού τομέα.

Με την ολοκλήρωση της δοκιμής, αφού συμφωνηθούν οι εκθέσεις και τα σχέδια επανόρθωσης, η χρηματοπιστωτική οντότητα και οι εξωτερικοί φορείς δοκιμών παρέχουν στην ***ενιαία δημόσια αρχή που έχει οριστεί με την παράγραφο 3α, ή, στην περίπτωση τρίτων παρόχων υπηρεσιών ΤΠΕ που συνάπτουν απευθείας συμβατικές ρυθμίσεις απευθείας με εξωτερικούς φορείς δοκιμών, στον ENISA, εμπιστευτική σύνοψη των αποτελεσμάτων των δοκιμών και την*** τεκμηρίωση με την οποία βεβαιώνεται ότι η δοκιμή διείσδυσης βάσει απειλών διενεργήθηκε σύμφωνα με τις απαιτήσεις. ***Η ενιαία δημόσια αρχή ή ο ENISA, όπως αρμόζει, χορηγούν βεβαίωση που επιβεβαιώνει ότι η δοκιμή διενεργήθηκε σύμφωνα με τις απαιτήσεις που εκτίθενται στην τεκμηρίωση, προκειμένου να καταστεί δυνατή η αμοιβαία αναγνώριση των δοκιμών διείσδυσης βάσει απειλών μεταξύ των αρμόδιων αρχών. Η βεβαίωση κοινοποιείται στην αρμόδια αρχή της χρηματοπιστωτικής οντότητας και, κατά περίπτωση, στον κύριο εποπτικό φορέα του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ.***

3. Οι χρηματοπιστωτικές οντότητες***, ή οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ στους οποίους επιτρέπεται να συνάπτουν απευθείας συμβατικές ρυθμίσεις με εξωτερικό φορέα δοκιμών σύμφωνα με την παράγραφο 2 του παρόντος άρθρου,*** συνάπτουν συμβάσεις με φορείς δοκιμών σύμφωνα με το άρθρο 24 για τους σκοπούς της ανάληψης δοκιμών διείσδυσης βάσει απειλών.

Με την επιφύλαξη της ικανότητάς τους να αναθέτουν καθήκοντα και αρμοδιότητες δυνάμει του παρόντος άρθρου σε άλλες αρμόδιες αρχές, οι οποίες είναι υπεύθυνες για τις δοκιμές διείσδυσης βάσει απειλών, οι αρμόδιες αρχές προσδιορίζουν τις χρηματοπιστωτικές οντότητες που καλούνται να διενεργήσουν δοκιμές διείσδυσης βάσει απειλών κατά ***αναλογικό*** τρόπο ▌αξιολογώντας τα ακόλουθα:

α) παράγοντες που σχετίζονται με τις επιπτώσεις, ιδίως όσον αφορά την κρισιμότητα των παρεχόμενων υπηρεσιών και των δραστηριοτήτων που αναλαμβάνει η χρηματοπιστωτική οντότητα·

β) πιθανούς προβληματισμούς σχετικά με τη χρηματοπιστωτική σταθερότητα, συμπεριλαμβανομένου του συστημικού χαρακτήρα της χρηματοπιστωτικής οντότητας σε εθνικό ή ενωσιακό επίπεδο, ανάλογα με την περίπτωση·

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

3α. Τα κράτη μέλη ορίζουν ενιαία δημόσια αρχή υπεύθυνη για τις δοκιμές διείσδυσης βάσει απειλών στον χρηματοπιστωτικό τομέα σε εθνικό επίπεδο, με εξαίρεση τον προσδιορισμό των χρηματοπιστωτικών οντοτήτων σύμφωνα με την παράγραφο 3, συμπεριλαμβανομένων των δοκιμών διείσδυσης βάσει απειλών που διενεργούνται από χρηματοπιστωτικές οντότητες και από τρίτους παρόχους υπηρεσιών ΤΠΕ που συνάπτουν απευθείας συμβατικές ρυθμίσεις με εξωτερικούς φορείς δοκιμών. Στην

ορισθείσα ενιαία δημόσια αρχή ανατίθενται όλες οι αρμοδιότητες και τα καθήκοντα για τον σκοπό αυτό.

4. ***Οι ΕΕΑ, σε συντονισμό με τον ENISA,*** κατόπιν διαβούλευσης με την ΕΚΤ και λαμβάνοντας υπόψη τα σχετικά πλαίσια στην Ένωση που εφαρμόζονται σε δοκιμές διείσδυσης ***βάσει απειλών με βάση στοιχεία, συμπεριλαμβανομένου του πλαισίου TIBER-EU***, καταρτίζουν ***μια δέσμη σχεδίων*** ρυθμιστικών τεχνικών προτύπων για τον περαιτέρω προσδιορισμό:

α) των κριτηρίων που χρησιμοποιούνται για την εφαρμογή του δεύτερου εδαφίου της παραγράφου 3 του παρόντος άρθρου·

β) των απαιτήσεων σχετικά με:

i) το εύρος των δοκιμών διείσδυσης βάσει απειλών που αναφέρονται στην παράγραφο 2 του παρόντος άρθρου·

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 επανόρθωσης στο πλαίσιο της δοκιμής·

γ) το είδος της εποπτικής συνεργασίας που απαιτείται για την εφαρμογή ***και τη διευκόλυνση της πλήρους αμοιβαίας αναγνώρισης των*** δοκιμών διείσδυσης βάσει απειλών στο πλαίσιο των χρηματοπιστωτικών οντοτήτων που δραστηριοποιούνται σε περισσότερα από ένα κράτη μέλη ***και δοκιμών που διενεργούνται από εξωτερικούς φορείς δοκιμών που έχουν συνάψει απευθείας συμβατικές ρυθμίσεις με τρίτους παρόχους υπηρεσιών ΤΠΕ σύμφωνα με την παράγραφο 2 του παρόντος άρθρου***, ώστε να παρέχεται η δυνατότητα κατάλληλου επιπέδου εποπτικής συμμετοχής, καθώς και η δυνατότητα ευέλικτης εφαρμογής για την κάλυψη των ιδιαίτερων χαρακτηριστικών επιμέρους χρηματοπιστωτικών τομέων ή τοπικών χρηματοπιστωτικών αγορών.

Οι ΕΕΑ υποβάλλουν στην Επιτροπή τα εν λόγω σχέδια ρυθμιστικών τεχνικών προτύπων έως τη(ν) [ΕΕ: Να συμπληρωθεί ημερομηνία ***6*** μήνες μετά την ημερομηνία έναρξης ισχύος].

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

Άρθρο 24

Απαιτήσεις για φορείς δοκιμών

1. Οι χρηματοπιστωτικές οντότητες ***και οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ στους οποίους επιτρέπεται να συνάπτουν απευθείας συμβατικές ρυθμίσεις με εξωτερικό φορέα δοκιμών σύμφωνα με το άρθρο 23 παράγραφος 2,*** χρησιμοποιούν για την πραγματοποίηση δοκιμών διείσδυσης βάσει απειλών μόνο φορείς δοκιμών οι οποίοι:

α) είναι απολύτως κατάλληλοι και έγκριτοι·

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

γ) έχουν πιστοποίηση από οργανισμό διαπίστευσης κράτους μέλους ή τηρούν επίσημους κώδικες ή πλαίσια δεοντολογίας***, ανεξάρτητα από το αν οι φορείς δοκιμών προέρχονται από την Ένωση ή από τρίτη χώρα***·

δ) ▌παρέχουν ανεξάρτητη διαβεβαίωση ή έκθεση ελέγχου όσον αφορά την ορθή διαχείριση των κινδύνων που σχετίζονται με την εκτέλεση δοκιμών διείσδυσης βάσει απειλών, συμπεριλαμβανομένης της δέουσας προστασίας των εμπιστευτικών πληροφοριών της χρηματοπιστωτικής οντότητας και της αντιμετώπισης των επιχειρηματικών κινδύνων της χρηματοπιστωτικής οντότητας·

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

εα) στην περίπτωση εσωτερικών φορέων δοκιμών, η χρήση τους έχει εγκριθεί από τη σχετική αρμόδια αρχή και από την ενιαία δημόσια αρχή που έχει οριστεί σύμφωνα με το άρθρο 23 παράγραφος 3α, και οι εν λόγω αρχές έχουν επαληθεύσει ότι η χρηματοπιστωτική οντότητα διαθέτει επαρκείς πόρους και έχουν διασφαλίσει την αποφυγή συγκρούσεων συμφερόντων καθ' όλη τη διάρκεια των φάσεων σχεδιασμού και εκτέλεσης της δοκιμής.

2. Οι χρηματοπιστωτικές οντότητες ***και οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ στους οποίους επιτρέπεται να συνάπτουν απευθείας συμβατικές ρυθμίσεις με εξωτερικό φορέα δοκιμών σύμφωνα με το άρθρο 23 παράγραφος 2*** διασφαλίζουν ότι οι ***ρυθμίσεις*** που συνάπτονται με εξωτερικούς φορείς δοκιμών προϋποθέτουν την ορθή διαχείριση των αποτελεσμάτων των δοκιμών διείσδυσης βάσει απειλών και ότι οποιαδήποτε επεξεργασία τους, συμπεριλαμβανομένης τυχόν παραγωγής, σχεδίου, αποθήκευσης, συγκέντρωσης, αναφοράς, επικοινωνίας ή καταστροφής, δεν προκαλεί κινδύνους για τη χρηματοπιστωτική οντότητα.

ΚΕΦΑΛΑΙΟ V

ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΟΥ ΤΡΙΤΟΥ ΠΑΡΟΧΟΥ ΤΠΕ

ΤΜΗΜΑ I

ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΓΙΑ ΤΗ ΧΡΗΣΤΗ ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΟΥ ΤΡΙΤΩΝ ΠΑΡΟΧΩΝ ΤΠΕ

Άρθρο 25

Γενικές αρχές

Οι χρηματοπιστωτικές οντότητες διαχειρίζονται τον κίνδυνο τρίτων παρόχων ΤΠΕ ως αναπόσπαστο στοιχείο των κινδύνων ΤΠΕ εντός του πλαισίου διαχείρισης κινδύνων ΤΠΕ που εφαρμόζουν και σύμφωνα με τις ακόλουθες αρχές:

1. Οι χρηματοπιστωτικές 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 την ισχύουσα νομοθεσία για τις χρηματοπιστωτικές υπηρεσίες.

2. Η διαχείριση κινδύνου τρίτων παρόχων ΤΠΕ από τις χρηματοπιστωτικές οντότητες εφαρμόζεται βάσει της αρχής της αναλογικότητας, λαμβάνοντας υπόψη:

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

   β) 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 την ποιότητα των χρηματοπιστωτικών υπηρεσιών και δραστηριοτήτων, τόσο σε μεμονωμένο επίπεδο όσο και σε επίπεδο ομίλου,

   βα) εάν ένας πάροχος υπηρεσιών ΤΠΕ είναι ενδοομιλικός πάροχος υπηρεσιών ΤΠΕ.

3. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ, οι χρηματοπιστωτικές οντότητες***, πλην των πολύ μικρών επιχειρήσεων,*** εγκρίνουν και επανεξετάζουν τακτικά στρατηγική για τον κίνδυνο τρίτων παρόχων ΤΠΕ ▌. Η στρατηγική αυτή περιλαμβάνει την πολιτική για τη χρήση υπηρεσιών ΤΠΕ που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ και εφαρμόζεται σε μεμονωμένο επίπεδο και, ανάλογα με την περίπτωση, σε υποενοποιημένη και ενοποιημένη βάση. Το διοικητικό όργανο επανεξετάζει τακτικά τους κινδύνους που εντοπίζονται σε σχέση με την εξωτερική ανάθεση κρίσιμων ή σημαντικών λειτουργιών.

4. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ, οι χρηματοπιστωτικές 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 ***υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες, οι οποίες*** παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ.

Οι συμβατικές ρυθμίσεις που αναφέρονται στο πρώτο εδάφιο τεκμηριώνονται κατάλληλα ▌.

Εφόσον είναι διαθέσιμες, οι χρηματοπιστωτικές οντότητες ακολουθούν τις κατευθυντήριες γραμμές και άλλα μέτρα που εκδίδονται από τις ΕΕΑ και τις αρμόδιες αρχές έως την έναρξη ισχύος των εκτελεστικών τεχνικών προτύπων που αναφέρονται στην παράγραφο 10.

Οι χρηματοπιστωτικές οντότητες υποβάλλουν στις αρμόδιες αρχές, τουλάχιστον ετησίως, πληροφορίες σχετικά με τον αριθμό των νέων συμβατικών ρυθμίσεων για τη χρήση υπηρεσιών ΤΠΕ ***που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες***, τις κατηγορίες τρίτων παρόχων υπηρεσιών ΤΠΕ, το είδος των συμβατικών ρυθμίσεων και τις παρεχόμενες υπηρεσίες και λειτουργίες.

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

Οι χρηματοπιστωτικές οντότητες ενημερώνουν εγκαίρως την αρμόδια αρχή για την προγραμματισμένη σύναψη συμβάσεων παροχής κρίσιμων ή σημαντικών λειτουργιών, καθώς και για τη χρονική στιγμή κατά την οποία καθίσταται κρίσιμη ή σημαντική μια λειτουργία.

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

α) αξιολογούν αν η συμβατική ρύθμιση καλύπτει 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 των εν λόγω συμβατικών ρυθμίσεων στην ενίσχυση του κινδύνου συγκέντρωσης ΤΠΕ·

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.

6. Οι χρηματοπιστωτικές οντότητες μπορούν να συνάπτουν συμβατικές ρυθμίσεις μόνο με τρίτους παρόχους υπηρεσιών ΤΠΕ που συμμορφώνονται με υψηλά, κατάλληλα και ***επικαιροποιημένα*** πρότυπα ασφάλειας των πληροφοριών. ***Τα πλέον πρόσφατα πρότυπα λαμβάνονται επίσης υπόψη κατά τον προσδιορισμό του κατά πόσον τα ισχύοντα πρότυπα είναι κατάλληλα.***

7. Κατά την άσκηση των δικαιωμάτων πρόσβασης, επιθεώρησης και ελέγχου έναντι του τρίτου παρόχου υπηρεσιών ΤΠΕ ***σε σχέση με κρίσιμες ή σημαντικές λειτουργίες***, οι χρηματοπιστωτικές οντότητες προκαθορίζουν, σύμφωνα με 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.

Όσον αφορά τις συμβατικές ρυθμίσεις που συνεπάγονται ***λεπτομερή*** τεχνολογική πολυπλοκότητα, η χρηματοπιστωτική οντότητα εξακριβώνει αν οι ελεγκτές, είτε πρόκειται για εσωτερικούς ελεγκτές είτε για ομάδες ελεγκτών ή για εξωτερικούς ελεγκτές, διαθέτουν τις κατάλληλες δεξιότητες και γνώσεις για την αποτελεσματική διενέργεια σχετικών ελέγχων και αξιολογήσεων.

8. Οι χρηματοπιστωτικές οντότητες διασφαλίζουν ότι οι συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ ***επιτρέπουν στις χρηματοπιστωτικές οντότητες να λαμβάνουν κατάλληλα διορθωτικά μέτρα, τα οποία θα μπορούσαν να περιλαμβάνουν την πλήρη καταγγελία των ρυθμίσεων, εάν δεν είναι δυνατή η διόρθωση, ή τη μερική καταγγελία των ρυθμίσεων, εάν είναι δυνατή η διόρθωση, σύμφωνα με το εφαρμοστέο δίκαιο***, τουλάχιστον στις ακόλουθες περιπτώσεις:

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

αα) σύσταση που εκδίδεται από το όργανο κοινής εποπτείας με βάση το άρθρο 37 για έναν κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ·

β) συνθήκες που προσδιορίζονται καθ' όλη τη διάρκεια παρακολούθησης του κινδύνου τρίτων παρόχων ΤΠΕ και 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 κινδύνων ΤΠΕ ***της σύμβασής του με τη χρηματοπιστωτική οντότητα*** και ειδικότερα όσον αφορά τον τρόπο με τον οποίο διασφαλίζει την ασφάλεια και την ακεραιότητα εμπιστευτικών, προσωπικών ή άλλως ευαίσθητων δεδομένων ή μη προσωπικών πληροφοριών·

δ) συνθήκες κατά τις οποίες η αρμόδια αρχή ***αποδεδειγμένα*** δεν μπορεί πλέον να εποπτεύει αποτελεσματικά τη χρηματοπιστωτική οντότητα συνεπεία της αντίστοιχης συμβατικής ρύθμισης.

8α. Προκειμένου να μειωθεί ο κίνδυνος διαταραχών στο επίπεδο της χρηματοπιστωτικής οντότητας, σε δεόντως αιτιολογημένες περιστάσεις και σε συμφωνία με τις αρμόδιες αρχές τους, η χρηματοπιστωτική οντότητα μπορεί να αποφασίσει να μην καταγγείλει τις συμβατικές ρυθμίσεις με τον τρίτο πάροχο υπηρεσιών ΤΠΕ έως ότου μπορέσει να αλλάξει τρίτο πάροχο υπηρεσιών ΤΠΕ ή να καταφύγει στη χρήση λύσεων εντός της επιχείρησης, ανάλογα με την πολυπλοκότητα της παρεχόμενης υπηρεσίας, σύμφωνα με τη στρατηγική εξόδου που αναφέρεται στην παράγραφο 9.

8β. Σε περιπτώσεις κατά τις οποίες οι συμβατικές ρυθμίσεις με τρίτους παρόχους υπηρεσιών ΤΠΕ καταγγέλλονται υπό οποιαδήποτε από τις περιστάσεις που απαριθμούνται στην παράγραφο 8 στοιχεία α) έως δ), οι χρηματοπιστωτικές οντότητες δεν επωμίζονται το κόστος διαβίβασης δεδομένων από τρίτο πάροχο υπηρεσιών ΤΠΕ όταν η εν λόγω διαβίβαση υπερβαίνει το κόστος διαβίβασης δεδομένων που προβλέπεται στην αρχική σύμβαση.

9. ***Για τις υπηρεσίες ΤΠΕ που σχετίζονται με κρίσιμες ή σημαντικές λειτουργίες,*** οι χρηματοπιστωτικές οντότητες εφαρμόζουν στρατηγικές εξόδου***, οι οποίες επανεξετάζονται περιοδικά***. ***Οι στρατηγικές εξόδου*** λαμβάνουν υπόψη τους κινδύνους

που ενδέχεται να προκύψουν στο επίπεδο των τρίτων παρόχων υπηρεσιών ΤΠΕ, ιδίως όσον αφορά την πιθανότητα αθέτησης υποχρεώσεων εκ μέρους τους, την υποβάθμιση της ποιότητας των παρεχόμενων λειτουργιών, τυχόν διακοπή της δραστηριότητας λόγω ακατάλληλης ή μη παροχής υπηρεσιών ή λόγω σημαντικού κινδύνου που προκύπτει σε σχέση με την ενδεδειγμένη και συνεχή ανάπτυξη της λειτουργίας ***ή, σε περίπτωση συμβατικών ρυθμίσεων με τρίτους παρόχους υπηρεσιών ΤΠΕ υπό οποιαδήποτε από τις περιστάσεις που απαριθμούνται στην παράγραφο 8 στοιχεία α) έως δ)***.

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

α) χωρίς διακοπή 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 της παροχής των υπηρεσιών τους σε πελάτες.

Τα σχέδια αποχώρησης είναι ολοκληρωμένα, τεκμηριωμένα και, κατά περίπτωση, επαρκώς δοκιμασμένα.

Οι χρηματοπιστωτικές οντότητες προσδιορίζουν εναλλακτικές λύσεις και καταρτίζουν μεταβατικά σχέδια που τους παρέχουν τη δυνατότητα να αφαιρέσουν τις συμβατικές λειτουργίες 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 χρηματοπιστωτικές οντότητες λαμβάνουν τα κατάλληλα μέτρα έκτακτης ανάγκης με σκοπό να διατηρηθεί η αδιάλειπτη λειτουργία υπό όλες τις συνθήκες που αναφέρονται στο πρώτο εδάφιο.

10. 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 4.

Οι ΕΕΑ υποβάλλουν στην Επιτροπή τα εν λόγω σχέδια εκτελεστικών τεχνικών προτύπων έως τη(ν) [ΕΕ: Να συμπληρωθεί ημερομηνία 1 έτος μετά την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού].

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. 1095/2010 και (ΕΕ) αριθ. 1094/2010, αντίστοιχα.

11. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, καταρτίζουν σχέδια ρυθμιστικών προτύπων:

α) για τον περαιτέρω προσδιορισμό των λεπτομερειών του περιεχομένου της πολιτικής που αναφέρεται στην παράγραφο 3 σε σχέση με τις συμβατικές ρυθμίσεις για τη χρήση υπηρεσιών ΤΠΕ που παρέχονται από τρίτους παρόχους ΤΠΕ, παραπέμποντας στα βασικά στάδια του κύκλου ζωής των αντίστοιχων ρυθμίσεων σχετικά με τη χρήση υπηρεσιών ΤΠΕ·

β) τα είδη των πληροφοριών που πρέπει να περιλαμβάνονται στο μητρώο πληροφοριών που αναφέρεται στην παράγραφο 4.

Οι ΕΕΑ υποβάλλουν στην Επιτροπή τα εν λόγω σχέδια ρυθμιστικών τεχνικών προτύπων έως τη(ν) [ΕΕ: Να συμπληρωθεί ημερομηνία 18 μήνες μετά την ημερομηνία έναρξης ισχύος].

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

Άρθρο 26

Προκαταρκτική αξιολόγηση του κινδύνου συγκέντρωσης ΤΠΕ και περαιτέρω ρυθμίσεις υπεργολαβικής ανάθεσης

1. Κατά τον προσδιορισμό και την αξιολόγηση του κινδύνου συγκέντρωσης ΤΠΕ που αναφέρεται στο άρθρο 25 παράγραφος 5 στοιχείο γ), οι χρηματοπιστωτικές οντότητες λαμβάνουν υπόψη αν η σύναψη συμβατικής ρύθμισης σε σχέση με τις υπηρεσίες ΤΠΕ ***που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες*** μπορεί να έχει οποιοδήποτε από τα ακόλουθα αποτελέσματα:

   α) σύμβαση με 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 χρηματοπιστωτικές 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 η συμβατική ρύθμιση σχετικά με τη χρήση υπηρεσιών ΤΠΕ ***που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες*** περιλαμβάνει την πιθανότητα ένας τρίτος πάροχος υπηρεσιών ΤΠΕ να αναθέσει περαιτέρω με υπεργολαβία μια κρίσιμη ή σημαντική λειτουργία σε άλλους τρίτους παρόχους υπηρεσιών ΤΠΕ, οι χρηματοπιστωτικές οντότητες σταθμίζουν τα οφέλη και τους κινδύνους που ενδέχεται να προκύψουν σε σχέση με την εν λόγω πιθανή υπεργολαβία [redacted].

   Όταν οι συμβατικές ρυθμίσεις για τη χρήση υπηρεσιών ΤΠΕ ***που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες*** συνάπτονται με τρίτο πάροχο υπηρεσιών ΤΠΕ [redacted], οι χρηματοπιστωτικές οντότητες εξετάζουν ως συναφείς τουλάχιστον τους ακόλουθους παράγοντες:

   α) [redacted]

   β) [redacted]

   γ) τις διατάξεις του δικαίου περί αφερεγγυότητας που θα ισχύουν σε περίπτωση πτώχευσης του τρίτου παρόχου υπηρεσιών ΤΠΕ· ***και***

   δ) τυχόν περιορισμούς που ενδέχεται να προκύπτουν σε σχέση με την επείγουσα ανάκτηση των δεδομένων της χρηματοπιστωτικής οντότητας.

   Όταν οι συμβατικές ρυθμίσεις για τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες συνάπτονται με τρίτο πάροχο υπηρεσιών ΤΠΕ εγκατεστημένο σε τρίτη χώρα, οι χρηματοπιστωτικές οντότητες, εκτός από τους

παράγοντες που αναφέρθηκαν στο πρώτο και στο δεύτερο εδάφιο, εξετάζουν επίσης:

i) την τήρηση των κανόνων της Ένωσης περί προστασίας δεδομένων· και,

ii) την αποτελεσματική επιβολή των κανόνων που ορίζονται στον παρόντα κανονισμό.

Όταν αυτές οι συμβατικές ρυθμίσεις συμπεριλαμβάνουν υπεργολαβική ανάθεση κρίσιμων ή σημαντικών λειτουργιών, οι χρηματοπιστωτικές οντότητες αξιολογούν αν και με ποιον τρόπο μπορούν οι δυνητικά μεγάλες και πολύπλοκες αλυσίδες υπεργολαβικής ανάθεσης να επηρεάσουν την ικανότητά τους να ***αξιολογούν*** πλήρως ***τους παράγοντες που απαριθμούνται στο δεύτερο και το τρίτο εδάφιο και*** να παρακολουθούν τις λειτουργίες που αποτελούν αντικείμενο ανάθεσης, καθώς και την ικανότητα της αρμόδιας αρχής να εποπτεύει αποτελεσματικά τη χρηματοπιστωτική οντότητα στο πλαίσιο αυτό.

Άρθρο 27

Βασικές συμβατικές διατάξεις

1. Τα δικαιώματα και οι υποχρεώσεις της χρηματοπιστωτικής οντότητας και του τρίτου παρόχου υπηρεσιών ΤΠΕ επιμερίζονται με σαφήνεια και καθορίζονται σε γραπτή συμφωνία. Η πλήρης σύμβαση, η οποία περιλαμβάνει τις συμφωνίες επιπέδου εξυπηρέτησης, τεκμηριώνεται ***εγγράφως και*** τίθεται στη διάθεση των συμβαλλομένων σε έντυπη μορφή ή σε μορφή με δυνατότητα μεταφόρτωσης και πρόσβασης.

2. ***Οι χρηματοπιστωτικές οντότητες και οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ διασφαλίζουν ότι*** οι συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ περιλαμβάνουν τουλάχιστον τα ακόλουθα:

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

β) τις τοποθεσίες***, δηλαδή τις περιφέρειες ή 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 ***εκ των προτέρων*** ενημέρωσης της χρηματοπιστωτικής οντότητας από τον τρίτο πάροχο υπηρεσιών ΤΠΕ σε περίπτωση που προτίθεται να αλλάξει τις τοποθεσίες αυτές·

γ) διατάξεις σχετικά με την προσβασιμότητα, τη διαθεσιμότητα, την ακεραιότητα, την ασφάλεια, ***την εμπιστευτικότητα*** και την προστασία των δεδομένων***, συμπεριλαμβανομένων των δεδομένων*** προσωπικού χαρακτήρα·

γα) 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 χρηματοπιστωτική οντότητα σε περίπτωση αφερεγγυότητας, εξυγίανσης, διακοπής των επιχειρηματικών δραστηριοτήτων του τρίτου παρόχου υπηρεσιών ΤΠΕ***, ή σε περίπτωση καταγγελίας των συμβατικών ρυθμίσεων·***

δ) πλήρη περιγραφή των επιπέδων εξυπηρέτησης, συμπεριλαμβανομένων των επικαιροποιήσεων και των αναθεωρήσεών τους, και ακριβείς ποσοτικούς και ποιοτικούς στόχους επιδόσεων εντός των συμφωνημένων επιπέδων εξυπηρέτησης, ώστε να παρέχεται η δυνατότητα αποτελεσματικής παρακολούθησης από τη χρηματοπιστωτική οντότητα και να επιτρέπεται, χωρίς αδικαιολόγητη καθυστέρηση, η λήψη κατάλληλων διορθωτικών μέτρων όταν δεν πληρούνται τα συμφωνημένα επίπεδα εξυπηρέτησης·

ε) ▌

στ) την υποχρέωση του τρίτου παρόχου υπηρεσιών ΤΠΕ να παρέχει συνδρομή σε περίπτωση συμβάντος ΤΠΕ ***που σχετίζεται με τον πάροχο υπηρεσιών*** χωρίς επιπλέον κόστος ή με κόστος που προσδιορίζεται εκ των προτέρων·

ζ) απαιτήσεις για τον τρίτο πάροχο υπηρεσιών ΤΠΕ να θέτει σε εφαρμογή και να υποβάλλει σε δοκιμή επιχειρηματικά σχέδια έκτακτης ανάγκης και να εφαρμόζει μέτρα, εργαλεία και πολιτικές ασφάλειας των ΤΠΕ που ***παρέχουν κατάλληλο*** επίπεδο ασφαλούς παροχής υπηρεσιών από τη χρηματοπιστωτική οντότητα σύμφωνα με το κανονιστικό της πλαίσιο·

η) ▌

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

ι) δικαιώματα καταγγελίας και συναφείς ελάχιστες περιόδους προειδοποίησης για την καταγγελία της σύμβασης, σύμφωνα με τις προσδοκίες των αρμόδιων αρχών ***και των αρχών εξυγίανσης και, όταν η εν λόγω συμβατική ρύθμιση επηρεάζει έναν ενδοομιλικό πάροχο υπηρεσιών ΤΠΕ εντός του ίδιου ομίλου, ανάλυση βάσει προσέγγισης βάσει κινδύνου***·

ια) 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 με σκοπό τη μείωση του κινδύνου διαταραχών στη χρηματοπιστωτική οντότητα ***ή τη διασφάλιση της αποτελεσματικής εξυγίανσης και αναδιάρθρωσής της***·

ii) η οποία παρέχει στη χρηματοπιστωτική οντότητα τη δυνατότητα μετάβασης σε άλλον τρίτο πάροχο υπηρεσιών ΤΠΕ ή τη δυνατότητα επιλογής άλλων λύσεων εντός των χώρων της, ανάλογα με την πολυπλοκότητα της παρεχόμενης υπηρεσίας·

iia) όταν αυτή η συμβατική ρύθμιση έχει αντίκτυπο σε έναν ενδοομιλικό τρίτο πάροχο υπηρεσιών ΤΠΕ εντός του ίδιου ομίλου, αναλύεται σύμφωνα με μια προσέγγιση βάσει κινδύνων·

ιαα) μια διάταξη για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τρίτο πάροχο υπηρεσιών ΤΠΕ, η οποία πρέπει να συμμορφώνεται με τον κανονισμό (ΕΕ) 2016/679.

2α. Οι συμβατικές ρυθμίσεις για την παροχή κρίσιμων ή σημαντικών λειτουργιών

περιλαμβάνουν, επιπροσθέτως της παραγράφου 2, τουλάχιστον τα ακόλουθα:

α) προθεσμίες προειδοποίησης και υποχρεώσεις υποβολής εκθέσεων εκ μέρους του τρίτου παρόχου υπηρεσιών ΤΠΕ προς τη χρηματοπιστωτική οντότητα, συμπεριλαμβανομένης της κοινοποίησης οποιασδήποτε εξέλιξης η οποία μπορεί να έχει σημαντικές επιπτώσεις στην ικανότητα του τρίτου παρόχου υπηρεσιών ΤΠΕ όσον αφορά την αποτελεσματική εκτέλεση κρίσιμων ή σημαντικών λειτουργιών σύμφωνα με τα συμφωνημένα επίπεδα εξυπηρέτησης·

β) το δικαίωμα παρακολούθησης σε διαρκή βάση των επιδόσεων του τρίτου παρόχου υπηρεσιών ΤΠΕ, στο οποίο περιλαμβάνονται:

i) δικαιώματα πρόσβασης, επιθεώρησης και ελέγχου από τη χρηματοπιστωτική οντότητα ή από διορισμένο τρίτο φορέα, και το δικαίωμα εξέτασης αντιγράφων της σχετικής τεκμηρίωσης επί τόπου 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 επί εναλλακτικών επιπέδων βεβαιότητας όταν θίγονται τα δικαιώματα άλλων πελατών·

iii) τη δέσμευση 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 χρηματοπιστωτική οντότητα ή διορισμένο τρίτο φορέα, και λεπτομέρειες σχετικά με το εύρος, τους τρόπους και τη συχνότητα διενέργειας των εν λόγω επιθεωρήσεων και ελέγχων.

Κατά παρέκκλιση από το στοιχείο β), ο τρίτος πάροχος υπηρεσιών ΤΠΕ και η χρηματοπιστωτική οντότητα μπορούν να συμφωνήσουν ότι τα δικαιώματα πρόσβασης, επιθεώρησης και ελέγχου μπορούν να ανατεθούν σε ανεξάρτητο τρίτο μέρος, το οποίο ορίζεται από τον τρίτο πάροχο υπηρεσιών ΤΠΕ, και ότι η χρηματοπιστωτική οντότητα είναι σε θέση να ζητήσει πληροφορίες και διαβεβαιώσεις σχετικά με την απόδοση του τρίτου παρόχου υπηρεσιών ΤΠΕ από το τρίτο μέρος ανά πάσα στιγμή.

2β. Οι συμβατικές ρυθμίσεις για την παροχή υπηρεσιών ΤΠΕ από τρίτο πάροχο υπηρεσιών ΤΠΕ εγκατεστημένο σε τρίτη χώρα, ο οποίος χαρακτηρίζεται ως κρίσιμος σύμφωνα με το άρθρο 28 παράγραφος 9, πρέπει, επιπροσθέτως προς τις παραγράφους 2 και 2α του παρόντος άρθρου:

α) να ορίζουν ότι η σύμβαση διέπεται από το δίκαιο κράτους μέλους· και

β) να εγγυώνται ότι το όργανο κοινής εποπτείας και ο κύριος εποπτικός φορέας μπορούν να ασκούν τα καθήκοντά του που ορίζονται στο άρθρο 30 βάσει των αρμοδιοτήτων τους που ορίζονται στο άρθρο 31.

Οι υπηρεσίες για τις οποίες συνάπτονται οι συμβατικές ρυθμίσεις δεν απαιτείται να παρέχονται από την επιχείρηση που έχει συσταθεί στην Ένωση βάσει του δικαίου κράτους μέλους.

3. Κατά τη διαπραγμάτευση των συμβατικών ρυθμίσεων, οι χρηματοπιστωτικές οντότητες

και οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ λαμβάνουν υπόψη τη χρήση τυποποιημένων συμβατικών ρητρών που έχουν αναπτυχθεί για συγκεκριμένες υπηρεσίες.

3α ***Οι αρμόδιες αρχές μπορούν να έχουν πρόσβαση στις συμβατικές ρυθμίσεις που αναφέρονται στο παρόν άρθρο. Τα μέρη των εν λόγω συμβατικών ρυθμίσεων μπορούν να συμφωνήσουν να αποκρύψουν εμπορικά ευαίσθητες ή εμπιστευτικές πληροφορίες πριν από τη χορήγηση της εν λόγω πρόσβασης στις αρμόδιες αρχές, υπό την προϋπόθεση ότι οι τελευταίες ενημερώνονται πλήρως ως προς την έκταση και τη φύση των αποκρύψεων.***

4. Οι ΕΕΑ καταρτίζουν, μέσω της μεικτής επιτροπής, σχέδια ρυθμιστικών τεχνικών προτύπων για τον περαιτέρω προσδιορισμό των στοιχείων που πρέπει να καθορίζει και να αξιολογεί η χρηματοπιστωτική οντότητα κατά την υπεργολαβική ανάθεση κρίσιμων ή σημαντικών λειτουργιών με σκοπό την ορθή εφαρμογή των διατάξεων της παραγράφου 2 στοιχείο α). ***Κατά την κατάρτιση των εν λόγω σχεδίων ρυθμιστικών τεχνικών προτύπων, οι ΕΕΑ λαμβάνουν υπόψη το μέγεθος των χρηματοπιστωτικών οντοτήτων, τη φύση, την κλίμακα και την πολυπλοκότητα των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών τους, καθώς και το συνολικό προφίλ κινδύνου τους.***

Οι ΕΕΑ υποβάλλουν στην Επιτροπή τα εν λόγω σχέδια ρυθμιστικών τεχνικών προτύπων έως τη(ν) [ΕΕ: Να συμπληρωθεί ημερομηνία ***18 μήνες*** μετά την ημερομηνία έναρξης ισχύος].

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. 1095/2010 και (ΕΕ) αριθ. 1094/2010, αντίστοιχα.

ΤΜΗΜΑ ΙΙ

ΠΛΑΙΣΙΟ ΕΠΟΠΤΕΙΑΣ ΚΡΙΣΙΜΩΝ ΤΡΙΤΩΝ ΠΑΡΟΧΩΝ ΥΠΗΡΕΣΙΩΝ ΤΠΕ

Άρθρο 28

Ορισμός κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ

1. Οι ΕΕΑ, μέσω της μεικτής επιτροπής και κατόπιν σύστασης του ***οργάνου κοινής*** εποπτείας που συγκροτείται βάσει του άρθρου 29 παράγραφος 1, ***ύστερα από διαβούλευση με τον ENISA***:

   α) ορίζουν τους τρίτους παρόχους υπηρεσιών ΤΠΕ που είναι κρίσιμης σημασίας για τις χρηματοπιστωτικές οντότητες, λαμβάνοντας υπόψη τα κριτήρια που καθορίζονται στην παράγραφο 2·

   β) ορίζουν την ΕΒΑ, την ESMA ή την ΕΙΟΡΑ ως κύριο εποπτικό φορέα για κάθε κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ, ανάλογα με το αν η συνολική αξία των περιουσιακών στοιχείων των χρηματοπιστωτικών οντοτήτων που χρησιμοποιούν τις υπηρεσίες του εν λόγω κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ, και οι οποίες καλύπτονται από κάποιον από τους κανονισμούς (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 ή (ΕΕ) αριθ. 1095/2010 αντίστοιχα, αντιπροσωπεύει ποσοστό άνω του 50 % της αξίας των συνολικών περιουσιακών στοιχείων όλων των χρηματοπιστωτικών οντοτήτων που χρησιμοποιούν τις υπηρεσίες του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ, όπως αποδεικνύεται από τους ενοποιημένους ισολογισμούς αυτών των χρηματοπιστωτικών οντοτήτων ή από τους επιμέρους ισολογισμούς τους, σε περίπτωση που οι ισολογισμοί τους δεν είναι ενοποιημένοι.

   Ο κύριος εποπτικός φορέας που διορίζεται σύμφωνα με το πρώτο εδάφιο στοιχείο β) είναι υπεύθυνος για την καθημερινή εποπτεία του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ.

2. Ο ορισμός που αναφέρονται στην παράγραφο 1 στοιχείο α) βασίζεται στα ακόλουθα κριτήρια:

   α) τις συστημικές επιπτώσεις στη σταθερότητα, τη συνέχεια ή την ποιότητα της παροχής χρηματοπιστωτικών 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 χρηματοπιστωτικών οντοτήτων στις οποίες ο οικείος τρίτος πάροχος υπηρεσιών ΤΠΕ παρέχει τις υπηρεσίες του·

   β) τον συστημικό χαρακτήρα ή τη σημασία των χρηματοπιστωτικών 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 χρηματοπιστωτικών οντοτήτων, συμπεριλαμβανομένων των καταστάσεων στις οποίες τα G-SII ή τα O-SII παρέχουν υπηρεσίες χρηματοπιστωτικών υποδομών σε άλλες χρηματοπιστωτικές οντότητες·

γ) την εξάρτηση των χρηματοπιστωτικών οντοτήτων από τις υπηρεσίες που παρέχονται από τον σχετικό τρίτο πάροχο υπηρεσιών ΤΠΕ σε σχέση με κρίσιμες ή σημαντικές λειτουργίες χρηματοπιστωτικών οντοτήτων στις οποίες συμμετέχει τελικά ο ίδιος τρίτος πάροχος υπηρεσιών ΤΠΕ, ανεξάρτητα από το αν οι χρηματοπιστωτικές οντότητες στηρίζονται στις υπηρεσίες αυτές άμεσα ή έμμεσα, μέσω ή δυνάμει 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 μερικής ή συνολικής μεταφοράς των σχετικών δεδομένων και του φόρτου εργασίας από τον οικείο τρίτο πάροχο υπηρεσιών ΤΠΕ σε άλλον, είτε λόγω του σημαντικού οικονομικού κόστους, του χρόνου ή άλλου είδους πόρων που μπορεί να συνεπάγεται η διαδικασία μεταφοράς είτε λόγω αυξημένων κινδύνων ΤΠΕ ή άλλων λειτουργικών κινδύνων στους οποίους ενδέχεται να εκτεθεί η χρηματοπιστωτική οντότητα λόγω της μεταφοράς αυτής.

ε) τον αριθμό των κρατών μελών στα οποία παρέχει υπηρεσίες ο οικείος τρίτος πάροχος υπηρεσιών ΤΠΕ·

στ) τον αριθμό των κρατών μελών στα οποία δραστηριοποιούνται χρηματοπιστωτικές οντότητες που χρησιμοποιούν τον οικείο τρίτο πάροχο υπηρεσιών ΤΠΕ·

στα) την ουσιαστικότητα και τη σημασία των υπηρεσιών που παρέχονται από τον σχετικό τρίτο πάροχο υπηρεσιών ΤΠΕ.

2α. Το όργανο κοινής εποπτείας ενημερώνει τον τρίτο πάροχο υπηρεσιών ΤΠΕ προτού ξεκινήσει την αξιολόγησή του για τους σκοπούς του χαρακτηρισμού που αναφέρεται στο στοιχείο α) της παραγράφου 1.

Το όργανο κοινής εποπτείας κοινοποιεί στον τρίτο πάροχο υπηρεσιών ΤΠΕ το αποτέλεσμα της αξιολόγησης που αναφέρεται στο πρώτο εδάφιο, παρέχοντας σχέδιο σύστασης σχετικά με την κρισιμότητα. Εντός 6 εβδομάδων από την ημερομηνία παραλαβής του εν λόγω σχεδίου σύστασης, ο τρίτος πάροχος υπηρεσιών ΤΠΕ μπορεί να υποβάλει στο όργανο κοινής εποπτείας αιτιολογημένη δήλωση σχετικά με την αξιολόγηση. Η αιτιολογημένη δήλωση περιέχει όλες τις σχετικές πρόσθετες πληροφορίες που θεωρούνται κατάλληλες από τον τρίτο πάροχο υπηρεσιών ΤΠΕ προκειμένου να υποστηρίξει την πληρότητα και την ακρίβεια της διαδικασίας χαρακτηρισμού ή να αμφισβητήσει το σχέδιο σύστασης σχετικά με την κρισιμότητα. Η μεικτή επιτροπή των ΕΕΑ λαμβάνει δεόντως υπόψη την αιτιολογημένη δήλωση και μπορεί να ζητήσει περαιτέρω πληροφορίες ή αποδεικτικά στοιχεία από τον τρίτο πάροχο υπηρεσιών ΤΠΕ πριν από τη λήψη απόφασης σχετικά με τον ορισμό.

Η μεικτή επιτροπή των ΕΕΑ κοινοποιεί στον τρίτο πάροχο υπηρεσιών ότι έχει χαρακτηριστεί κρίσιμος. Ο τρίτος πάροχος υπηρεσιών ΤΠΕ έχει στη διάθεσή του προθεσμία τουλάχιστον τριών μηνών από την ημερομηνία παραλαβής της κοινοποίησης για να προβεί στις αναγκαίες προσαρμογές ώστε να μπορέσει το όργανο κοινής εποπτείας να εκτελέσει τα καθήκοντά του σύμφωνα με το άρθρο 30, καθώς και για να ενημερώσει τις χρηματοπιστωτικές οντότητες στις οποίες ο τρίτος πάροχος υπηρεσιών ΤΠΕ παρέχει υπηρεσίες. Το όργανο κοινής εποπτείας μπορεί να επιτρέψει την παράταση της περιόδου προσαρμογής για μια ελάχιστη περίοδο τριών μηνών, εάν ζητηθεί από τον χαρακτηρισμένο τρίτο πάροχο υπηρεσιών ΤΠΕ και εάν αυτό είναι δεόντως αιτιολογημένο.

3. Η Επιτροπή εξουσιοδοτείται να εκδίδει κατ' εξουσιοδότηση πράξη σύμφωνα με το άρθρο 50, με σκοπό ***τον περαιτέρω προσδιορισμό*** των κριτηρίων που αναφέρονται στην παράγραφο 2 έως τη(ν) [ΕΕ:

4. Ο μηχανισμός ορισμού που αναφέρεται στην παράγραφο 1 στοιχείο α) δεν χρησιμοποιείται έως ότου η Επιτροπή εκδώσει κατ' εξουσιοδότηση πράξη σύμφωνα με την παράγραφο 3.

5. Ο μηχανισμός ορισμού που αναφέρεται στην παράγραφο 1 στοιχείο α) δεν εφαρμόζεται σε σχέση με τρίτους παρόχους υπηρεσιών ΤΠΕ που υπόκεινται σε πλαίσια εποπτείας, τα οποία έχουν θεσπιστεί με σκοπό τη υποστήριξη των καθηκόντων που αναφέρονται στο άρθρο 127 παράγραφος 2 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης.

6. ***Το όργανο κοινής εποπτείας, σε συνεννόηση με τον ENISA,*** καταρτίζουν, δημοσιεύουν και επικαιροποιούν ***τακτικά*** τον κατάλογο των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ σε επίπεδο Ένωσης.

7. Για τους σκοπούς της παραγράφου 1 στοιχείο α), οι αρμόδιες αρχές διαβιβάζουν, σε ετήσια και συγκεντρωτική βάση, τις εκθέσεις που αναφέρονται στο άρθρο 25 παράγραφος 4 στο ***όργανο κοινής εποπτείας***, το οποίο συγκροτείται σύμφωνα με το άρθρο 29. Το ***όργανο κοινής εποπτείας*** αξιολογεί τις εξαρτήσεις των τρίτων παρόχων ΤΠΕ από χρηματοπιστωτικές οντότητες βάσει των πληροφοριών που λαμβάνει από τις αρμόδιες αρχές.

8. Οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που δεν περιλαμβάνονται στον κατάλογο που αναφέρεται στην παράγραφο 6 μπορούν να ζητήσουν να συμπεριληφθούν στον κατάλογο.

   Για τους σκοπούς του πρώτου εδαφίου, ο τρίτος πάροχος υπηρεσιών ΤΠΕ υποβάλλει αιτιολογημένη αίτηση στην ΕΒΑ, την ESMA ή την ΕΙΟΡΑ, οι οποίες αποφασίζουν, μέσω της μεικτής επιτροπής, αν ο εν λόγω τρίτος πάροχος υπηρεσιών ΤΠΕ πρέπει να συμπεριληφθεί στον κατάλογο 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.

8α. Η Μεικτή Επιτροπή των ΕΕΑ, κατόπιν σύστασης του οργάνου κοινής εποπτείας, ορίζει τους τρίτους παρόχους υπηρεσιών ΤΠΕ που είναι εγκατεστημένοι σε τρίτη χώρα και είναι κρίσιμοι για τις χρηματοπιστωτικές οντότητες σύμφωνα με την παράγραφο 1 στοιχείο α).

Κατά τον ορισμό που αναφέρεται στο πρώτο εδάφιο της παρούσας παραγράφου, οι ΕΕΑ και το κοινό όργανο εποπτείας ακολουθούν τα διαδικαστικά στάδια που ορίζονται στην παράγραφο 2α.

9. Οι χρηματοπιστωτικές οντότητες δεν κάνουν χρήση ***κρίσιμου*** τρίτου παρόχου υπηρεσιών ΤΠΕ που είναι εγκατεστημένος σε τρίτη χώρα***, εκτός εάν ο εν λόγω τρίτος πάροχος υπηρεσιών ΤΠΕ έχει επιχείρηση που έχει συσταθεί στην Ένωση δυνάμει του δικαίου κράτους μέλους και έχει συνάψει συμβατικές ρυθμίσεις σύμφωνα με το άρθρο 27 παράγραφος 2β***.

Άρθρο 29

Δομή του πλαισίου εποπτείας

1. ***Το όργανο κοινής εποπτείας συγκροτείται*** για τους σκοπούς της ***εποπτείας του κινδύνου*** τρίτων παρόχων ΤΠΕ σε όλους τους χρηματοπιστωτικούς τομείς ***και της διενέργειας άμεσης εποπτείας τρίτων παρόχων υπηρεσιών ΤΠΕ που χαρακτηρίζονται ως κρίσιμοι σύμφωνα με το άρθρο 28***.

Ο ρόλος του οργάνου κοινής εποπτείας περιορίζεται στις εξουσίες εποπτείας που σχετίζονται με κινδύνους ΤΠΕ σχετικά με τις υπηρεσίες ΤΠΕ που παρέχονται από κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ σε χρηματοπιστωτικές οντότητες.

Το ***όργανο κοινής*** εποπτείας συζητά τακτικά τις σχετικές εξελίξεις όσον αφορά τους κινδύνους και τις ευπάθειες των ΤΠΕ και προωθεί την υιοθέτηση συνεκτικής προσέγγισης για την παρακολούθηση του κινδύνου τρίτων παρόχων ΤΠΕ στην κλίμακα της Ένωσης.

2. Το ***όργανο κοινής*** εποπτείας προβαίνει ετησίως σε συλλογική αξιολόγηση των αποτελεσμάτων και των πορισμάτων 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 χρηματοπιστωτικών οντοτήτων, την προώθηση βέλτιστων πρακτικών αντιμετώπισης του κινδύνου συγκέντρωσης ΤΠΕ και τη διερεύνηση μέσων μετριασμού σε περιπτώσεις διατομεακής μεταφοράς κινδύνων.

Το ***όργανο κοινής*** εποπτείας υποβάλλει γενικούς δείκτες αναφοράς κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ για 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.

3. Το ***όργανο κοινής*** εποπτείας απαρτίζεται από τους ***εκτελεστικούς διευθυντές*** των ΕΕΑ, έναν υψηλόβαθμο εκπρόσωπο προερχόμενο από το εν ενεργεία προσωπικό ***των ΕΕΑ και έναν εκπρόσωπο υψηλού επιπέδου από τουλάχιστον οκτώ από τις εθνικές αρμόδιες αρχές***. ▌Ένας εκπρόσωπος από την Ευρωπαϊκή Επιτροπή, το ΕΣΣΚ, την ΕΚΤ και τον ENISA ***και τουλάχιστον ένας ανεξάρτητος εμπειρογνώμονας διορισμένος σύμφωνα με την παράγραφο 3α του παρόντος άρθρου*** συμμετέχουν ως παρατηρητές.

Μετά τον ετήσιο ορισμό κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 28 παράγραφος 1 στοιχείο α), η μεικτή επιτροπή των ΕΕΑ αποφασίζει ποιες εθνικές αρμόδιες αρχές είναι μέλη του οργάνου κοινής εποπτείας, λαμβάνοντας υπόψη τους ακόλουθους παράγοντες:

α) τον αριθμό των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ που είναι εγκατεστημένοι ή παρέχουν υπηρεσίες στο κράτος μέλος·

β) την εξάρτηση των χρηματοπιστωτικών οντοτήτων σε ένα κράτος μέλος από κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ·

γ) την σχετική εμπειρογνωμοσύνη εθνικής αρμόδιας αρχής·

δ) τους διαθέσιμους πόρους και την διαθέσιμη ικανότητα εθνικής αρμόδιας αρχής·

ε) την ανάγκη εξορθολογισμού και εξασφάλισης της λιτότητας και της αποτελεσματικότητας της λειτουργίας και των διαδικασιών λήψης αποφάσεων του οργάνου κοινής εποπτείας.

Το όργανο κοινής εποπτείας κοινοποιεί την τεκμηρίωση και τις αποφάσεις του σε όλες τις αρμόδιες εθνικές αρχές που δεν είναι μέλη του οργάνου κοινής εποπτείας.

Το έργο του οργάνου κοινής εποπτείας υποστηρίζεται και επικουρείται από ειδικό προσωπικό από όλες τις ΕΕΑ.

3α. Ο ανεξάρτητος εμπειρογνώμονας που αναφέρεται στην παράγραφο 3 του παρόντος άρθρου διορίζεται ως παρατηρητής από το όργανο κοινής εποπτείας μετά από δημόσια και διαφανή διαδικασία υποβολής αιτήσεων.

Ο ανεξάρτητος εμπειρογνώμονας διορίζεται με βάση την εμπειρογνωσία του σε θέματα χρηματοπιστωτικής σταθερότητας, ψηφιακής επιχειρησιακής ανθεκτικότητας και ασφάλειας ΤΠΕ για περίοδο δύο ετών.

Ο διορισθείς ανεξάρτητος εμπειρογνώμονας δεν κατέχει άλλη θέση σε εθνικό, ενωσιακό ή διεθνές επίπεδο. Ο ανεξάρτητος εμπειρογνώμονας ενεργεί ανεξάρτητα και αντικειμενικά αποκλειστικά προς το συμφέρον της Ένωσης συνολικά και ούτε ζητεί ούτε δέχεται οδηγίες από θεσμικά όργανα ή οργανισμούς της Ένωσης, από οποιαδήποτε κυβέρνηση κράτους μέλους ή από οποιονδήποτε άλλον δημόσιο ή ιδιωτικό φορέα.

Το όργανο κοινής εποπτείας μπορεί να αποφασίσει να διορίσει περισσότερους από έναν ανεξάρτητους εμπειρογνώμονες παρατηρητές.

4. Σύμφωνα με το άρθρο 16 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010, οι ΕΕΑ εκδίδουν κατευθυντήριες γραμμές ***έως τη(ν) [ΕΕ: Να συμπληρωθεί ημερομηνία 18 μήνες μετά την ημερομηνία έναρξης ισχύος]*** σχετικά με τη συνεργασία μεταξύ ***του οργάνου κοινής εποπτείας, του κύριου εποπτικού φορέα*** και των αρμόδιων αρχών για τους σκοπούς του παρόντος τμήματος ως προς τις λεπτομερείς διαδικασίες και προϋποθέσεις που αφορούν την εκτέλεση των καθηκόντων μεταξύ των αρμόδιων αρχών και ***του οργάνου κοινής εποπτείας***, καθώς και τις λεπτομέρειες σχετικά με την ανταλλαγή των πληροφοριών που χρειάζονται οι αρμόδιες αρχές προκειμένου να διασφαλιστεί ότι δίνεται συνέχεια στις συστάσεις που ***απευθύνει το όργανο κοινής εποπτείας***, σύμφωνα με το άρθρο 31 παράγραφος 1 στοιχείο δ), σε κρίσιμους τρίτους παρόχους ΤΠΕ.

5. Οι απαιτήσεις που ορίζονται στο παρόν τμήμα δεν θίγουν την εφαρμογή της οδηγίας (ΕΕ) 2016/1148 και άλλων κανόνων της Ένωσης για την εποπτεία που εφαρμόζεται σε παρόχους υπηρεσιών υπολογιστικού νέφους.

6. Το ***όργανο κοινής*** εποπτείας ***υποβάλλει*** ετησίως στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Επιτροπή έκθεση σχετικά με την εφαρμογή του παρόντος τμήματος.

Άρθρο 30

Καθήκοντα του κύριου εποπτικού φορέα

1. Ο κύριος εποπτικός φορέας***, ο οποίος διορίζεται σύμφωνα με το άρθρο 28 παράγραφος 1 στοιχείο β), διευθύνει και συντονίζει την καθημερινή εποπτεία κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ και αποτελεί το κύριο σημείο επαφής για τους εν λόγω κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ.***

1α. ***Ο κύριος εποπτικός φορέας*** εξακριβώνει αν κάθε κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ διαθέτει εμπεριστατωμένους, ορθούς και αποτελεσματικούς κανόνες, διαδικασίες, μηχανισμούς και ρυθμίσεις για τη διαχείριση κινδύνων ΤΠΕ στους οποίους ενδέχεται να εκθέτει τις χρηματοπιστωτικές οντότητες. ***Η αξιολόγηση επικεντρώνεται πρωτίστως στις υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες που παρέχουν οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ σε χρηματοπιστωτικές οντότητες, αλλά μπορεί επίσης να είναι ευρύτερη, εάν σχετίζεται με την εκτίμηση των κινδύνων για τις εν λόγω υπηρεσίες.***

2. Η αξιολόγηση που αναφέρεται στην παράγραφο 1***α*** περιλαμβάνει:

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 χρηματοπιστωτικές οντότητες, καθώς και την ικανότητα να διατηρεί ανά πάσα στιγμή υψηλά πρότυπα ασφάλειας, εμπιστευτικότητας και ακεραιότητας 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 των σχεδίων αδιάλειπτης λειτουργίας και αποκατάστασης λειτουργίας των ΤΠΕ μετά από καταστροφή·

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 χρηματοπιστωτικές 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 χρηματοπιστωτικές οντότητες·

ζ) τη δοκιμή συστημάτων, υποδομών και ελέγχων ΤΠΕ·

η) του ελέγχους ΤΠΕ·

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

3. Με βάση την αξιολόγηση που αναφέρεται στην παράγραφο ***1α και πραγματοποιείται από τον κύριο εποπτικό φορέα, το όργανο κοινής εποπτείας, υπό τον συντονισμό και τη διεύθυνση του κύριου εποπτικού φορέα, συντάσσει και προτείνει*** σαφές, λεπτομερές και τεκμηριωμένο εξατομικευμένο σχέδιο εποπτείας για κάθε κρίσιμο τρίτο

πάροχο υπηρεσιών ΤΠΕ.

Κατά την προετοιμασία του προκαταρκτικού σχεδίου εποπτείας, το όργανο κοινής εποπτείας διαβουλεύεται με όλες τις σχετικές αρμόδιες αρχές και τα ενιαία κέντρα επαφής που αναφέρονται στο άρθρο 8 της οδηγίας (ΕΕ) 2016/1148 για να διασφαλίσει ότι δεν θα υπάρξουν αντιφάσεις ή επικαλύψεις με τις υποχρεώσεις του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ βάσει της εν λόγω οδηγίας.

Το σχέδιο εποπτείας εγκρίνεται σε ετήσια βάση από το διοικητικό συμβούλιο του κύριου εποπτικού φορέα.

Προτού εγκριθεί, το προκαταρκτικό σχέδιο ***εποπτείας*** κοινοποιείται στον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ.

Μετά την παραλαβή του προκαταρκτικού σχεδίου εποπτείας, ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ διαθέτει προθεσμία έξι εβδομάδων για να επανεξετάσει και να υποβάλει αιτιολογημένη δήλωση σχετικά με το προκαταρκτικό σχέδιο εποπτείας. Η εν λόγω αιτιολογημένη δήλωση μπορεί να υποβληθεί μόνον εάν ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ είναι σε θέση να προσκομίσει στοιχεία που αποδεικνύουν ότι η εκτέλεση του σχεδίου εποπτείας θα προκαλούσε δυσανάλογες επιπτώσεις ή διαταραχή σε πελάτες που δεν υπόκεινται στον παρόντα κανονισμό, ή ότι υπάρχει αποτελεσματικότερη ή αποδοτικότερη λύση για τη διαχείριση των εντοπισθέντων κινδύνων ΤΠΕ. Εάν υποβληθεί τέτοια δήλωση, ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ προτείνει στο όργανο κοινής εποπτείας μια αποτελεσματικότερη ή αποδοτικότερη λύση για την επίτευξη των στόχων του προκαταρκτικού σχεδίου εποπτείας.

Πριν από την έγκριση του σχεδίου εποπτείας, το διοικητικό συμβούλιο του κύριου εποπτικού φορέα λαμβάνει δεόντως υπόψη την αιτιολογημένη δήλωση και μπορεί να ζητήσει περαιτέρω πληροφορίες ή αποδεικτικά στοιχεία από τον τρίτο πάροχο υπηρεσιών ΤΠΕ.

4. Μόλις ***εγκριθούν*** τα ετήσια σχέδια εποπτείας που αναφέρονται στην παράγραφο 3 και κοινοποιηθούν στους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, οι αρμόδιες αρχές δύνανται να λάβουν μέτρα για τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ μόνον κατόπιν συμφωνίας με ***το όργανο κοινής εποπτείας***.

Άρθρο 31

Εποπτικές εξουσίες

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

α) να ζητεί όλες τις σχετικές πληροφορίες και τα έγγραφα τεκμηρίωσης σύμφωνα με το άρθρο 32·

β) να διενεργεί γενικές έρευνες και ***επιτόπιες*** επιθεωρήσεις σύμφωνα με τα άρθρα 33 και 34·

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 ***κρίσιμοι*** τρίτοι πάροχοι υπηρεσιών ΤΠΕ όσον

αφορά τις συστάσεις που αναφέρονται ***στην παράγραφο 1α***·

1α. ***Για τους σκοπούς της εκτέλεσης των καθηκόντων που ορίζονται στο παρόν τμήμα, και με βάση τις πληροφορίες που λαμβάνει ο κύριος εποπτικός φορέας και τα αποτελέσματα των ερευνών που διεξάγει ο κύριος εποπτικός φορέας, το όργανο κοινής εποπτείας έχει την εξουσία*** να διατυπώνει συστάσεις για τους τομείς που αναφέρονται στο άρθρο 30 παράγραφος 2, 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 ***το όργανο κοινής εποπτείας*** θεωρεί συναφή για τη διασφάλιση της ασφάλειας των υπηρεσιών ΤΠΕ που παρέχονται στις χρηματοπιστωτικές οντότητες·

ii) τη χρήση όρων και προϋποθέσεων, συμπεριλαμβανομένης της τεχνικής εφαρμογής τους, σύμφωνα με τις οποίες οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ παρέχουν υπηρεσίες σε χρηματοπιστωτικές οντότητες, τις οποίες ***το όργανο κοινής εποπτείας*** θεωρεί συναφείς για την αποτροπή της δημιουργίας μοναδικών σημείων αποτυχίας, ή την ενίσχυσή τους, ή για την ελαχιστοποίηση των πιθανών συστημικών επιπτώσεων στον χρηματοπιστωτικό τομέα της Ένωσης σε περίπτωση κινδύνου συγκέντρωσης ΤΠΕ·

iii) κατά την εξέταση των ρυθμίσεων υπεργολαβίας που πραγματοποιείται σύμφωνα με τα άρθρα 32 και 33, συμπεριλαμβανομένων των ρυθμίσεων υπεργολαβίας 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, κάθε προγραμματισμένη υπεργολαβία, συμπεριλαμβανομένης της υπεργολαβικής ανάθεσης, όταν ***το όργανο κοινής εποπτείας*** θεωρεί ότι η περαιτέρω υπεργολαβία ενδέχεται να ενεργοποιήσει κινδύνους όσον αφορά την παροχή υπηρεσιών από τη χρηματοπιστωτική οντότητα ή κινδύνους για τη χρηματοπιστωτική σταθερότητα·

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 ***και δεν διαθέτει επιχείρηση που έχει συσταθεί στην Ένωση βάσει του δικαίου κράτους μέλους***·

– η υπεργολαβία αφορά κρίσιμη ή σημαντική λειτουργία της χρηματοπιστωτικής οντότητας·

– ***η υπεργολαβία θα οδηγήσει σε σοβαρούς και σαφείς κινδύνους για τη χρηματοπιστωτική οντότητα ή τη χρηματοπιστωτική σταθερότητα του χρηματοπιστωτικού συστήματος της Ένωσης.***

1β. ***Οι εξουσίες που αναφέρονται στις παραγράφους 1 και 1α ασκούνται όσον αφορά τις υπηρεσίες ΤΠΕ που υποστηρίζουν μη κρίσιμες ή σημαντικές λειτουργίες που παρέχονται από τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ, όταν είναι αναγκαίο.***

1γ. Κατά την άσκηση των εξουσιών που αναφέρονται στις παραγράφους 1 και 1α, ο κύριος εποπτικός φορέας και το όργανο κοινής εποπτείας λαμβάνουν δεόντως υπόψη το πλαίσιο που θεσπίστηκε με την οδηγία (ΕΕ) 2016/1148, και, όπου είναι αναγκαίο, διαβουλεύονται με τις σχετικές αρμόδιες αρχές που έχουν ορισθεί από εκείνη την οδηγία, προκειμένου να αποφευχθεί η περιττή επικάλυψη τεχνικών και οργανωσιακών μέτρων που ενδέχεται να ισχύουν για κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ σύμφωνα με εκείνη την οδηγία.

2. ***Πριν από την οριστικοποίηση και την έκδοση συστάσεων σύμφωνα με την παράγραφο 1 στοιχείο δ), το όργανο κοινής εποπτείας ενημερώνει τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ σχετικά με τις προθέσεις του και παρέχει στον τρίτο πάροχο υπηρεσιών ΤΠΕ την ευκαιρία να παράσχει πληροφορίες για τις οποίες ευλόγως πιστεύει ότι θα πρέπει να ληφθούν υπόψη πριν από την οριστικοποίηση της σύστασης ή προκειμένου να αμφισβητήσει τις συστάσεις που πρόκειται να εκδοθούν. Οι λόγοι αμφισβήτησης μιας σύστασης μπορεί να περιλαμβάνουν το ενδεχόμενο δυσανάλογου αντικτύπου ή διαταραχής σε πελάτες που δεν υπόκεινται στον παρόντα κανονισμό ή την ύπαρξη αποτελεσματικότερης ή αποδοτικότερης λύσης για τη διαχείριση του εντοπισθέντος κινδύνου.***

3. Οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ συνεργάζονται καλόπιστα ***και επικουρούν*** τον κύριο εποπτικό φορέα και ***το όργανο κοινής εποπτείας*** κατά την εκπλήρωση των καθηκόντων ***τους***.

4. Ο κύριος εποπτικός φορέας μπορεί ***να αποφασίσει, σε περίπτωση ολικής ή μερικής μη συμμόρφωσης με τα μέτρα που απαιτείται να ληφθούν σύμφωνα με την παράγραφο 1 στοιχεία α), β) ή γ), και μετά την εκπνοή περιόδου τουλάχιστον 60 ημερολογιακών ημερών από την ημερομηνία κατά την οποία ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ έλαβε κοινοποίηση του μέτρου,*** να επιβάλει περιοδική χρηματική ποινή για να υποχρεώσει τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ να συμμορφωθεί ▌.

4α. Η περιοδική χρηματική ποινή που αναφέρεται στην παράγραφο 4 επιβάλλεται από τον κύριο εποπτικό φορέα μόνο ως έσχατη λύση και σε περιπτώσεις στις οποίες ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ δεν έχει συμμορφωθεί με τα μέτρα που απαιτείται να ληφθούν σύμφωνα με την παράγραφο 1 στοιχεία α), β) ή γ).

5. Η περιοδική χρηματική ποινή που αναφέρεται στην παράγραφο 4 επιβάλλεται σε ημερήσια βάση έως ότου επιτευχθεί συμμόρφωση και για μέγιστο διάστημα έξι μηνών από την κοινοποίηση στον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ.

6. Το ύψος της περιοδικής χρηματικής ποινής, το οποίο υπολογίζεται από την ημερομηνία που ορίζεται στην απόφαση επιβολής της περιοδικής χρηματικής ποινής, ισούται ***το πολύ*** με το 1 % του μέσου ημερήσιου κύκλου εργασιών ***για υπηρεσίες που παρασχέθηκαν σε χρηματοπιστωτικές οντότητες που καλύπτονται από τον παρόντα κανονισμό*** που πραγματοποίησε παγκοσμίως ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ κατά την προηγούμενη χρήση.

7. 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.

8. Οι ΕΕΑ δημοσιοποιούν κάθε περιοδική χρηματική ποινή που έχει επιβληθεί, εκτός εάν η εν λόγω δημοσιοποίηση θέτει σε σοβαρό κίνδυνο τις χρηματοπιστωτικές αγορές ή προκαλεί δυσανάλογη ζημία στα εμπλεκόμενα μέρη.

9. Πριν από την επιβολή περιοδικής χρηματικής ποινής σύμφωνα με την παράγραφο 4, ο κύριος εποπτικός φορέας παρέχει στους εκπροσώπους του κρίσιμου τρίτου παρόχου ΤΠΕ που υπόκειται στην πειθαρχική διαδικασία, τη δυνατότητα να εκθέσουν την άποψή τους σχετικά με τα πορίσματα και στηρίζει τις αποφάσεις του μόνο σε πορίσματα για τα οποία είχε την ευκαιρία να διατυπώσει παρατηρήσεις ο κρίσιμος τρίτος πάροχος ΤΠΕ που υπόκειται στην πειθαρχική διαδικασία. Κατά τη διεξαγωγή της διαδικασίας διασφαλίζονται πλήρως τα δικαιώματα υπεράσπισης των προσώπων που υπόκεινται σε πειθαρχικές διαδικασίες. Τα πρόσωπα αυτά έχουν 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 32

Αιτήματα παροχής πληροφοριών

1. Ο κύριος εποπτικός φορέας δύναται να ζητήσει από τον κρίσιμο τρίτο πάροχο 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 ΤΠΕ έχει αναθέσει εξωτερικά επιχειρησιακές λειτουργίες ή δραστηριότητες.

Οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ υποχρεούνται να παρέχουν τις πληροφορίες που αναφέρονται στο πρώτο εδάφιο μόνο όσον αφορά τις υπηρεσίες που παρέχονται σε χρηματοπιστωτικές οντότητες που υπόκεινται στον παρόντα κανονισμό και χρησιμοποιούν τις υπηρεσίες κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ για κρίσιμες ή σημαντικές λειτουργίες. Οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ κοινοποιούν στην οικεία χρηματοπιστωτική οντότητα τα αιτήματα που αφορούν ειδικά την εν λόγω χρηματοπιστωτική οντότητα.

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) πληροφορεί 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 ***εύλογη*** προθεσμία εντός της οποίας πρέπει να παρασχεθούν οι πληροφορίες·

ε) επισημαίνει τις περιοδικές χρηματικές ποινές που προβλέπονται στο άρθρο 31 παράγραφος 4 στην περίπτωση ελλιπούς παροχής των απαιτούμενων πληροφοριών ***ή όταν οι πληροφορίες αυτές δεν παρέχονται εντός της προθεσμίας που αναφέρεται στο στοιχείο δ)***·

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

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 αποστέλλει αμελλητί αντίγραφο της απόφασης για την παροχή πληροφοριών στις αρμόδιες αρχές των χρηματοπιστωτικών οντοτήτων που χρησιμοποιούν υπηρεσίες των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ.

Άρθρο 33

Γενικές έρευνες

1. Για την εκτέλεση των καθηκόντων του σύμφωνα με τον παρόντα κανονισμό, ο κύριος εποπτικός φορέας, επικουρούμενος από την εξεταστική ομάδα που αναφέρεται στο άρθρο ***35*** παράγραφος 1, μπορεί να διεξαγάγει τις απαραίτητες έρευνες σε τρίτους παρόχους υπηρεσιών ΤΠΕ ***σύμφωνα με την αρχή της αναλογικότητας. Κατά τη διεξαγωγή ερευνών, ο κύριος εποπτικός φορέας επιδεικνύει σύνεση και διασφαλίζει την προστασία των δικαιωμάτων των πελατών των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ που δεν καλύπτονται από τον παρόντα κανονισμό, μεταξύ άλλων όσον αφορά τον αντίκτυπο στα επίπεδα υπηρεσιών, τη διαθεσιμότητα των δεδομένων και την εμπιστευτικότητα.***

2. Ο κύριος εποπτικός φορέας εξουσιοδοτείται:

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 επισκοπεί, με ασφαλή τρόπο,*** θεωρημένα αντίγραφα ή αποσπάσματα από τα εν λόγω αρχεία, τα δεδομένα, τις διαδικασίες και άλλο υλικό·

γ) να καλεί εκπροσώπους του 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 31 παράγραφος 4, όταν τα απαιτούμενα αρχεία, τα δεδομένα, οι 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 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 31 παράγραφος 4, 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 έρευνα, οι κύριοι εποπτικοί φορείς ενημερώνουν εγκαίρως την αρμόδια αρχή της χρηματοπιστωτικής οντότητας που χρησιμοποιεί τον οικείο τρίτο πάροχο υπηρεσιών ΤΠΕ σχετικά με την έρευνα και την ταυτότητα των εξουσιοδοτημένων προσώπων.

Άρθρο 34

Επιτόπιες επιθεωρήσεις

1. Για την εκπλήρωση των καθηκόντων του σύμφωνα με τον παρόντα κανονισμό, ο κύριος εποπτικός φορέας, επικουρούμενος από τις εξεταστικές ομάδες που αναφέρονται στο άρθρο 35 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 εκτός λειτουργίας.

Η εξουσία διενέργειας επιτόπιων επιθεωρήσεων που αναφέρονται στο πρώτο εδάφιο δεν περιορίζεται σε χώρους εντός της Ένωσης, υπό την προϋπόθεση ότι η επιθεώρηση χώρου σε τρίτη χώρα πληροί όλες τις ακόλουθες απαιτήσεις:

- ***είναι αναγκαία προκειμένου ο κύριος εποπτικός φορέας να εκτελέσει τα καθήκοντά του δυνάμει του παρόντος κανονισμού·***
- ***έχει άμεση σύνδεση με την παροχή υπηρεσιών ΤΠΕ σε χρηματοπιστωτικές οντότητες της Ένωσης·***
- ***έχει σημασία για διεξαγόμενη έρευνα.***

1α. Κατά τη διεξαγωγή επιτόπιων επιθεωρήσεων, ο κύριος εποπτικός φορέας και η ομάδα εξέτασης επιδεικνύουν σύνεση και διασφαλίζουν την προστασία των

δικαιωμάτων των πελατών των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ που δεν καλύπτονται από τον παρόντα κανονισμό, μεταξύ άλλων, όσον αφορά τον αντίκτυπο στα επίπεδα υπηρεσιών, τη διαθεσιμότητα των δεδομένων και την εμπιστευτικότητα.

2. Οι υπάλληλοι, καθώς και άλλα πρόσωπα που εξουσιοδοτούνται από τον κύριο εποπτικό φορέα να διενεργούν επιτόπια επιθεώρηση, μπορούν να εισέρχονται σε τέτοιου είδους επιχειρηματικούς χώρους, εκτάσεις ή ιδιοκτησίες και διαθέτουν όλες τις εξουσίες να σφραγίζουν τυχόν επιχειρηματικούς χώρους και βιβλία ή αρχεία για την περίοδο της επιθεώρησης και στον βαθμό που κρίνεται αναγκαίο για την επιθεώρηση αυτή.

   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 31 παράγραφος 4, σε περίπτωση που οι εκπρόσωποι των εν λόγω τρίτων παρόχων υπηρεσιών ΤΠΕ δεν αποδέχονται την επιθεώρηση.

3. Πριν από την επιθεώρηση, οι κύριοι εποπτικοί φορείς ενημερώνουν εγκαίρως τις αρμόδιες αρχές των χρηματοπιστωτικών οντοτήτων που χρησιμοποιούν τον εν λόγω τρίτο πάροχο ΤΠΕ.

4. Οι επιθεωρήσεις καλύπτουν το πλήρες φάσμα των σχετικών συστημάτων, δικτύων, συσκευών, πληροφοριών και δεδομένων ΤΠΕ ***που ο κύριος εποπτικός φορέας θεωρεί κατάλληλα και τεχνολογικά συναφή,*** τα οποία χρησιμοποιούνται ή συμβάλλουν στην παροχή υπηρεσιών προς χρηματοπιστωτικές οντότητες.

5. Πριν από κάθε προγραμματισμένη επιτόπια ***επιθεώρηση***, οι κύριοι εποπτικοί φορείς ειδοποιούν 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 έναρξής της και αναφέρει τις περιοδικές χρηματικές ποινές που προβλέπονται στο άρθρο 31 παράγραφος 4, τα ένδικα μέσα 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 καταγγελίας των συμβατικών ρυθμίσεων που έχουν συναφθεί με τον εν λόγω κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ από τις αρμόδιες αρχές των σχετικών χρηματοπιστωτικών οντοτήτων.

Άρθρο 35

Συνεχής εποπτεία

1. Κατά τη διεξαγωγή γενικών ερευνών ή επιτόπιων επιθεωρήσεων, οι κύριοι εποπτικοί φορείς επικουρούνται από την 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 του κύριου εποπτικού φορέα***, των άλλων ΕΕΑ,*** και των σχετικών αρμόδιων αρχών που εποπτεύουν τις χρηματοπιστωτικές οντότητες στις οποίες παρέχει υπηρεσίες ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ, και τα οποία θα συμμετέχουν στην κατάρτιση και την εκτέλεση των δραστηριοτήτων εποπτείας, με μέγιστο αριθμό 10 μελών. Όλα τα μέλη της κοινής εξεταστικής ομάδα διαθέτουν εμπειρογνωσία σε θέματα ΤΠΕ και λειτουργικού κινδύνου. Η κοινή εξεταστική ομάδα εκτελεί τις εργασίες της υπό τον συντονισμό ενός μέλους του προσωπικού των ΕΕΑ που ορίζεται για τον σκοπό αυτόν (στο εξής: συντονιστής κύριου εποπτικού φορέα).

3. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, καταρτίζουν κοινά σχέδια ρυθμιστικών τεχνικών προτύπων προκειμένου να προσδιοριστεί περαιτέρω ο διορισμός των μελών της κοινής εξεταστικής ομάδας που προέρχονται από τις σχετικές αρμόδιες αρχές, καθώς και τα καθήκοντα και τις ρυθμίσεις συνεργασίας της εξεταστικής ομάδας. Οι ΕΕΑ υποβάλλουν στην Επιτροπή τα εν λόγω σχέδια ρυθμιστικών τεχνικών προτύπων έως τη(ν) [ΕΕ: Να συμπληρωθεί ημερομηνία 1 έτος μετά την ημερομηνία έναρξης ισχύος].

   Ανατίθεται στην Επιτροπή η εξουσία να εγκρίνει 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, αντίστοιχα.

4. Εντός 3 μηνών από την ολοκλήρωση μιας έρευνας ή επιτόπιας επιθεώρησης, ***ο κύριος εποπτικός φορέας*** εγκρίνει συστάσεις τις οποίες πρέπει να απευθύνει στον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ σύμφωνα με τις εξουσίες που αναφέρονται στο άρθρο 31.

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

   Για την εκπλήρωση των δραστηριοτήτων εποπτείας, οι κύριοι εποπτικοί φορείς ***και το όργανο κοινής εποπτείας*** μπορούν να λαμβάνουν υπόψη τυχόν σχετικές πιστοποιήσεις τρίτων και εσωτερικές ή εξωτερικές εκθέσεις ελέγχου τρίτων παρόχων ΤΠΕ, τις οποίες θέτει στη διάθεσή τους ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ.

Άρθρο 36

Εναρμόνιση με τους όρους που καθιστούν δυνατή την άσκηση της εποπτείας

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

   α) τις πληροφορίες που πρέπει να παρέχονται από τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ κατά την εφαρμογή της προαιρετικής συμμετοχής που ορίζεται στο άρθρο 28 παράγραφος 8·

   β) το περιεχόμενο και τη μορφή των εκθέσεων που μπορεί να ζητηθούν για τους σκοπούς του άρθρου 31 παράγραφος 1 στοιχείο γ)·

   γ) την παρουσίαση των πληροφοριών, συμπεριλαμβανομένης της δομής, της μορφής και των μεθόδων, τις οποίες καλείται να υποβάλει, να γνωστοποιήσει ή να αναφέρει ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο

31 παράγραφος 1·

δ) τις λεπτομέρειες της αξιολόγησης όσον αφορά τα μέτρα που έλαβε ο τρίτος πάροχος υπηρεσιών ΤΠΕ βάσει των συστάσεων του ***κύριου εποπτικού φορέα*** σύμφωνα με το άρθρο 37 παράγραφος 2.

2. Οι ΕΕΑ υποβάλλουν στην Επιτροπή τα εν λόγω σχέδια ρυθμιστικών τεχνικών προτύπων έως την 1η Ιανουαρίου 20xx [ΕΕ: Να συμπληρωθεί ημερομηνία 1 έτος μετά την ημερομηνία έναρξης ισχύος].

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εκδίδοντας τα ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στο πρώτο εδάφιο, 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, αντίστοιχα.

Άρθρο 37

Συνέχεια που δίνεται από τις αρμόδιες αρχές

1. Εντός 30 ημερολογιακών ημερών από την παραλαβή των συστάσεων που ***εκδίδει το όργανο κοινής εποπτείας*** σύμφωνα με το άρθρο 31 ***παράγραφος 1α***, οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ ενημερώνουν ***το όργανο κοινής εποπτείας*** αν σκοπεύουν να ακολουθήσουν τις εν λόγω συστάσεις. ***Το όργανο κοινής εποπτείας διαβιβάζει*** αμέσως τις πληροφορίες αυτές στις αρμόδιες αρχές ***των σχετικών χρηματοπιστωτικών οντοτήτων***.

2. Οι αρμόδιες αρχές ***ενημερώνουν τις χρηματοπιστωτικές οντότητες που έχουν συνάψει συμβατικές ρυθμίσεις με κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ σχετικά με τους κινδύνους που προσδιορίζονται στις συστάσεις που απευθύνονται στους εν λόγω κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ από το όργανο κοινής εποπτείας σύμφωνα με το άρθρο 31 παράγραφος 1α και*** παρακολουθούν κατά πόσον οι χρηματοπιστωτικές οντότητες λαμβάνουν υπόψη τους εντοπισθέντες κινδύνους. ***Το όργανο κοινής εποπτείας παρακολουθεί κατά πόσον οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ έχουν αντιμετωπίσει τους κινδύνους που προσδιορίζονται στις εν λόγω συστάσεις.***

3. ***Όταν δεν είναι δυνατόν να εξασφαλιστούν με άλλα μέτρα οι ρυθμιστικοί στόχοι, και όταν έχουν εκδοθεί από τις εθνικές αρμόδιες αρχές προειδοποιήσεις προς τις θιγόμενες χρηματοπιστωτικές οντότητες με βάση πληροφορίες που έχουν διαβιβαστεί από το όργανο κοινής εποπτείας, το διοικητικό συμβούλιο του κύριου εποπτικού φορέα μπορεί να αποφασίσει, κατόπιν σύστασης του οργάνου κοινής εποπτείας και κατόπιν διαβούλευσης με τις αρμόδιες αρχές των θιγόμενων χρηματοπιστωτικών οντοτήτων*** να αναστείλουν προσωρινά, εν μέρει ή πλήρως, τη χρήση ή την ανάπτυξη μιας υπηρεσίας που παρέχεται ***σε χρηματοπιστωτικές οντότητες εκτεθειμένες*** στους κινδύνους που προσδιορίζονται στις συστάσεις που απευθύνονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ, έως ότου αντιμετωπιστούν οι κίνδυνοι αυτοί. Εάν κρίνεται σκόπιμο***, και ως μέτρο εσχάτης ανάγκης,*** μπορούν να ζητήσουν από ***τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ*** να προβούν σε μερική ή ολική καταγγελία των σχετικών συμβατικών ρυθμίσεων που έχουν συναφθεί με ***τις χρηματοπιστωτικές οντότητες που είναι εκτεθειμένες στους εντοπισθέντες κινδύνους***.

4. Κατά τη λήψη των αποφάσεων που αναφέρονται στην παράγραφο 3, ***το όργανο κοινής εποπτείας λαμβάνει*** 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 τους εσωτερικούς ελέγχους 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 τελέστηκε εκ προθέσεως ή εξ αμελείας.

δα) αν η αναστολή ή η καταγγελία ενέχει κίνδυνο ασυνέχειας για τις επιχειρηματικές λειτουργίες του χρήστη των υπηρεσιών του κρίσιμου τρίτου παρόχου υπηρεσιών ΤΠΕ.

4α. Οι αποφάσεις που προβλέπονται στην παράγραφο 3 εφαρμόζονται μόνον αφού ενημερωθούν δεόντως όλες οι θιγόμενες χρηματοπιστωτικές οντότητες. Στις θιγόμενες χρηματοπιστωτικές οντότητες παρέχεται χρονικό διάστημα, το οποίο δεν υπερβαίνει το απολύτως αναγκαίο, για να προσαρμόσουν την εξωτερική ανάθεση και τις συμβατικές ρυθμίσεις τους με κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ κατά τρόπο ώστε να μην τίθεται σε κίνδυνο η ψηφιακή επιχειρησιακή ανθεκτικότητα και να εκτελέσουν τις στρατηγικές εξόδου και τα σχέδια μετάβασης που αναφέρονται στο άρθρο 25.

Οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που υπόκεινται στις αποφάσεις που προβλέπονται στην παράγραφο 3 συνεργάζονται πλήρως με τις θιγόμενες χρηματοπιστωτικές οντότητες.

5. Οι αρμόδιες αρχές ενημερώνουν τακτικά ***το όργανο κοινής εποπτείας*** σχετικά με τις προσεγγίσεις και τα μέτρα που λαμβάνονται κατά την εκτέλεση των εποπτικών καθηκόντων τους σε σχέση με τις χρηματοπιστωτικές οντότητες.

Άρθρο 38

Εποπτικά τέλη

1. Οι ΕΕΑ χρεώνουν σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ τέλη, τα οποία καλύπτουν πλήρως τις απαιτούμενες δαπάνες των ΕΕΑ σε σχέση με την εκτέλεση καθηκόντων εποπτείας σύμφωνα με τον παρόντα κανονισμό, συμπεριλαμβανομένης της επιστροφής τυχόν δαπανών που ενδέχεται να προκύψουν λόγω των εργασιών των αρμόδιων αρχών που συμμετέχουν στις δραστηριότητες εποπτείας σύμφωνα με το άρθρο 35.

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.

1α. Εάν συναφθεί μια διοικητική ρύθμιση με ρυθμιστική και εποπτική αρχή τρίτης χώρας σύμφωνα με την παράγραφο 1 του παρόντος άρθρου, η εν λόγω αρχή μπορεί να αποτελεί μέρος της εξεταστικής ομάδας που αναφέρεται στο άρθρο 35 παράγραφος 1.

2. Ανατίθεται στην Επιτροπή η εξουσία να εκδώσει κατ' εξουσιοδότηση πράξη, σύμφωνα

με το άρθρο 50, για τη συμπλήρωση του παρόντος κανονισμού με τον προσδιορισμό του ύψους των τελών και του τρόπου καταβολής τους.

Άρθρο 39

Διεθνής συνεργασία

1. Η ΕΒΑ, η ESMA και η ΕΙΟΡΑ δύνανται, σύμφωνα με το άρθρο 33 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010, αντίστοιχα, να συνάπτουν διοικητικές ρυθμίσεις με κανονιστικές και εποπτικές αρχές τρίτων χωρών, με σκοπό την προώθηση της διεθνούς συνεργασίας όσον αφορά τον κίνδυνο τρίτων παρόχων ΤΠΕ σε διάφορους χρηματοπιστωτικούς 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 πορίσματα των σχετικών συζητήσεων που διεξάγονται με τις αρχές τρίτων χωρών που αναφέρονται στην παράγραφο 1, εστιάζοντας στην εξέλιξη του κινδύνου τρίτων παρόχων ΤΠΕ και στις συνέπειες που έχει για τη χρηματοπιστωτική σταθερότητα, την ακεραιότητα της αγοράς, την προστασία των επενδυτών ή τη λειτουργία της ενιαίας αγοράς.

ΚΕΦΑΛΑΙΟ VI

ΡΥΘΜΙΣΕΙΣ ΑΝΤΑΛΛΑΓΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

Άρθρο 40

Ρυθμίσεις ανταλλαγής πληροφοριών όσον αφορά στοιχεία και πληροφορίες για κυβερνοαπειλές

1. Οι χρηματοπιστωτικές οντότητες ***επιδιώκουν να*** ανταλλάσσουν μεταξύ τους ***και με τρίτους παρόχους υπηρεσιών ΤΠΕ*** στοιχεία και πληροφορίες για κυβερνοαπειλές, συμπεριλαμβανομένων των δεικτών έκθεσης σε κίνδυνο, τακτικών, τεχνικών και διαδικασιών, προειδοποιήσεων 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 χρηματοπιστωτικών οντοτήτων ***και των τρίτων παρόχων υπηρεσιών ΤΠΕ***, 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 αποκατάστασης·

   β) πραγματοποιείται στο πλαίσιο αξιόπιστων κοινοτήτων χρηματοπιστωτικών οντοτήτων ***και τρίτων παρόχων υπηρεσιών ΤΠΕ***·

   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[26] και των κατευθυντήριων γραμμών για την πολιτική ανταγωνισμού[27].

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, καθώς και τα επιχειρησιακά στοιχεία, συμπεριλαμβανομένης της χρήσης ειδικών πλατφορμών ΤΠ.

3. Οι χρηματοπιστωτικές 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.

---

26 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).

27 Ανακοίνωση της Επιτροπής – Κατευθυντήριες γραμμές για την εφαρμογή του άρθρου 101 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης στις συμφωνίες οριζόντιας συνεργασίας (ΕΕ C 11 της 14.1.2011, σ. 1).

ΚΕΦΑΛΑΙΟ VII

ΑΡΜΟΔΙΕΣ ΑΡΧΕΣ

Άρθρο 41

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 τις υποχρεώσεις που καθορίζονται στον 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, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 4 της οδηγίας 2013/36/ΕΕ, με την επιφύλαξη των συγκεκριμένων καθηκόντων που ανατίθενται στην ΕΚΤ βάσει του κανονισμού (ΕΕ) αριθ. 1024/2013·

β) για παρόχους υπηρεσιών πληρωμών, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 22 της οδηγίας (ΕΕ) 2015/2366·

γ) για ιδρύματα ηλεκτρονικών πληρωμών, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 37 της οδηγίας 2009/110/ΕΚ·

δ) για επιχειρήσεις επενδύσεων, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 4 της οδηγίας (ΕΕ) 2019/2034·

ε) για παρόχους υπηρεσιών κρυπτοστοιχείων, εκδότες ***και προσφέροντες*** κρυπτοστοιχείων, εκδότες ***και προσφέροντες*** ψηφιακών κερμάτων με εγγύηση περιουσιακών στοιχείων και εκδότες σημαντικών ψηφιακών κερμάτων με εγγύηση περιουσιακών στοιχείων, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 3 παράγραφος 1 στοιχείο λα) πρώτη περίπτωση του [κανονισμού (ΕΕ) 20xx, κανονισμός MICA]·

στ) για κεντρικά αποθετήρια τίτλων ***και διαχειριστές συστημάτων διακανονισμού τίτλων***, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 11 του κανονισμού (ΕΕ) αριθ. 909/2014·

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

η) για τόπους διαπραγμάτευσης και παρόχους υπηρεσιών αναφοράς δεδομένων, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 67 της οδηγίας 2014/65/ΕΕ·

θ) για αρχεία καταγραφής συναλλαγών, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 55 του κανονισμού (ΕΕ) αριθ. 648/2012·

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

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

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

ιγ) 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·

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

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

ιστ) για νόμιμους ελεγκτές και ελεγκτικά γραφεία, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 3 παράγραφος 2 και το άρθρο 32 της οδηγίας 2006/43/ΕΚ·

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

ιη) για παρόχους υπηρεσιών πληθοχρηματοδότησης, την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο ***29*** του κανονισμού ***(ΕΕ) 2020/1503***·

ιθ) 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 42

Συνεργασία με δομές και αρχές που έχουν συγκροτηθεί βάσει της οδηγίας (ΕΕ) 2016/1148

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 11 της οδηγίας (ΕΕ) 2016/1148, οι ΕΕΑ και οι αρμόδιες αρχές ***καλούνται*** να συμμετέχουν στις εργασίες της ομάδας συνεργασίας ***στον βαθμό που οι εργασίες αυτές αφορούν δραστηριότητες επίβλεψης και εποπτείας, αντίστοιχα, σε σχέση με οντότητες που αναφέρονται στο σημείο 7 του παραρτήματος ΙΙ της οδηγίας (ΕΕ) 2016/1148, οι οποίες έχουν επίσης χαρακτηριστεί ως κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 28 του παρόντος κανονισμού***.

2. Οι αρμόδιες αρχές μπορούν να διαβουλεύονται, εφόσον κρίνεται σκόπιμο, με το ενιαίο σημείο επαφής και τις εθνικές ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών που αναφέρονται, αντίστοιχα, στα άρθρα 8 και 9 της οδηγίας (ΕΕ) 2016/1148.

2α. Ο κύριος εποπτικός φορέας ενημερώνει και συνεργάζεται με τις αρμόδιες αρχές που ορίζονται βάσει της οδηγίας (ΕΕ) 2016/1148 πριν από τη διεξαγωγή γενικών ερευνών και επιτόπιων επιθεωρήσεων σύμφωνα με τα άρθρα 33 και 34 του παρόντος κανονισμού.

Άρθρο 43

Ασκήσεις, επικοινωνία και συνεργασία μεταξύ των χρηματοπιστωτικών τομέων

1. Οι ΕΕΑ, μέσω της μεικτής επιτροπής και σε συνεργασία με τις αρμόδιες αρχές, την

ΕΚΤ***, το Ενιαίο Συμβούλιο Εξυγίανσης σε σχέση με πληροφορίες που αφορούν τις οντότητες που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού (ΕΕ) αριθ. 806/2014*** και τον ΕΣΣΚ, μπορούν να θεσπίσουν μηχανισμούς ώστε να είναι δυνατή η ανταλλαγή αποτελεσματικών πρακτικών μεταξύ των χρηματοπιστωτικών 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 την εξασφάλιση της δυνατότητας αποτελεσματικής συντονισμένης απόκρισης σε επίπεδο ΕΕ, σε περίπτωση σημαντικού διασυνοριακού συμβάντος που σχετίζεται με τις ΤΠΕ ή ***σημαντικής κυβερνοαπειλής*** με συστημικές επιπτώσεις στον χρηματοπιστωτικό τομέα της Ένωσης συνολικά.

Στο πλαίσιο των ασκήσεων αυτών παρέχεται, κατά περίπτωση, η δυνατότητα δοκιμής των εξαρτήσεων του χρηματοπιστωτικού τομέα από άλλους οικονομικούς τομείς.

2. Οι αρμόδιες αρχές, η ΕΒΑ, η ESMA ή η ΕΙΟΡΑ, η ΕΚΤ, ***οι εθνικές αρχές εξυγίανσης και το Ενιαίο Συμβούλιο Εξυγίανσης όσον αφορά τις πληροφορίες που εμπίπτουν στο πεδίο του κανονισμού (ΕΕ) αριθ. 806/2014*** συνεργάζονται στενά μεταξύ τους και ανταλλάσσουν πληροφορίες στο πλαίσιο της εκτέλεσης των καθηκόντων τους, σύμφωνα με τα άρθρα 42 έως 48. 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 44

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 εξουσίες:

   α) να έχουν 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) να διενεργούν επιτόπιους ελέγχους ή έρευνες·

   γ) να ζητούν τη λήψη διορθωτικών μέτρων και μέτρων αποκατάστασης για παραβιάσεις των απαιτήσεων του παρόντος κανονισμού.

3. Με την επιφύλαξη του δικαιώματος των κρατών μελών να επιβάλλουν ποινικές κυρώσεις σύμφωνα με το άρθρο 46, 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 των 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 διακόψει τη συμπεριφορά του και να μην την επαναλάβει·

   β) να απαιτούν την προσωρινή ή οριστική διακοπή κάθε πρακτικής ή συμπεριφοράς που ***θεωρείται*** 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 χρηματοπιστωτικές 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 οι διατάξεις της παραγράφου 2 στοιχείο γ) και της παραγράφου 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 διατάξεων 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 45

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 44 σύμφωνα με το εκάστοτε εθνικό νομικό πλαίσιο, ανάλογα με την περίπτωση:

   α) άμεσα·

   β) σε συνεργασία με άλλες αρχές·

   γ) υπό την ευθύνη τους με ανάθεση καθηκόντων σε άλλες αρχές·

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 44, λαμβάνουν υπόψη αν η παραβίαση τελέστηκε εκ προθέσεως ή εξ αμελείας, καθώς και όλες τις άλλες σχετικές περιστάσεις, μεταξύ των οποίων, 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 διασφάλισης της παραίτησης από αποκτηθέντα κέρδη ή αποφευχθείσες ζημίες,

ζ) προηγούμενες παραβιάσεις του υπαίτιου φυσικού ή νομικού προσώπου.

Άρθρο 46

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 είναι εξουσιοδοτημένες 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 ΕΒΑ, την ESMA και την ΕΙΟΡΑ, στο πλαίσιο της τήρησης των υποχρεώσεών τους όσον αφορά τη συνεργασία για τους σκοπούς του παρόντος κανονισμού.

Άρθρο 47

Υποχρεώσεις κοινοποίησης

Τα κράτη μέλη κοινοποιούν στην Επιτροπή, την ESMA, την ΕΒΑ και την ΕΙΟΡΑ τις νομικές, κανονιστικές και διοικητικές διατάξεις για την εφαρμογή του παρόντος κεφαλαίου, συμπεριλαμβανομένων τυχόν διατάξεων του ποινικού δικαίου, έως τη(ν) [ΕΕ: Να συμπληρωθεί ημερομηνία ***12 μήνες*** μετά την ημερομηνία έναρξης ισχύος]. Τα κράτη μέλη

κοινοποιούν στην Επιτροπή, την ESMA, την EBA και την EIOPA, χωρίς αδικαιολόγητη καθυστέρηση, κάθε μεταγενέστερη τροποποίησή τους.

Άρθρο 48

Δημοσιοποίηση των 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, ***τις ποινές που επιβλήθηκαν και, κατ' εξαίρεση,*** 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, θα έθετε σε κίνδυνο τη σταθερότητα των χρηματοπιστωτικών 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 τη χρονική στιγμή που παύουν να συντρέχουν οι λόγοι για τη μη δημοσίευσή της·

   β) τη δημοσιεύει σε ανώνυμη βάση, σύμφωνα με την εθνική νομοθεσία· ή

   γ) αποφεύγει 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 χρηματοπιστωτικών αγορών ή σε περίπτωση που η δημοσίευση δεν θα ήταν ανάλογη με την επιείκεια της επιβληθείσας κύρωσης.

4. Σε περίπτωση απόφασης για ανώνυμη δημοσίευση διοικητικής κύρωσης 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 περί 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 τουλάχιστον για χρονικό διάστημα πέντε ετών από τη δημοσίευση. Τα δεδομένα προσωπικού χαρακτήρα που περιλαμβάνονται στη δημοσίευση τηρούνται μόνον στον επίσημο δικτυακό τόπο της αρμόδιας αρχής για το χρονικό διάστημα που απαιτείται σύμφωνα με τους ισχύοντες κανόνες για την προστασία των δεδομένων προσωπικού χαρακτήρα.

Άρθρο 49

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 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.

ΚΕΦΑΛΑΙΟ VIII

ΚΑΤ' ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΠΡΑΞΕΙΣ

Άρθρο 50

Άσκηση της εξουσιοδότησης

1. Η εξουσία έκδοσης κατ' εξουσιοδότηση πράξεων ανατίθεται στην Επιτροπή υπό τους όρους του παρόντος άρθρου.

2. Η προβλεπόμενη στο άρθρο 28 παράγραφος 3 και στο άρθρο 38 παράγραφος 2 εξουσία έκδοσης κατ' εξουσιοδότηση πράξεων ανατίθεται στην Επιτροπή για περίοδο πέντε ετών από τη(ν) [Υπηρεσία Εκδόσεων: Να συμπληρωθεί ημερομηνία 5 έτη μετά την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού]. ***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 28 παράγραφος 3 και στο άρθρο 38 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 τη εγκυρότητα των κατ' εξουσιοδότηση πράξεων που ισχύουν ήδη.

4. Πριν από την έκδοση 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. Η Επιτροπή, μόλις εκδώσει κατ' εξουσιοδότηση πράξη, την κοινοποιεί ταυτοχρόνως στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο.

6. Οι κατ' εξουσιοδότηση πράξεις που εκδίδονται σύμφωνα με το άρθρο 28 παράγραφος 3 και το άρθρο 38 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

ΜΕΤΑΒΑΤΙΚΕΣ ΚΑΙ ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

ΤΜΗΜΑ I

Άρθρο 51

Ρήτρα επανεξέτασης

Έως τη(ν) [Υπηρεσία Εκδόσεων: Να συμπληρωθεί ημερομηνία 5 έτη μετά την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού], η Επιτροπή, κατόπιν διαβούλευσης με την ΕΒΑ, την ESMA, την ΕΙΟΡΑ και την ΕΕΣΚ, ανάλογα με την περίπτωση, επανεξετάζει και υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο έκθεση σχετικά με τα κριτήρια ορισμού των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ του άρθρου 28 παράγραφος 2, συνοδευόμενη από νομοθετική πρόταση, εφόσον ενδείκνυται. ***Η έκθεση περιέχει τουλάχιστον τα ακόλουθα:***

α) ***τη δυνατότητα επέκτασης του πεδίου εφαρμογής του παρόντος κανονισμού στους φορείς εκμετάλλευσης συστημάτων πληρωμών·***

β) ***τον εθελοντικό χαρακτήρα της κοινοποίησης για σημαντικές κυβερνοαπειλές·***

γ) τα κριτήρια ορισμού των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ του άρθρου 28 παράγραφος 2· ***και***

δ) ***την αποτελεσματικότητα της λήψης αποφάσεων του οργάνου κοινής εποπτείας και την ανταλλαγή πληροφοριών μεταξύ του οργάνου κοινής εποπτείας και των αρμόδιων εθνικών αρχών που δεν είναι μέλη.***

ΤΜΗΜΑ ΙΙ

ΤΡΟΠΟΠΟΙΗΣΕΙΣ

Άρθρο 52

Τροποποιήσεις του κανονισμού (ΕΚ) αριθ. 1060/2009

Στο παράρτημα Ι του κανονισμού (ΕΚ) αριθ. 1060/2009, το πρώτο εδάφιο του σημείου 4 της ενότητας Α 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) 2021/xx του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου* [DORA].

* Κανονισμός (ΕΕ) 2021/xx του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου […] (ΕΕ L XX της ΗΗ.ΜΜ.ΕΕΕΕ, σ. Χ).».

Άρθρο 53

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) 2021/xx του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου* [DORA].

* Κανονισμός (ΕΕ) 2021/xx του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου […] (ΕΕ L XX της ΗΗ.ΜΜ.ΕΕΕΕ, σ. Χ).»·

β) η παράγραφος 6 απαλείφεται·

(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 αδιάλειπτης λειτουργίας και σχέδιο αποκατάστασης λειτουργίας μετά από καταστροφή, στα οποία περιλαμβάνονται σχέδια αδιάλειπτης λειτουργίας και αποκατάστασης λειτουργίας των ΤΠΕ μετά από καταστροφή που καταρτίζονται σύμφωνα με τον κανονισμό (ΕΕ) 2021/xx [DORA], 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:

«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 αδιάλειπτης λειτουργίας και του σχεδίου αποκατάστασης λειτουργίας μετά από καταστροφή, με εξαίρεση τα σχέδια αδιάλειπτης λειτουργίας και αποκατάστασης 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 αντικαθίστανται από το ακόλουθο κείμενο:

«1. Το αρχείο καταγραφής συναλλαγών εντοπίζει τις πηγές λειτουργικού κινδύνου και τις ελαχιστοποιεί, με την ανάπτυξη κατάλληλων συστημάτων, ελέγχων και διαδικασιών, συμπεριλαμβανομένων συστημάτων ΤΠΕ τα οποία διαχειρίζεται σύμφωνα με τον κανονισμό (ΕΕ) 2021/xx [DORA].

2. Το αρχείο καταγραφής συναλλαγών διαμορφώνει, εφαρμόζει και διατηρεί κατάλληλη πολιτική αδιάλειπτης λειτουργίας και σχέδιο αποκατάστασης λειτουργίας μετά από καταστροφή, συμπεριλαμβανομένων σχεδίων αδιάλειπτης λειτουργίας και αποκατάστασης λειτουργίας των ΤΠΕ μετά από καταστροφή τα οποία καταρτίζονται σύμφωνα με τον κανονισμό (ΕΕ) 2021/xx [DORA], 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 απαλείφεται.

Άρθρο 54

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 αντίκτυπο τους μέσω της χρησιμοποίησης κατάλληλων εργαλείων, διαδικασιών και πολιτικών ΤΠΕ που έχουν θεσπιστεί και τελούν υπό διαχείριση σύμφωνα με τον κανονισμό (ΕΕ) 2021/xx του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου* [DORA], καθώς και μέσω οποιωνδήποτε άλλων σχετικών κατάλληλων εργαλείων, ελέγχων και διαδικασιών για άλλα είδη λειτουργικού κινδύνου, μεταξύ άλλων για όλα τα συστήματα διακανονισμού αξιογράφων που διαχειρίζεται.

* Κανονισμός (ΕΕ) 2021/xx του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου […] (ΕΕ L XX της ΗΗ.ΜΜ.ΕΕΕΕ, σ. Χ).»·

(2) η παράγραφος 2 απαλείφεται·

(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 αδιάλειπτης λειτουργίας και σχέδιο αποκατάστασης λειτουργίας μετά από καταστροφή, συμπεριλαμβανομένων σχεδίων αδιάλειπτης λειτουργίας και αποκατάστασης λειτουργίας των ΤΠΕ μετά από καταστροφή τα οποία καταρτίζονται σύμφωνα με τον κανονισμό (ΕΕ) 2021/xx [DORA], για να διασφαλίσει τη διατήρηση των λειτουργιών του, την έγκαιρη αποκατάσταση των εργασιών και την εκπλήρωση των υποχρεώσεων του ΚΑΤ, σε περίπτωση γεγονότων που συνεπάγονται σημαντικό κίνδυνο διακοπής 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 διακοπής, όπως προβλέπεται στο άρθρο 11 παράγραφοι 5 και 7 του κανονισμού (ΕΕ) 2021/xx [DORA].»·

Άρθρο 55

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 απαλείφεται·

β) στην παράγραφο 8, το στοιχείο γ) αντικαθίσταται από το ακόλουθο κείμενο:

γ) «γ) τις συγκεκριμένες οργανωτικές απαιτήσεις που ορίζονται στις παραγράφους 3 και 5.»·

(2) το άρθρο 27η τροποποιείται ως εξής:

α) η παράγραφος 5 απαλείφεται·

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 απαλείφεται·

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 56

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 τη(ν) [Υπηρεσία Εκδόσεων: Να συμπληρωθεί ημερομηνία – 24 μήνες μετά

την ημερομηνία έναρξης ισχύος].

Ωστόσο, τα άρθρα 23 και 24 εφαρμόζονται από τη(ν) [Υπηρεσία Εκδόσεων: Να συμπληρωθεί ημερομηνία – 36 μήνες μετά την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού].

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Βρυξέλλες,

Για το Ευρωπαϊκό Κοινοβούλιο	*Για το Συμβούλιο*
Ο Πρόεδρος	*Ο Πρόεδρος*

ΔΙΑΔΙΚΑΣΙΑ ΤΗΣ ΑΡΜΟΔΙΑΣ ΕΠΙ ΤΗΣ ΟΥΣΙΑΣ ΕΠΙΤΡΟΠΗΣ

Τίτλος	Ψηφιακή επιχειρησιακή ανθεκτικότητα για τον χρηματοπιστωτικό τομέα και τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και (ΕΕ) αριθ. 909/2014
Έγγραφα αναφοράς	COM(2020)0595 – C9-0304/2020 – 2020/0266(COD)
Ημερομηνία υποβολής στο ΕΚ	24.9.2020
Επιτροπή αρμόδια επί της ουσίας Ημερομ. αναγγελίας στην Ολομέλεια	ECON 17.12.2020
Γνωμοδοτικές επιτροπές Ημερομ. αναγγελίας στην Ολομέλεια	ITRE 17.12.2020 IMCO 17.12.2020
Αποφάσισε να μη γνωμοδοτήσει Ημερομηνία της απόφασης	ITRE 15.10.2020 IMCO 27.10.2020
Εισηγητές Ημερομηνία ορισμού	Billy Kelleher 15.10.2020
Εξέταση στην επιτροπή	14.4.2021 14.6.2021
Ημερομηνία έγκρισης	1.12.2021
Αποτέλεσμα της τελικής ψηφοφορίας	+: 44 –: 5 0: 5
Βουλευτές παρόντες κατά την τελική ψηφοφορία	Gerolf Annemans, Gunnar Beck, Marek Belka, Isabel Benjumea Benjumea, Stefan Berger, Gilles Boyer, Engin Eroglu, Markus Ferber, Jonás Fernández, Raffaele Fitto, Frances Fitzgerald, Luis Garicano, Sven Giegold, Valentino Grant, Claude Gruffat, José Gusmão, Enikő Győri, Eero Heinäluoma, Danuta Maria Hübner, Stasys Jakeliūnas, France Jamet, Billy Kelleher, Ondřej Kovařík, Γεώργιος Κύρτσος, Aurore Lalucq, Philippe Lamberts, Aušra Maldeikienė, Pedro Marques, Κώστας Μαυρίδης, Jörg Meuthen, Csaba Molnár, Siegfried Mureşan, Caroline Nagtegaal, Luděk Niedermayer, Λευτέρης Νικολάου-Αλαβάνος, Lídia Pereira, Kira Marie Peter-Hansen, Sirpa Pietikäinen, Evelyn Regner, Antonio Maria Rinaldi, Alfred Sant, Martin Schirdewan, Joachim Schuster, Ralf Seekatz, Pedro Silva Pereira, Paul Tang, Irene Tinagli, Ernest Urtasun, Inese Vaidere, Johan Van Overtveldt, Stéphanie Yon-Courtin, Marco Zanni, Roberts Zīle
Αναπληρωτές παρόντες κατά την τελική ψηφοφορία	Λευτέρης Χριστοφόρου
Ημερομηνία κατάθεσης	7.12.2021

ΤΕΛΙΚΗ ΨΗΦΟΦΟΡΙΑ ΜΕ ΟΝΟΜΑΣΤΙΚΗ ΚΛΗΣΗ ΣΤΗΝ ΑΡΜΟΔΙΑ ΕΠΙ ΤΗΣ ΟΥΣΙΑΣ ΕΠΙΤΡΟΠΗ

44	+
ECR	Raffaele Fitto, Johan Van Overtveldt, Roberts Zīle
NI	Enikő Győri
PPE	Isabel Benjumea Benjumea, Stefan Berger, Λευτέρης Χριστοφόρου, Markus Ferber, Frances Fitzgerald, Danuta Maria Hübner, Γεώργιος Κύρτσος, Aušra Maldeikienė, Siegfried Mureşan, Luděk Niedermayer, Lídia Pereira, Sirpa Pietikäinen, Ralf Seekatz, Inese Vaidere
Renew	Gilles Boyer, Engin Eroglu, Luis Garicano, Billy Kelleher, Ondřej Kovařík, Caroline Nagtegaal, Stéphanie Yon-Courtin
S&D	Marek Belka, Jonás Fernández, Eero Heinäluoma, Aurore Lalucq, Pedro Marques, Κώστας Μαυρίδης, Csaba Molnár, Evelyn Regner, Alfred Sant, Joachim Schuster, Pedro Silva Pereira, Paul Tang, Irene Tinagli
Verts/ALE	Sven Giegold, Claude Gruffat, Stasys Jakeliūnas, Philippe Lamberts, Kira Marie Peter-Hansen, Ernest Urtasun

5	-
ID	Gerolf Annemans, Gunnar Beck, France Jamet, Jörg Meuthen
NI	Λευτέρης Νικολάου-Αλαβάνος

5	0
ID	Valentino Grant, Antonio Maria Rinaldi, Marco Zanni
The Left	José Gusmão, Martin Schirdewan

Υπόμνημα των χρησιμοποιούμενων συμβόλων:
+ : υπέρ
- : κατά
0 : αποχή