ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 24.9.2020
COM(2020) 595 final

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)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ

1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ

- Αιτιολόγηση και στόχοι της πρότασης

Η παρούσα πρόταση αποτελεί μέρος της δέσμης μέτρων για τον ψηφιακό χρηματοοικονομικό τομέα, σκοπός της οποίας είναι να διευκολύνει και να στηρίξει περαιτέρω τις δυνατότητες του ψηφιακού χρηματοοικονομικού τομέα όσον αφορά την καινοτομία και τον ανταγωνισμό, μετριάζοντας παράλληλα τους κινδύνους. Συνάδει με τις προτεραιότητες της Επιτροπής όσον αφορά την προετοιμασία της Ευρώπης για την ψηφιακή εποχή και την οικοδόμηση μιας οικονομίας στην υπηρεσία των πολιτών που θα είναι έτοιμη για το μέλλον. Η δέσμη μέτρων για τον ψηφιακό χρηματοοικονομικό τομέα περιλαμβάνει μια νέα στρατηγική ψηφιακών χρηματοοικονομικών υπηρεσιών για τον χρηματοπιστωτικό τομέα της ΕΕ[1], η οποία αποσκοπεί να διασφαλίσει ότι η ΕΕ θα προσχωρήσει στην ψηφιακή επανάσταση και θα ηγηθεί αυτής, με επικεφαλής καινοτόμες ευρωπαϊκές επιχειρήσεις, θέτοντας τα οφέλη του ψηφιακού χρηματοοικονομικού τομέα στη διάθεση των καταναλωτών και των επιχειρήσεων. Επιπλέον της παρούσας πρότασης, η δέσμη μέτρων περιλαμβάνει επίσης πρόταση κανονισμού για τις αγορές κρυπτοστοιχείων[2], πρόταση κανονισμού σχετικά με ένα πιλοτικό καθεστώς για τις υποδομές της αγοράς που βασίζονται σε τεχνολογία κατανεμημένου καθολικού (DLT)[3] και πρόταση οδηγίας για την αποσαφήνιση ή την τροποποίηση ορισμένων συναφών κανόνων της ΕΕ για τις χρηματοπιστωτικές υπηρεσίες[4]. Η ψηφιοποίηση και η επιχειρησιακή ανθεκτικότητα στον χρηματοπιστωτικό τομέα αποτελούν τις δύο όψεις του ίδιου νομίσματος. Οι ψηφιακές τεχνολογίες, ή οι τεχνολογίες των πληροφοριών και των επικοινωνιών (ΤΠΕ), συνεπάγονται τόσο ευκαιρίες όσο και κινδύνους. Οι εν λόγω ευκαιρίες και κίνδυνοι πρέπει να εμπεδωθούν και να αποτελέσουν αντικείμενο ορθής διαχείρισης, ιδίως σε περιόδους ακραίων καταστάσεων.

Ως εκ τούτου, οι υπεύθυνοι χάραξης πολιτικής και οι εποπτικές αρχές εστιάζουν ολοένα και περισσότερο στους κινδύνους που οφείλονται στην εξάρτηση από τις ΤΠΕ. Ειδικότερα, έχουν προσπαθήσει να ενισχύσουν την ανθεκτικότητα των επιχειρήσεων μέσω του καθορισμού προτύπων και μέσω του συντονισμού των ρυθμιστικών ή εποπτικών εργασιών. Οι εργασίες αυτές πραγματοποιήθηκαν σε διεθνές αλλά και σε ευρωπαϊκό επίπεδο, σε όλους τους κλάδους αλλά και σε ορισμένους συγκεκριμένους τομείς, συμπεριλαμβανομένων των χρηματοπιστωτικών υπηρεσιών.

Ωστόσο, οι κίνδυνοι ΤΠΕ εξακολουθούν να συνιστούν πρόκληση για την επιχειρησιακή ανθεκτικότητα, τις επιδόσεις και τη σταθερότητα του χρηματοπιστωτικού συστήματος της ΕΕ. Η μεταρρύθμιση που ακολούθησε μετά τη χρηματοπιστωτική κρίση του 2008 ενίσχυσε

---

1 Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Κεντρική Τράπεζα, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών σχετικά με μια Στρατηγική ψηφιακών χρηματοοικονομικών υπηρεσιών για την ΕΕ, COM(2020) 591 της 24ης Σεπτεμβρίου 2020.

2 Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις αγορές κρυπτοστοιχείων και την τροποποίηση της οδηγίας (ΕΕ) 2019/1937, COM(2020) 593.

3 Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ένα πιλοτικό καθεστώς για τις υποδομές της αγοράς που βασίζονται σε τεχνολογία κατανεμημένου καθολικού, COM(2020) 594.

4 Πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την τροποποίηση των οδηγιών 2006/43/ΕΚ, 2009/65/ΕΚ, 2009/138/ΕΕ, 2011/61/ΕΕ, ΕΕ/2013/36, 2014/65/ΕΕ, (ΕΕ) 2015/2366 και ΕΕ/2016/2341, COM(2020) 596.

πρωτίστως τη χρηματοπιστωτική ανθεκτικότητα[5] του χρηματοπιστωτικού τομέα της ΕΕ, με την έμμεση μόνο αντιμετώπιση των κινδύνων ΤΠΕ σε ορισμένους τομείς, στο πλαίσιο των μέτρων για την ευρύτερη αντιμετώπιση των λειτουργικών κινδύνων.

Παρότι με τις αλλαγές που επήλθαν μετά την κρίση στη νομοθεσία της ΕΕ για τις χρηματοπιστωτικές υπηρεσίες θεσπίστηκε ένα ενιαίο εγχειρίδιο κανόνων το οποίο διέπει μεγάλα τμήματα των χρηματοοικονομικών κινδύνων που συνδέονται με τις χρηματοπιστωτικές υπηρεσίες, δεν αντιμετωπίστηκε πλήρως το ζήτημα της ψηφιακής επιχειρησιακής ανθεκτικότητας. Τα μέτρα που λήφθηκαν σε σχέση με το ζήτημα αυτό διέπονταν από ορισμένα χαρακτηριστικά που περιόριζαν την αποτελεσματικότητά τους. Για παράδειγμα, ήταν συχνά σχεδιασμένα ως οδηγίες ελάχιστης εναρμόνισης ή κανονισμοί βάσει αρχών, με συνέπεια να αφήνουν σημαντικά περιθώρια για αποκλίνουσες προσεγγίσεις σε ολόκληρη την ενιαία αγορά. Επιπλέον, διαπιστώθηκε περιορισμένη ή πλημμελής μόνο εστίαση στους κινδύνους ΤΠΕ στο πλαίσιο της κάλυψης του λειτουργικού κινδύνου. Τέλος, τα μέτρα αυτά διαφοροποιούνται στην τομεακή νομοθεσία για τις χρηματοπιστωτικές υπηρεσίες. Κατά συνέπεια, η παρέμβαση σε επίπεδο Ένωσης δεν ανταποκρινόταν πλήρως στις ανάγκες των ευρωπαϊκών χρηματοπιστωτικών οντοτήτων για τη διαχείριση των λειτουργικών κινδύνων κατά τέτοιον τρόπο ώστε να ανθίστανται στις επιπτώσεις των συμβάντων ΤΠΕ, να τις αντιμετωπίζουν και να ανακάμπτουν από αυτές. Επιπροσθέτως, δεν παρείχε στις αρχές χρηματοπιστωτικής εποπτείας τα πλέον κατάλληλα εργαλεία για την εκπλήρωση των εντολών τους όσον αφορά την πρόληψη της χρηματοπιστωτικής αστάθειας που οφείλεται στους εν λόγω κινδύνους ΤΠΕ.

Η απουσία λεπτομερών και ολοκληρωμένων κανόνων για την ψηφιακή επιχειρησιακή ανθεκτικότητα σε επίπεδο ΕΕ είχε ως αποτέλεσμα τον πολλαπλασιασμό των κανονιστικών πρωτοβουλιών (π.χ. σχετικά με τις δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας) και των εποπτικών προσεγγίσεων (π.χ. για την αντιμετώπιση της εξάρτησης από τρίτους παρόχους ΤΠΕ) σε εθνικό επίπεδο. Ωστόσο, η ανάληψη δράσης σε επίπεδο κρατών μελών έχει περιορισμένο μόνο αντίκτυπο, δεδομένου του διασυνοριακού χαρακτήρα των κινδύνων ΤΠΕ. Επιπλέον, οι μη συντονισμένες εθνικές πρωτοβουλίες έχουν οδηγήσει σε αλληλεπικαλύψεις, ασυνέπειες, επαναλαμβανόμενες απαιτήσεις, υψηλό διοικητικό κόστος και κόστος συμμόρφωσης —ιδίως για τις διασυνοριακές χρηματοπιστωτικές οντότητες— ή σε κινδύνους ΤΠΕ που εξακολουθούν να μην εντοπίζονται και, συνεπώς, να μην αντιμετωπίζονται. Η κατάσταση αυτή κατακερματίζει την ενιαία αγορά, υπονομεύει τη σταθερότητα και την ακεραιότητα του χρηματοπιστωτικού τομέα της ΕΕ, ενώ θέτει επίσης σε κίνδυνο την προστασία των καταναλωτών και των επενδυτών.

Ως εκ τούτου, είναι απαραίτητο να θεσπιστεί ένα λεπτομερές και ολοκληρωμένο πλαίσιο για την ψηφιακή επιχειρησιακή ανθεκτικότητα των χρηματοπιστωτικών οντοτήτων της ΕΕ. Το πλαίσιο αυτό θα εμβαθύνει τη διάσταση της διαχείρισης ψηφιακού κινδύνου του ενιαίου εγχειριδίου κανόνων. Ειδικότερα, θα ενισχύσει και θα εξορθολογίσει την άσκηση της διαχείρισης κινδύνων ΤΠΕ από τις χρηματοπιστωτικές οντότητες, θα καθιερώσει διεξοδικές δοκιμές των συστημάτων ΤΠΕ, θα αυξήσει την ευαισθητοποίηση των εποπτικών αρχών όσον αφορά κινδύνους στον κυβερνοχώρο και τα συμβάντα που σχετίζονται με τις ΤΠΕ, τα οποία αντιμετωπίζουν οι χρηματοπιστωτικές οντότητες, ενώ θα θεσπίσει επίσης εξουσίες για τις αρχές χρηματοπιστωτικής εποπτείας ώστε να παρακολουθούν τους κινδύνους που οφείλονται στην εξάρτηση των χρηματοπιστωτικών οντοτήτων από τρίτους παρόχους υπηρεσιών ΤΠΕ.

[5] Τα διάφορα μέτρα που θεσπίστηκαν αποσκοπούσαν ουσιαστικά στην αύξηση των κεφαλαίων και της ρευστότητας των χρηματοπιστωτικών οντοτήτων, καθώς και στη μείωση των κινδύνων αγοράς και των πιστωτικών κινδύνων.

Η πρόταση θα δημιουργήσει έναν συνεκτικό μηχανισμό αναφοράς συμβάντων, ο οποίος θα συμβάλει στη μείωση των διοικητικών επιβαρύνσεων για τις χρηματοπιστωτικές οντότητες και θα ενισχύσει την αποτελεσματικότητα της εποπτείας.

- Συνοχή με τις ισχύουσες διατάξεις στον τομέα πολιτικής

Η παρούσα πρόταση εντάσσεται στο πλαίσιο των ευρύτερων υπό εξέλιξη εργασιών σε ευρωπαϊκό και διεθνές επίπεδο για την ενίσχυση της κυβερνοασφάλειας στον τομέα των χρηματοπιστωτικών υπηρεσιών και την αντιμετώπιση ευρύτερων λειτουργικών κινδύνων[6].

Ανταποκρίνεται επίσης στις κοινές τεχνικές συμβουλές που εξέδωσαν το 2019 οι ευρωπαϊκές εποπτικές αρχές (ΕΕΑ)[7], οι οποίες ζήτησαν την υιοθέτηση πιο συνεκτικής προσέγγισης για την αντιμετώπιση των κινδύνων ΤΠΕ στον χρηματοπιστωτικό τομέα και συνέστησαν στην Επιτροπή να ενισχύσει, με αναλογικό τρόπο, την ψηφιακή επιχειρησιακή ανθεκτικότητα του κλάδου των χρηματοπιστωτικών υπηρεσιών μέσω ειδικής τομεακής πρωτοβουλίας της ΕΕ. Η γνωμοδότηση των ΕΕΑ ήταν η απάντηση στο σχέδιο δράσης της Επιτροπής του 2018 για τη χρηματοοικονομική τεχνολογία[8] .

- Συνοχή με άλλες πολιτικές της Ένωσης

Όπως δήλωσε η πρόεδρος κ. von der Leyen στις πολιτικές κατευθύνσεις της[9], και όπως αναφέρεται στην ανακοίνωση με τίτλο «Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης»[10], είναι καίριας σημασίας για την Ευρώπη να αποκομίσει όλα τα οφέλη που προσφέρει η ψηφιακή εποχή και να ενισχύσει τη βιομηχανία και την ικανότητα καινοτομίας της, μέσα στα όρια που επιβάλλουν η ασφάλεια και η δεοντολογία. Η ευρωπαϊκή στρατηγική για τα δεδομένα[11] καθορίζει τέσσερις πυλώνες —προστασία δεδομένων, θεμελιώδη δικαιώματα, ασφάλεια και κυβερνοασφάλεια— ως βασικές προϋποθέσεις για μια κοινωνία που βασίζεται στη χρήση δεδομένων. Όσον αφορά πιο πρόσφατες εργασίες, το Ευρωπαϊκό Κοινοβούλιο επεξεργάζεται επί του παρόντος έκθεση σχετικά με τον ψηφιακό χρηματοοικονομικό τομέα, με την οποία ζητείται, μεταξύ άλλων, κοινή προσέγγιση όσον αφορά την κυβερνοανθεκτικότητα του χρηματοπιστωτικού τομέα[12]. Η θέσπιση νομοθετικού πλαισίου για την ενίσχυση της ψηφιακής επιχειρησιακής ανθεκτικότητας των χρηματοπιστωτικών οντοτήτων της ΕΕ συνάδει με αυτούς τους στόχους πολιτικής. Η πρόταση θα στηρίξει επίσης πολιτικές οι οποίες αποσκοπούν στην ανάκαμψη από την κρίση

---

6 Επιτροπή της Βασιλείας για την τραπεζική εποπτεία, *Cyber-resilience: Range of practices*, Δεκέμβριος 2018, και *Principles for sound management of operational risk (PSMOR)*, Οκτώβριος 2014.

7 Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector, JC 2019 26 (2019).

8 Ευρωπαϊκή Επιτροπή, *Σχέδιο δράσης για τη χρηματοοικονομική τεχνολογία*, COM(2018) 0109 final.

9 Πρόεδρος Ursula von der Leyen, Πολιτικές κατευθύνσεις για την επόμενη Ευρωπαϊκή Επιτροπή, 2019-2024, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_el.pdf.

10 Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, *Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης*, COM(2020) 67 final.

11 Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, *Ευρωπαϊκή στρατηγική για τα δεδομένα*, COM(2020) 66 final.

12 Έκθεση που περιέχει συστάσεις προς την Επιτροπή σχετικά με τον ψηφιακό χρηματοοικονομικό τομέα: αναδυόμενοι κίνδυνοι σε κρυπτο-στοιχεία του ενεργητικού — ρυθμιστικές και εποπτικές προκλήσεις στον τομέα των χρηματοπιστωτικών υπηρεσιών, ιδρυμάτων και αγορών [2020/2034(INL)], https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en

του κορονοϊού, καθώς θα διασφαλίσει ότι η αυξημένη ανθεκτικότητα στον ψηφιακό χρηματοοικονομικό τομέα συμβαδίζει με την επιχειρησιακή ανθεκτικότητα.

Η πρωτοβουλία θα διατηρήσει τα οφέλη που συνδέονται με το οριζόντιο πλαίσιο για την κυβερνοασφάλεια [π.χ. οδηγία για την ασφάλεια συστημάτων δικτύου και πληροφοριών (στο εξής: οδηγία NIS)], καθώς ο χρηματοπιστωτικός τομέας θα παραμείνει εντός του πεδίου εφαρμογής της. Ο χρηματοπιστωτικός τομέας θα παραμείνει στενά συνδεδεμένος με τον φορέα συνεργασίας για την ασφάλεια δικτύων και πληροφοριών και οι αρχές χρηματοπιστωτικής εποπτείας θα είναι σε θέση να ανταλλάσσουν σχετικές πληροφορίες εντός του υφιστάμενου οικοσυστήματος NIS. Η πρωτοβουλία συνάδει με την οδηγία για τις ευρωπαϊκές υποδομές ζωτικής σημασίας (στο εξής: οδηγία ECI), η οποία αποτελεί επί του παρόντος αντικείμενο επανεξέτασης, ώστε να βελτιωθεί η προστασία και η ανθεκτικότητα των υποδομών ζωτικής σημασίας έναντι απειλών που δεν σχετίζονται με τον κυβερνοχώρο. Τέλος, η παρούσα πρόταση συνάδει πλήρως με τη στρατηγική για την Ένωση Ασφάλειας[13], με την οποία ζητήθηκε η ανάληψη πρωτοβουλίας σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα, δεδομένης της μεγάλης εξάρτησής του από τις υπηρεσίες ΤΠΕ και της υψηλής ευαισθησίας του σε κυβερνοεπιθέσεις.

2. ΝΟΜΙΚΗ ΒΑΣΗ, ΕΠΙΚΟΥΡΙΚΟΤΗΤΑ ΚΑΙ ΑΝΑΛΟΓΙΚΟΤΗΤΑ

- Νομική βάση

Η πρόταση κανονισμού βασίζεται στο άρθρο 114 της ΣΛΕΕ.

Εξαλείφει τους φραγμούς στην εσωτερική αγορά χρηματοπιστωτικών υπηρεσιών και διευκολύνει την εδραίωση και τη λειτουργία της μέσω της εναρμόνισης των κανόνων που εφαρμόζονται στον τομέα της διαχείρισης κινδύνων ΤΠΕ, της αναφοράς, των δοκιμών και του κινδύνου τρίτων παρόχων ΤΠΕ. Οι υφιστάμενες ανισότητες στον τομέα αυτόν, τόσο σε νομοθετικό όσο και σε εποπτικό επίπεδο, καθώς και σε εθνικό και ενωσιακό επίπεδο, λειτουργούν ως φραγμοί για την ενιαία αγορά χρηματοπιστωτικών υπηρεσιών, διότι οι χρηματοπιστωτικές οντότητες που ασκούν διασυνοριακές δραστηριότητες αντιμετωπίζουν διαφορετικές —όπου δεν αλληλεπικαλύπτονται— κανονιστικές απαιτήσεις ή εποπτικές προσδοκίες, οι οποίες μπορούν να παρεμποδίσουν την άσκηση των ελευθεριών τους όσον αφορά την εγκατάσταση και την παροχή υπηρεσιών. Οι διαφορετικοί κανόνες στρεβλώνουν επίσης τον ανταγωνισμό μεταξύ χρηματοπιστωτικών οντοτήτων του ιδίου τύπου σε διαφορετικά κράτη μέλη. Επιπλέον, σε τομείς στους οποίους η εναρμόνιση είναι απούσα, μερική ή περιορισμένη, η ανάπτυξη κανόνων ή προσεγγίσεων που αποκλίνουν μεταξύ των κρατών μελών, είτε βρίσκονται ήδη σε ισχύ είτε στη διαδικασία έγκρισης και εφαρμογής σε εθνικό επίπεδο, μπορεί να λειτουργήσει αποτρεπτικά για τις ελευθερίες της ενιαίας αγοράς χρηματοπιστωτικών υπηρεσιών. Αυτό ισχύει ιδίως στην περίπτωση των πλαισίων ψηφιακών επιχειρησιακών δοκιμών και της εποπτείας κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ.

Δεδομένου ότι η πρόταση έχει αντίκτυπο σε διάφορες οδηγίες του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που εκδόθηκαν βάσει του άρθρου 53 παράγραφος 1 της ΣΛΕΕ, εκδίδεται επίσης ταυτόχρονα πρόταση οδηγίας η οποία αντικατοπτρίζει τις απαραίτητες τροποποιήσεις των εν λόγω οδηγιών.

- Επικουρικότητα

[13] Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Ευρωπαϊκό Συμβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφάλειας, COM(2020) 605 final.

Λόγω του υψηλού βαθμού διασύνδεσης μεταξύ των χρηματοπιστωτικών υπηρεσιών, της σημαντικής διασυνοριακής δραστηριότητας των χρηματοπιστωτικών οντοτήτων και της εκτεταμένης εξάρτησης του χρηματοπιστωτικού τομέα συνολικά από τρίτους παρόχους υπηρεσιών ΤΠΕ, απαιτείται η διασφάλιση ισχυρής ψηφιακής επιχειρησιακής ανθεκτικότητας ως ζήτημα κοινού συμφέροντος για τη διατήρηση της ευρωστίας των χρηματοπιστωτικών αγορών της ΕΕ. Οι διαφορές που προκύπτουν από ανομοιόμορφα ή αποσπασματικά καθεστώτα, αλληλεπικαλύψεις ή πολλαπλές απαιτήσεις που ισχύουν για τις ίδιες χρηματοπιστωτικές οντότητες, οι οποίες είτε δραστηριοποιούνται σε διασυνοριακό επίπεδο ή κατέχουν περισσότερες άδειες[14] σε ολόκληρη την ενιαία αγορά, μπορούν να αντιμετωπιστούν αποτελεσματικά μόνο σε επίπεδο Ένωσης.

Η παρούσα πρόταση εναρμονίζει την ψηφιακή επιχειρησιακή συνιστώσα ενός τομέα με μεγάλο βαθμό ενοποίησης και διασύνδεσης, ο οποίος επωφελείται ήδη από ένα ενιαίο σύνολο κανόνων και εποπτείας στους περισσότερους άλλους βασικούς τομείς. Για θέματα όπως η αναφορά συμβάντων που σχετίζονται με ΤΠΕ, μόνο ενωσιακοί εναρμονισμένοι κανόνες θα μπορούσαν να μειώσουν το επίπεδο των διοικητικών επιβαρύνσεων και του οικονομικού κόστους που συνδέεται με την αναφορά του ίδιου συμβάντος ΤΠΕ σε διαφορετικές ενωσιακές και εθνικές αρχές. Η ανάληψη δράσης σε επίπεδο ΕΕ είναι αναγκαία προκειμένου να διευκολυνθεί επίσης η αμοιβαία αναγνώριση των αποτελεσμάτων των προηγμένων δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας για οντότητες που δραστηριοποιούνται σε διασυνοριακή βάση και οι οποίες, ελλείψει ενωσιακών κανόνων, υπόκεινται ή ενδέχεται να υπόκεινται σε διαφορετικά πλαίσια στα διάφορα κράτη μέλη. Μόνο με την ανάληψη δράσης σε ενωσιακό επίπεδο είναι δυνατή η αντιμετώπιση των διαφορών ως προς τις προσεγγίσεις δοκιμών που έχουν υιοθετήσει τα κράτη μέλη. Η ανάληψη δράσης σε επίπεδο ΕΕ είναι επίσης αναγκαία για την αντιμετώπιση της έλλειψης κατάλληλων εποπτικών εξουσιών για την παρακολούθηση των κινδύνων που απορρέουν από τρίτους παρόχους υπηρεσιών ΤΠΕ, συμπεριλαμβανομένων των κινδύνων συγκέντρωσης και μετάδοσης για τον χρηματοπιστωτικό τομέα της ΕΕ.

- Αναλογικότητα

Οι προτεινόμενοι κανόνες δεν βαίνουν πέραν των αναγκαίων ορίων για την επίτευξη των στόχων της πρότασης. Καλύπτουν μόνο τις πτυχές που τα κράτη μέλη δεν μπορούν να επιτύχουν μεμονωμένα, καθώς και περιπτώσεις στις οποίες η διοικητική επιβάρυνση και το κόστος είναι ανάλογα προς τους ειδικούς και γενικούς επιδιωκόμενους στόχους.

Η αναλογικότητα ως προς το πεδίο εφαρμογής και την ένταση διασφαλίζεται μέσω της χρήσης ποιοτικών και ποσοτικών κριτηρίων αξιολόγησης. Στόχος των κριτηρίων αυτών είναι να διασφαλίσουν ότι, παρά το γεγονός ότι οι νέοι κανόνες καλύπτουν όλες τις χρηματοπιστωτικές οντότητες, είναι συγχρόνως κατάλληλα προσαρμοσμένοι στους κινδύνους και στις ανάγκες των ιδιαίτερων χαρακτηριστικών τους όσον αφορά το μέγεθος και το επιχειρηματικό προφίλ τους. Η αναλογικότητα ενσωματώνεται επίσης στους κανόνες για τη διαχείριση κινδύνων ΤΠΕ, τις δοκιμές ψηφιακής ανθεκτικότητας, την αναφορά σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ, καθώς και για την εποπτεία κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ.

- Επιλογή της νομικής πράξης

[14] Η ίδια χρηματοπιστωτική οντότητα μπορεί να διαθέτει άδεια λειτουργίας τραπεζικού ιδρύματος, επιχείρησης επενδύσεων και ιδρύματος πληρωμών, καθεμία από τις οποίες έχει εκδοθεί από διαφορετική εποπτική αρχή σε ένα ή περισσότερα κράτη μέλη.

Τα μέτρα που απαιτούνται για τη διαχείριση κινδύνων ΤΠΕ, την αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ, τη δοκιμή και την εποπτεία κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ πρέπει να περιλαμβάνονται σε κανονισμό προκειμένου να διασφαλιστεί η αποτελεσματική και άμεση εφαρμογή των λεπτομερών απαιτήσεων με ομοιόμορφο τρόπο, με την επιφύλαξη της αναλογικότητας και των ειδικών κανόνων που προβλέπονται στον παρόντα κανονισμό. Η συνοχή ως προς την αντιμετώπιση των ψηφιακών επιχειρησιακών κινδύνων συμβάλλει στην ενίσχυση της εμπιστοσύνης στο χρηματοπιστωτικό σύστημα και διαφυλάσσει τη σταθερότητά του. Δεδομένου ότι η χρήση κανονισμού συμβάλλει στη μείωση της πολυπλοκότητας του κανονιστικού πλαισίου, ενισχύει την εποπτική σύγκλιση και αυξάνει την ασφάλεια δικαίου, ο παρών κανονισμός συμβάλλει επίσης στον περιορισμό του κόστους συμμόρφωσης των χρηματοπιστωτικών οντοτήτων, ιδίως εκείνων που δραστηριοποιούνται σε διασυνοριακή βάση, γεγονός που θα συνδράμει με τη σειρά του στην εξάλειψη των στρεβλώσεων του ανταγωνισμού.

Ο παρών κανονισμός εξαλείφει επίσης τις νομοθετικές διαφορές και τις ανομοιόμορφες εθνικές κανονιστικές ή εποπτικές προσεγγίσεις όσον αφορά τον κίνδυνο ΤΠΕ και αίρει, συνεπώς, τα εμπόδια στην ενιαία αγορά χρηματοπιστωτικών υπηρεσιών, ιδίως όσον αφορά την ομαλή άσκηση της ελευθερίας εγκατάστασης και την παροχή υπηρεσιών για τις χρηματοπιστωτικές οντότητες με διασυνοριακή παρουσία.

Τέλος, το ενιαίο εγχειρίδιο κανόνων αναπτύχθηκε κυρίως μέσω κανονισμών και η επικαιροποίησή του με τη συνιστώσα της ψηφιακής επιχειρησιακής ανθεκτικότητας θα πρέπει να ακολουθήσει την ίδια επιλογή νομικής πράξης.

3. ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΩΝ ΕΚ ΤΩΝ ΥΣΤΕΡΩΝ ΑΞΙΟΛΟΓΗΣΕΩΝ, ΤΩΝ ΔΙΑΒΟΥΛΕΥΣΕΩΝ ΜΕ ΤΑ ΕΝΔΙΑΦΕΡΟΜΕΝΑ ΜΕΡΗ ΚΑΙ ΤΩΝ ΕΚΤΙΜΗΣΕΩΝ ΕΠΙΠΤΩΣΕΩΝ

- Εκ των υστέρων αξιολογήσεις / έλεγχοι καταλληλότητας της ισχύουσας νομοθεσίας

Μέχρι στιγμής, δεν υπάρχει ενωσιακή νομοθεσία για τις χρηματοπιστωτικές υπηρεσίες που να έχει επικεντρωθεί στην επιχειρησιακή ανθεκτικότητα και να έχει αντιμετωπίσει συνολικά τους κινδύνους που προκύπτουν από την ψηφιοποίηση, ούτε καν οι κανόνες οι οποίοι αφορούν γενικότερα τη διάσταση του επιχειρησιακού κινδύνου που έχουν ως υποσυνιστώσα τον κίνδυνο ΤΠΕ. Η παρέμβαση της Ένωσης έχει συμβάλει μέχρι στιγμής στην αντιμετώπιση των αναγκών και των προβλημάτων που εμφανίστηκαν μετά τη χρηματοπιστωτική κρίση του 2008: τα πιστωτικά ιδρύματα δεν παρουσίαζαν επαρκές επίπεδο κεφαλαιοποίησης, οι χρηματοπιστωτικές αγορές δεν ήταν επαρκώς ενοποιημένες και ο βαθμός εναρμόνισης μέχρι εκείνη τη στιγμή περιοριζόταν στο ελάχιστο. Ο κίνδυνος ΤΠΕ δεν θεωρήθηκε τότε προτεραιότητα και, ως εκ τούτου, τα νομικά πλαίσια για τους διάφορους υποτομείς του χρηματοπιστωτικού τομέα εξελίχθηκαν με μη συντονισμένο τρόπο. Μολαταύτα, η δράση της Ένωσης έχει επιτύχει τους στόχους της για τη διασφάλιση της χρηματοπιστωτικής σταθερότητας και τη θέσπιση ενός ενιαίου συνόλου εναρμονισμένων κανόνων για την προληπτική εποπτεία και τη δεοντολογία της αγοράς που ισχύουν για τις χρηματοπιστωτικές οντότητες σε ολόκληρη την ΕΕ. Δεδομένου ότι οι παράγοντες που συνέβαλαν καθοριστικά στη νομοθετική παρέμβαση της Ένωσης κατά το παρελθόν δεν επέτρεψαν τη θέσπιση ειδικών ή ολοκληρωμένων κανόνων για την αντιμετώπιση της ευρείας χρήσης των ψηφιακών τεχνολογιών και των συνεπαγόμενων κινδύνων στον χρηματοοικονομικό τομέα, η διενέργεια άμεσης αξιολόγησης φαίνεται δύσκολη. Η διαδικασία έμμεσης αξιολόγησης και οι επακόλουθες νομοθετικές τροποποιήσεις αντικατοπτρίζονται σε κάθε πυλώνα του παρόντος κανονισμού.

- Διαβουλεύσεις με τα ενδιαφερόμενα μέρη

Η Επιτροπή διεξήγαγε διαβουλεύσεις με τα ενδιαφερόμενα μέρη καθ' όλη τη διάρκεια της διαδικασίας κατάρτισης της παρούσας πρότασης. Ειδικότερα:

i) η Επιτροπή διεξήγαγε ανοικτή δημόσια διαβούλευση (από τις 19 Δεκεμβρίου 2019 έως τις 19 Μαρτίου 2020)[15]·

ii) η Επιτροπή διεξήγαγε διαβούλευση με το κοινό μέσω αρχικής εκτίμησης επιπτώσεων (19 Δεκεμβρίου 2019 — 16 Ιανουαρίου 2020)[16]·

iii) οι υπηρεσίες της Επιτροπής ζήτησαν τη γνώμη εμπειρογνωμόνων από τα κράτη μέλη στο πλαίσιο της ομάδας εμπειρογνωμόνων για θέματα τραπεζών, πληρωμών και ασφαλίσεων (EGBPI) σε δύο περιστάσεις (18 Μαΐου 2020 και 16 Ιουλίου 2020)[17]·

iv) οι υπηρεσίες της Επιτροπής διοργάνωσαν ειδικό διαδικτυακό σεμινάριο σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα, στο πλαίσιο της σειράς εκδηλώσεων προβολής του ψηφιακού χρηματοοικονομικού τομέα του 2020 (19 Μαΐου 2020).

Σκοπός της δημόσιας διαβούλευσης ήταν η ενημέρωση της Επιτροπής σχετικά με την ανάπτυξη ενός πιθανού διατομεακού πλαισίου της ΕΕ για την ψηφιακή επιχειρησιακή ανθεκτικότητα στον τομέα των χρηματοπιστωτικών υπηρεσιών. Από τις απαντήσεις προέκυψε ευρεία στήριξη για τη θέσπιση ειδικού πλαισίου με δράσεις επικεντρωμένες στους τέσσερις τομείς που αποτέλεσαν αντικείμενο της διαβούλευσης, ενώ τονίστηκε παράλληλα η ανάγκη για τη διασφάλιση της αναλογικότητας και την προσεκτική εξέταση και επεξήγηση της αλληλεπίδρασης με τους οριζόντιους κανόνες της οδηγίας NIS. Η Επιτροπή έλαβε δύο απαντήσεις σχετικά με την αρχική εκτίμηση επιπτώσεων, στις οποίες οι απαντήσαντες εξέτασαν συγκεκριμένες πτυχές σχετικά με τον τομέα δραστηριότητάς τους.

Στο πλαίσιο της συνεδρίασης της EGBPI που διοργανώθηκε στις 18 Μαΐου 2020, τα κράτη μέλη τάχθηκαν σθεναρά υπέρ της ενίσχυσης της ψηφιακής επιχειρησιακής ανθεκτικότητας του χρηματοπιστωτικού τομέα μέσω των προβλεπόμενων δράσεων στο πλαίσιο των τεσσάρων στοιχείων που περιγράφονται από την Επιτροπή. Τα κράτη μέλη τόνισαν επίσης την ανάγκη σαφούς συνάρθρωσης των νέων κανόνων με τους κανόνες για τον λειτουργικό κίνδυνο (στο πλαίσιο της νομοθεσίας της ΕΕ για τις χρηματοπιστωτικές υπηρεσίες), καθώς και με τους οριζόντιους κανόνες για την κυβερνοασφάλεια (οδηγία NIS). Κατά τη δεύτερη συνεδρίαση, ορισμένα κράτη μέλη τόνισαν την ανάγκη να διασφαλιστεί η αναλογικότητα και να ληφθεί υπόψη η ειδική κατάσταση των μικρών επιχειρήσεων ή των θυγατρικών μεγαλύτερων ομίλων, καθώς και να δοθεί ισχυρή εντολή στις ΕΑΑ που συμμετέχουν στην εποπτεία.

Στην πρόταση αξιοποιούνται και ενσωματώνονται επίσης τα σχόλια και οι παρατηρήσεις που αντλήθηκαν από συναντήσεις με ενδιαφερόμενα μέρη, καθώς και με αρχές και θεσμικά όργανα της ΕΕ. Τα ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των τρίτων παρόχων

[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-

[17] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en

υπηρεσιών ΤΠΕ, εξέφρασαν συνολικά τη στήριξή τους. Η ανάλυση των σχολίων και των παρατηρήσεων που αντλήθηκαν καταδεικνύει την έκκληση διατήρησης της αναλογικότητας και υιοθέτησης μιας προσέγγισης βασιζόμενης σε αρχές και κινδύνους κατά τον σχεδιασμό των κανόνων. Από θεσμική άποψη, τα κύρια στοιχεία προήλθαν από το Ευρωπαϊκό Συμβούλιο Συστημικών Κινδύνων (ΕΕΣΚ), τις ΕΕΑ, τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) και την Ευρωπαϊκή Κεντρική Τράπεζα (ΕΚΤ), καθώς και από τις αρμόδιες αρχές των κρατών μελών.

- Συλλογή και χρήση εμπειρογνωσίας

Κατά την κατάρτιση της παρούσας πρότασης, η Επιτροπή βασίστηκε σε ποιοτικά και ποσοτικά στοιχεία που συλλέχθηκαν από αναγνωρισμένες πηγές, συμπεριλαμβανομένων δύο κοινών τεχνικών γνωμοδοτήσεων από τις ΕΕΑ. Τα στοιχεία αυτά συμπληρώθηκαν με εμπιστευτικές πληροφορίες και δημόσια διαθέσιμες εκθέσεις εποπτικών αρχών, διεθνών οργανισμών τυποποίησης και κορυφαίων ερευνητικών ιδρυμάτων, καθώς και με ποσοτικά και ποιοτικά στοιχεία αναγνωρισμένων ενδιαφερόμενων μερών από τον παγκόσμιο χρηματοπιστωτικό τομέα.

- Εκτίμηση επιπτώσεων

Η παρούσα πρόταση συνοδεύεται από εκτίμηση επιπτώσεων[18], η οποία υποβλήθηκε στην επιτροπή ρυθμιστικού ελέγχου (ΕΡΕ) στις 29 Απριλίου 2020 και εγκρίθηκε στις 29 Μαΐου 2020. Η ΕΡΕ συνέστησε βελτιώσεις σε ορισμένους τομείς με σκοπό: i) την παροχή περισσότερων πληροφοριών σχετικά με τον τρόπο διασφάλισης της αναλογικότητας· ii) την καλύτερη προβολή του βαθμού στον οποίο η προτιμώμενη επιλογή διαφοροποιείται από τις κοινές τεχνικές συμβουλές των ΕΕΑ, καθώς και των λόγων για τους οποίους θεωρείται η βέλτιστη επιλογή· και iii) την περαιτέρω ανάδειξη του τρόπου με τον οποίο η πρόταση αλληλεπιδρά με την υφιστάμενη νομοθεσία της ΕΕ, μεταξύ άλλων με τους κανόνες που αποτελούν επί του παρόντος αντικείμενο επανεξέτασης. Η εκτίμηση επιπτώσεων προσαρμόστηκε για την εξέταση των σημείων αυτών, λαμβανομένων επίσης υπόψη των αναλυτικότερων παρατηρήσεων της ΕΡΕ.

Η Επιτροπή εξέτασε διάφορες επιλογές πολιτικής για την ανάπτυξη ενός ψηφιακού επιχειρησιακού πλαισίου ανθεκτικότητας:

- «Μη ανάληψη δράσης»: οι κανόνες σχετικά με την επιχειρησιακή ανθεκτικότητα θα συνεχίσουν να καθορίζονται από το υφιστάμενο, αποκλίνον σύνολο διατάξεων της ΕΕ για τις χρηματοπιστωτικές υπηρεσίες, εν μέρει από την οδηγία NIS και από υφιστάμενα ή μελλοντικά εθνικά καθεστώτα·
- επιλογή 1: ενίσχυση των κεφαλαιακών αποθεμάτων ασφάλειας: θα θεσπιστούν πρόσθετα κεφαλαιακά αποθέματα ασφάλειας για την ενίσχυση της ικανότητας των χρηματοπιστωτικών οντοτήτων να απορροφούν ζημίες που ενδέχεται να προκύψουν λόγω έλλειψης ψηφιακής επιχειρησιακής ανθεκτικότητας·
- επιλογή 2: θέσπιση πράξης σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα των χρηματοπιστωτικών υπηρεσιών: εφαρμογή ολοκληρωμένου πλαισίου σε επίπεδο

[18] Έγγραφο εργασίας των υπηρεσιών της Επιτροπής — Έκθεση εκτίμησης επιπτώσεων που συνοδεύει το έγγραφο με τίτλο «Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 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», SWD(2020) 198 της 24ης Σεπτεμβρίου 2020.

ΕΕ με συνεκτικούς κανόνες για την αντιμετώπιση των αναγκών ψηφιακής επιχειρησιακής ανθεκτικότητας όλων των ρυθμιζόμενων χρηματοπιστωτικών οντοτήτων και την εδραίωση πλαισίου εποπτείας για κρίσιμους τρίτους παρόχους ΤΠΕ·

- επιλογή 3: πράξη σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα των χρηματοπιστωτικών υπηρεσιών, σε συνδυασμό με κεντρική εποπτεία των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ: επιπλέον της πράξης σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα (επιλογή 2), θα συσταθεί μια νέα αρχή για την εποπτεία της παροχής υπηρεσιών από τρίτους παρόχους υπηρεσιών ΤΠΕ.

Προκρίθηκε η δεύτερη επιλογή, διότι επιτυγχάνει τους περισσότερους από τους επιδιωκόμενους στόχους κατά τρόπο αποτελεσματικό, αποδοτικό και συνεκτικό με άλλες πολιτικές της Ένωσης. Η πλειονότητα των ενδιαφερόμενων μερών προτιμούν επίσης αυτή την επιλογή.

Η προκρινόμενη επιλογή συνεπάγεται εφάπαξ και επαναλαμβανόμενες δαπάνες[19]. Οι εφάπαξ δαπάνες συνίστανται κυρίως σε επενδύσεις σε συστήματα ΤΠ και, ως εκ τούτου, είναι δύσκολο να προσδιοριστούν ποσοτικώς λόγω της διαφορετικής κατάστασης του πολύπλοκου περιβάλλοντος ΤΠ των επιχειρήσεων και ιδίως των ήδη υφιστάμενων συστημάτων ΤΠ. Παρά ταύτα, το κόστος αυτό θα είναι πιθανότατα περιορισμένο για τις μεγάλες επιχειρήσεις, δεδομένων των σημαντικών επενδύσεων ΤΠΕ που έχουν ήδη πραγματοποιήσει. Το κόστος αναμένεται επίσης να είναι περιορισμένο για τις μικρότερες επιχειρήσεις, δεδομένου ότι θα ισχύουν αναλογικά μέτρα λόγω του χαμηλότερου κινδύνου τους.

Η προκρινόμενη επιλογή θα έχει θετικές επιπτώσεις στις ΜΜΕ που δραστηριοποιούνται στον κλάδο των χρηματοπιστωτικών υπηρεσιών όσον αφορά τις οικονομικές, κοινωνικές και περιβαλλοντικές επιπτώσεις. Η πρόταση θα αποσαφηνίσει τους κανόνες που ισχύουν για τις ΜΜΕ, γεγονός που θα μειώσει το κόστος συμμόρφωσης.

Οι κύριες κοινωνικές επιπτώσεις της προκρινόμενης επιλογής πολιτικής θα αφορούν τους καταναλωτές και τους επενδυτές. Τα υψηλότερα επίπεδα ψηφιακής επιχειρησιακής ανθεκτικότητας του χρηματοπιστωτικού συστήματος της ΕΕ θα μειώσουν τον αριθμό και το μέσο κόστος των συμβάντων. Η κοινωνία στο σύνολό της θα επωφεληθεί από την αυξημένη εμπιστοσύνη στον κλάδο των χρηματοπιστωτικών υπηρεσιών.

Τέλος, όσον αφορά τις περιβαλλοντικές επιπτώσεις, η προκρινόμενη επιλογή πολιτικής θα ενθαρρύνει την ενισχυμένη χρήση της τελευταίας γενιάς υποδομών και υπηρεσιών ΤΠΕ, οι οποίες αναμένεται να καταστούν πιο βιώσιμες από περιβαλλοντική άποψη.

- Καταλληλότητα και απλούστευση του κανονιστικού πλαισίου

Η κατάργηση των αλληεπικαλυπτόμενων απαιτήσεων αναφοράς συμβάντων που σχετίζονται με τις ΤΠΕ θα μειώσει τη διοικητική επιβάρυνση και το σχετικό κόστος. Επιπλέον, οι εναρμονισμένες δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας με αμοιβαία αναγνώριση σε ολόκληρη την ενιαία αγορά θα μειώσουν το κόστος, ιδίως για τις διασυνοριακές επιχειρήσεις οι οποίες, σε αντίθετη περίπτωση, μπορεί να υποβάλλονταν σε πολλαπλές δοκιμές στα διάφορα κράτη μέλη[20].

---

19 *Ό.π., σ. 89-94.*

20 *Ό.π.*

- Θεμελιώδη δικαιώματα

Η ΕΕ είναι προσηλωμένη στη διασφάλιση υψηλών προτύπων προστασίας των θεμελιωδών δικαιωμάτων. Όλες οι προαιρετικές ρυθμίσεις για την ανταλλαγή πληροφοριών μεταξύ χρηματοπιστωτικών οντοτήτων που προάγει ο παρών κανονισμός θα διεξάγονται σε περιβάλλοντα εμπιστοσύνης, τηρουμένων πλήρως των κανόνων της Ένωσης για την προστασία των δεδομένων, κυρίως του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[21], ιδίως όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απαραίτητη για τους σκοπούς του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας.

4. ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ

Όσον αφορά τις δημοσιονομικές επιπτώσεις, δεδομένου ότι ο ισχύων κανονισμός προβλέπει ενισχυμένο ρόλο για τις ΕΕΑ μέσω των εξουσιών που τους ανατίθενται για την κατάλληλη εποπτεία κρίσιμων τρίτων παρόχων ΤΠΕ, η πρόταση συνεπάγεται την ανάπτυξη αυξημένων πόρων, ιδίως για την εκπλήρωση των αποστολών εποπτείας (όπως επιτόπιες και διαδικτυακές επιθεωρήσεις και ελέγχους) και τη χρήση προσωπικού που διαθέτει ειδική εμπειρογνωσία στον τομέα της ασφάλειας των ΤΠΕ.

Η κλίμακα και η κατανομή των δαπανών αυτών θα εξαρτηθεί από την έκταση των νέων εποπτικών εξουσιών και από τα (ακριβή) καθήκοντα που πρέπει να εκτελούν οι ΕΕΑ. Όσον αφορά την παροχή νέων ανθρώπινων πόρων, για την Ευρωπαϊκή Αρχή Τραπεζών (ΕΒΑ), την Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών (ESMA) και την Ευρωπαϊκή Αρχή Ασφαλίσεων και Επαγγελματικών Συντάξεων (ΕΙΟΡΑ) θα απαιτηθούν συνολικά 18 υπάλληλοι πλήρους απασχόλησης (ΙΠΑ) —6 ΙΠΑ για κάθε αρχή— όταν τεθούν σε εφαρμογή οι διάφορες διατάξεις της πρότασης (εκτιμώμενο κόστος 15,71 εκατ. EUR για την περίοδο 2022-2027). Οι ΕΕΑ θα επιβαρυνθούν επίσης με πρόσθετες δαπάνες ΤΠ, δαπάνες αποστολής για επιτόπιες επιθεωρήσεις και δαπάνες μετάφρασης (που εκτιμώνται σε 12 εκατ. EUR για την περίοδο 2022-2027), καθώς και με άλλες διοικητικές δαπάνες (που εκτιμώνται σε 2,48 εκατ. EUR για την περίοδο 2022-2027). Επομένως, ο συνολικός εκτιμώμενος αντίκτυπος στο κόστος ανέρχεται σε περίπου σε 30,19 εκατ. EUR για την περίοδο 2022-2027.

Είναι επίσης σκόπιμο να επισημανθεί ότι, ενώ ο αριθμός των απασχολούμενων ατόμων (π.χ. νέα μέλη προσωπικού και άλλες δαπάνες που συνδέονται με τα νέα καθήκοντα) που απαιτούνται για την άμεση εποπτεία θα εξαρτηθεί σε βάθος χρόνου από την εξέλιξη του αριθμού και του μεγέθους των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ που τελούν υπό εποπτεία, οι αντίστοιχες δαπάνες θα χρηματοδοτούνται πλήρως από τέλη που θα εισπράττονται από τους εν λόγω συμμετέχοντες στην αγορά. Ως εκ τούτου, δεν προβλέπεται καμία επίπτωση στις πιστώσεις του προϋπολογισμού της ΕΕ (εκτός από τα πρόσθετα μέλη προσωπικού), δεδομένου ότι οι δαπάνες αυτές θα χρηματοδοτούνται εξ ολοκλήρου από τέλη.

Οι χρηματοδοτικές και δημοσιονομικές επιπτώσεις της παρούσας πρότασης επεξηγούνται καταλεπτώς στο νομοθετικό δημοσιονομικό δελτίο που επισυνάπτεται στην παρούσα πρόταση.

---

[21] 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).

5. ΛΟΙΠΑ ΣΤΟΙΧΕΙΑ

- Σχέδια εφαρμογής και ρυθμίσεις παρακολούθησης, αξιολόγησης και υποβολής εκθέσεων

Η πρόταση περιλαμβάνει ένα γενικό σχέδιο για την παρακολούθηση και την αξιολόγηση των επιπτώσεων στους ειδικούς στόχους, βάσει του οποίου η Επιτροπή υποχρεούται να προβεί σε επανεξέταση τουλάχιστον τρία έτη μετά την έναρξη ισχύος και να υποβάλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο έκθεση σχετικά με τα κύρια πορίσματά της.

Η επανεξέταση πρέπει να διενεργηθεί σύμφωνα με τις κατευθυντήριες γραμμές της Επιτροπής για τη βελτίωση της νομοθεσίας.

- Αναλυτική επεξήγηση των επιμέρους διατάξεων της πρότασης

Η πρόταση διαρθρώνεται γύρω από διάφορους κύριους τομείς πολιτικής που αποτελούν βασικούς αλληλένδετους πυλώνες, οι οποίοι περιλαμβάνονται κατόπιν συμφωνίας στις ευρωπαϊκές και διεθνείς κατευθυντήριες γραμμές και βέλτιστες πρακτικές, με σκοπό την ενίσχυση της κυβερνοανθεκτικότητας και της επιχειρησιακής ανθεκτικότητας του χρηματοπιστωτικού τομέα.

Πεδίο εφαρμογής του κανονισμού και αναλογική εφαρμογή των απαιτούμενων μέτρων αναλογικότητας (άρθρο 2)

Για τους σκοπούς της διασφάλισης της συνοχής όσον αφορά τις απαιτήσεις διαχείρισης κινδύνων ΤΠΕ που ισχύουν για τον χρηματοπιστωτικό τομέα, ο κανονισμός καλύπτει ευρύ φάσμα χρηματοπιστωτικών οντοτήτων που ρυθμίζονται σε επίπεδο Ένωσης, και συγκεκριμένα πιστωτικά ιδρύματα, ιδρύματα πληρωμών, ιδρύματα ηλεκτρονικού χρήματος, επιχειρήσεις επενδύσεων, παρόχους υπηρεσιών κρυπτοστοιχείων, κεντρικά αποθετήρια τίτλων, κεντρικούς αντισυμβαλλομένους, τόπους διαπραγμάτευσης, αρχεία καταγραφής συναλλαγών, διαχειριστές εναλλακτικών επενδυτικών ταμείων και εταιρειών διαχείρισης, παρόχους υπηρεσιών αναφοράς δεδομένων, ασφαλιστικές και αντασφαλιστικές επιχειρήσεις, ασφαλιστικούς διαμεσολαβητές και ασφαλιστικούς διαμεσολαβητές που ασκούν ως δευτερεύουσα δραστηριότητα την ασφαλιστική διαμεσολάβηση, ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών, οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας, νόμιμους ελεγκτές και ελεγκτικά γραφεία, διαχειριστές δεικτών αναφοράς κρίσιμης σημασίας και παρόχους υπηρεσιών πληθοχρηματοδότησης.

Η κάλυψη αυτή διευκολύνει την ομοιογενή και συνεκτική εφαρμογή όλων των συνιστωσών της διαχείρισης κινδύνων που σχετίζονται με τις ΤΠΕ, διαφυλάσσοντας παράλληλα τους ισότιμους όρους ανταγωνισμού μεταξύ των χρηματοπιστωτικών οντοτήτων όσον αφορά τις κανονιστικές υποχρεώσεις τους σχετικά με τον κίνδυνο ΤΠΕ. Από την άλλη πλευρά, στον κανονισμό αναγνωρίζεται ότι υπάρχουν σημαντικές διαφορές μεταξύ των χρηματοπιστωτικών οντοτήτων όσον αφορά το μέγεθος, το επιχειρηματικό προφίλ ή σε σχέση με την έκθεσή τους στον ψηφιακό κίνδυνο. Δεδομένου ότι οι μεγαλύτερες χρηματοπιστωτικές οντότητες διαθέτουν περισσότερους πόρους, μόνο οι χρηματοπιστωτικές οντότητες που δεν χαρακτηρίζονται ως πολύ μικρές επιχειρήσεις υποχρεούνται, για παράδειγμα, να προβλέπουν πολύπλοκες ρυθμίσεις διακυβέρνησης και ειδικές λειτουργίες διαχείρισης, να διενεργούν εις βάθος αξιολογήσεις μετά από σημαντικές αλλαγές στις υποδομές 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 των σχεδίων αντιμετώπισης και αποκατάστασης, ώστε να λαμβάνουν υπόψη σενάρια μετάβασης μεταξύ της κύριας υποδομής ΤΠΕ και των

εφεδρικών εγκαταστάσεών τους. Επιπλέον, μόνο οι χρηματοπιστωτικές οντότητες που χαρακτηρίζονται ως σημαντικές για τους σκοπούς των προηγμένων δοκιμών ψηφιακής ανθεκτικότητας θα υποχρεούνται να διεξάγουν δοκιμές διείσδυσης βάσει απειλών.

Παρά τον ευρύ χαρακτήρα της, η κάλυψη αυτή δεν είναι εξαντλητική. Συγκεκριμένα, ο παρών κανονισμός δεν περιλαμβάνει τους διαχειριστές συστημάτων, όπως ορίζονται στο άρθρο 2 στοιχείο ιστ) της οδηγίας 98/26/ΕΚ[22] σχετικά με το αμετάκλητο του διακανονισμού στα συστήματα πληρωμών και στα συστήματα διακανονισμού αξιογράφων (ΟΑΔ), ούτε τους συμμετέχοντες στο σύστημα, εκτός εάν ο εν λόγω συμμετέχων είναι χρηματοπιστωτική οντότητα που ρυθμίζεται σε επίπεδο Ένωσης και, ως εκ τούτου, καλύπτεται αυτοδικαίως από τον παρόντα κανονισμό (δηλαδή πιστωτικό ίδρυμα, επιχείρηση επενδύσεων, κεντρικός αντισυμβαλλόμενος). Επιπλέον, στο πεδίο εφαρμογής δεν εμπίπτει ούτε το ενωσιακό μητρώο δικαιωμάτων εκπομπής, το οποίο λειτουργεί, σύμφωνα με την οδηγία 2003/87/ΕΚ[23], υπό την αιγίδα της Ευρωπαϊκής Επιτροπής.

Στις εν λόγω εξαιρέσεις από την ΟΑΔ λαμβάνεται υπόψη η ανάγκη περαιτέρω επανεξέτασης των νομικών και πολιτικών θεμάτων που αφορούν τους διαχειριστές συστημάτων και τους συμμετέχοντες που προβλέπονται στην ΟΑΔ, ενώ συνεκτιμώνται επίσης δεόντως οι επιπτώσεις των πλαισίων που ισχύουν επί του παρόντος για τα συστήματα πληρωμών[24] που τελούν υπό τη διαχείριση κεντρικών τραπεζών. Δεδομένου ότι τα θέματα αυτά ενδέχεται να περιλαμβάνουν πτυχές οι οποίες εξακολουθούν να διαφέρουν από τα θέματα που καλύπτει ο παρών κανονισμός, η Επιτροπή θα συνεχίσει να αξιολογεί την αναγκαιότητα και τις επιπτώσεις της πιθανής περαιτέρω επέκτασης του πεδίου εφαρμογής του παρόντος κανονισμού ώστε να συμπεριληφθούν οι οντότητες και οι υποδομές ΤΠΕ που δεν εμπίπτουν επί του παρόντος στο πεδίο αρμοδιοτήτων της.

Απαιτήσεις σχετικές με τη διακυβέρνηση (άρθρο 4)

Ο παρών κανονισμός αποσκοπεί στην καλύτερη εναρμόνιση των επιχειρηματικών στρατηγικών των χρηματοπιστωτικών οντοτήτων και της άσκησης της διαχείρισης κινδύνων ΤΠΕ. Για τον σκοπό αυτόν, το διοικητικό όργανο θα υποχρεούται να επιτελεί καίριο, ενεργό ρόλο στον προσανατολισμό του πλαισίου διαχείρισης κινδύνων ΤΠΕ και να επιδιώκει την τήρηση αυστηρής κυβερνοϋγιεινής. Η πλήρης ευθύνη του διοικητικού οργάνου όσον αφορά τη διαχείριση κινδύνων ΤΠΕ της χρηματοπιστωτικής οντότητας θα αποτελέσει γενική αρχή, η οποία θα μετουσιωθεί περαιτέρω σε ένα σύνολο ειδικών απαιτήσεων, όπως η ανάθεση σαφών ρόλων και αρμοδιοτήτων για όλες τις λειτουργίες που σχετίζονται με τις ΤΠΕ, η διαρκής συμμετοχή στον έλεγχο της παρακολούθησης της διαχείρισης κινδύνων ΤΠΕ, καθώς και σε ολόκληρο το φάσμα των διαδικασιών έγκρισης και ελέγχου, και στην κατάλληλη κατανομή των επενδύσεων ΤΠΕ και της σχετικής κατάρτισης.

Απαιτήσεις διαχείρισης κινδύνων ΤΠΕ (άρθρα 5 έως 14)

---

22 Οδηγία 98/26/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Μαΐου 1998, σχετικά με το αμετάκλητο του διακανονισμού στα συστήματα πληρωμών και στα συστήματα διακανονισμού αξιογράφων (ΕΕ L 166 της 11.6.1998, σ. 45)

23 Οδηγία 2003/87/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Οκτωβρίου 2003, σχετικά με τη θέσπιση συστήματος εμπορίας δικαιωμάτων εκπομπής αερίων θερμοκηπίου εντός της Κοινότητας και την τροποποίηση της οδηγίας 96/61/ΕΚ του Συμβουλίου (ΕΕ L 275 της 25.10.2003, σ. 32).

24 Ειδικότερα ο κανονισμός της Ευρωπαϊκής Κεντρικής Τράπεζας (ΕΕ) αριθ. 795/2014, της 3ης Ιουλίου 2014, σχετικά με τις απαιτήσεις επίβλεψης για τα συστημικώς σημαντικά συστήματα πληρωμών.

Η ψηφιακή επιχειρησιακή ανθεκτικότητα στηρίζεται σε ένα σύνολο βασικών αρχών και απαιτήσεων σχετικά με το πλαίσιο διαχείρισης κινδύνων ΤΠΕ, σύμφωνα με την κοινή τεχνική γνωμοδότηση των ΕΕΑ. Οι απαιτήσεις αυτές, εμπνευσμένες από σχετικά διεθνή, εθνικά και κλαδικά πρότυπα, κατευθυντήριες γραμμές και συστάσεις, περιστρέφονται γύρω από συγκεκριμένες λειτουργίες της διαχείρισης κινδύνων ΤΠΕ (προσδιορισμός, προστασία και πρόληψη, εντοπισμός, αντιμετώπιση και αποκατάσταση, μάθηση και εξέλιξη και επικοινωνία). Προκειμένου να συμβαδίζουν με το ταχέως εξελισσόμενο τοπίο των απειλών στον κυβερνοχώρο, οι χρηματοπιστωτικές οντότητες οφείλουν να δημιουργούν και να διατηρούν ανθεκτικά συστήματα και εργαλεία ΤΠΕ που ελαχιστοποιούν τις επιπτώσεις του κινδύνου ΤΠΕ, να προσδιορίζουν σε αδιάλειπτη βάση όλες τις πηγές κινδύνου ΤΠΕ, να θεσπίζουν μέτρα προστασίας και πρόληψης, να εντοπίζουν άμεσα αντικανονικές δραστηριότητες, να θέτουν σε εφαρμογή ειδικές και ολοκληρωμένες πολιτικές αδιάλειπτης λειτουργίας και σχέδια αποκατάστασης λειτουργίας μετά από καταστροφές ως αναπόσπαστο μέρος της πολιτικής αδιάλειπτης επιχειρησιακής λειτουργίας. Οι τελευταίες συνιστώσες απαιτούνται για την άμεση αποκατάσταση μετά από συμβάντα που σχετίζονται με τις ΤΠΕ, ιδίως κυβερνοεπιθέσεις, με τον περιορισμό των ζημιών και την ιεράρχηση κατά προτεραιότητα της επανέναρξης των δραστηριοτήτων. Ο ίδιος ο κανονισμός δεν επιβάλλει ειδική τυποποίηση, αλλά βασίζεται σε ευρωπαϊκά και διεθνώς αναγνωρισμένα τεχνικά πρότυπα ή βέλτιστες πρακτικές του κλάδου, υπό την προϋπόθεση ότι συμμορφώνονται πλήρως με τις εποπτικές οδηγίες για τη χρήση και την ενσωμάτωση διεθνών προτύπων αυτού του είδους. Ο παρών κανονισμός καλύπτει επίσης την ακεραιότητα, την ασφάλεια και την ανθεκτικότητα των υλικών υποδομών και εγκαταστάσεων που υποστηρίζουν τη χρήση της τεχνολογίας και των σχετικών διαδικασιών και προσώπων που σχετίζονται με τις ΤΠΕ, στο πλαίσιο του ψηφιακού αποτυπώματος των δραστηριοτήτων μιας χρηματοπιστωτικής οντότητας.

Αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ (άρθρα 15 έως 20)

Η εναρμόνιση και ο εξορθολογισμός της αναφοράς συμβάντων που σχετίζονται με τις ΤΠΕ επιτυγχάνεται, πρώτον, μέσω μιας γενικής απαίτησης περί θέσπισης και εφαρμογής διαδικασίας διαχείρισης από τις χρηματοπιστωτικές οντότητες για την παρακολούθηση και την καταγραφή συμβάντων που σχετίζονται με τις ΤΠΕ, ακολουθούμενη από την υποχρέωση ταξινόμησής τους βάσει κριτηρίων που περιγράφονται καταλεπτώς στον κανονισμό και αναπτύσσονται περαιτέρω από τις ΕΕΑ για τον καθορισμό κατώτατων ορίων σημαντικότητας. Δεύτερον, μόνο συμβάντα που σχετίζονται με τις ΤΠΕ τα οποία θεωρούνται μείζονος σημασίας πρέπει να αναφέρονται στις αρμόδιες αρχές. Η αναφορά συμβάντων θα πρέπει να υποβάλλεται σε επεξεργασία με τη χρήση κοινού υποδείγματος και σύμφωνα με εναρμονισμένη διαδικασία, όπως έχει αναπτυχθεί από τις ΕΕΑ. Οι χρηματοπιστωτικές οντότητες θα πρέπει να υποβάλλουν αρχικές, ενδιάμεσες και τελικές εκθέσεις και να ενημερώνουν τους χρήστες και τους πελάτες τους σε περίπτωση που το συμβάν έχει ή ενδέχεται να έχει επιπτώσεις στα οικονομικά τους συμφέροντα. Οι αρμόδιες αρχές θα πρέπει να παρέχουν συναφείς λεπτομέρειες των συμβάντων σε άλλα ιδρύματα ή αρχές: στις ΕΕΑ, στην ΕΚΤ και στα ενιαία κέντρα επαφής που ορίζονται βάσει της οδηγίας (ΕΕ) 2016/1148.

Προκειμένου να ξεκινήσει μεταξύ των χρηματοπιστωτικών οντοτήτων και των αρμόδιων αρχών ο διάλογος που θα συμβάλει στην ελαχιστοποίηση των επιπτώσεων και στον προσδιορισμό των κατάλληλων διορθωτικών μέτρων, η αναφορά σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ θα πρέπει να συμπληρώνεται από εποπτική ανατροφοδότηση και καθοδήγηση.

Τέλος, η δυνατότητα κεντρικής διαχείρισης, σε ενωσιακό επίπεδο, της αναφοράς συμβάντων που σχετίζονται με τις ΤΠΕ θα πρέπει να διερευνηθεί περαιτέρω στο πλαίσιο κοινής έκθεσης των ΕΕΑ, της ΕΚΤ και του ENISA, στην οποία θα αξιολογείται η σκοπιμότητα της

δημιουργίας ενιαίου κόμβου της ΕΕ για την αναφορά σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ από τις χρηματοπιστωτικές οντότητες.

Δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας (άρθρα 21 έως 24)

Οι ικανότητες και οι λειτουργίες που περιλαμβάνονται στο πλαίσιο διαχείρισης κινδύνων ΤΠΕ πρέπει να ελέγχονται περιοδικά για τους σκοπούς της ετοιμότητας και του εντοπισμού αδυναμιών, ελλείψεων ή κενών, καθώς και για τους σκοπούς της άμεσης εφαρμογής διορθωτικών μέτρων. Ο παρών κανονισμός παρέχει τη δυνατότητα αναλογικής εφαρμογής των απαιτήσεων δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας ανάλογα με το μέγεθος, το επιχειρηματικό προφίλ και το προφίλ κινδύνου των χρηματοπιστωτικών οντοτήτων: μολονότι όλες οι οντότητες θα πρέπει να διενεργούν δοκιμές εργαλείων και συστημάτων ΤΠΕ, μόνο οι οντότητες που χαρακτηρίζονται από τις αρμόδιες αρχές (βάσει των κριτηρίων που περιλαμβάνονται στον παρόντα κανονισμό και αναπτύσσονται περαιτέρω από τις ΕΕΑ) ως σημαντικές και ώριμες στον κυβερνοχώρο θα πρέπει να υποχρεούνται να διενεργούν προηγμένες δοκιμές διείσδυσης βάσει απειλών. Ο παρών κανονισμός καθορίζει επίσης απαιτήσεις για τους φορείς δοκιμών και την αναγνώριση των αποτελεσμάτων της δοκιμής διείσδυσης βάσει απειλών σε ολόκληρη την Ένωση για τις χρηματοπιστωτικές οντότητες που δραστηριοποιούνται σε διάφορα κράτη μέλη.

Κίνδυνος τρίτων παρόχων ΤΠΕ (άρθρα 25 έως 39)

Ο κανονισμός αποσκοπεί στη διασφάλιση ορθής παρακολούθησης του κινδύνου τρίτων παρόχων ΤΠΕ. Ο στόχος αυτός θα επιτευχθεί, πρώτον, μέσω της τήρησης των κανόνων που βασίζονται σε αρχές και ισχύουν για την παρακολούθηση, εκ μέρους των χρηματοπιστωτικών οντοτήτων, του κινδύνου που προκύπτει από τρίτους παρόχους ΤΠΕ. Δεύτερον, ο παρών κανονισμός εναρμονίζει βασικά στοιχεία της εξυπηρέτησης από τρίτους παρόχους ΤΠΕ, καθώς και της σχέσης με αυτούς. Τα στοιχεία αυτά καλύπτουν τις ελάχιστες πτυχές που θεωρούνται καίριας σημασίας για την εξασφάλιση της δυνατότητας πλήρους παρακολούθησης, εκ μέρους της χρηματοπιστωτικής οντότητας, του κινδύνου τρίτων παρόχων ΤΠΕ σε όλα τα στάδια της σχέσης τους, κατά τη σύναψη, την εκτέλεση και τη λύση της σχέσης, καθώς και κατά το μετασυμβατικό στάδιο.

Ειδικότερα, οι συμβάσεις που διέπουν τη σχέση αυτή θα πρέπει να υπόκεινται στην υποχρέωση να περιλαμβάνουν πλήρη περιγραφή των υπηρεσιών, ένδειξη των τοποθεσιών στις οποίες θα υποβάλλονται σε επεξεργασία δεδομένα, πλήρη περιγραφή των επιπέδων εξυπηρέτησης, συνοδευόμενη από ποσοτικούς και ποιοτικούς στόχους επιδόσεων, σχετικές διατάξεις για την προσβασιμότητα, τη διαθεσιμότητα, την ακεραιότητα, την ασφάλεια και την προστασία των δεδομένων προσωπικού χαρακτήρα, καθώς και εγγυήσεις για την πρόσβαση, την ανάκτηση και την επιστροφή σε περίπτωση αθέτησης υποχρεώσεων εκ μέρους των τρίτων παρόχων υπηρεσιών ΤΠΕ, προθεσμίες προειδοποίησης και υποχρεώσεις υποβολής εκθέσεων των τρίτων παρόχων υπηρεσιών ΤΠΕ, δικαιώματα πρόσβασης, επιθεώρησης και ελέγχου από τη χρηματοπιστωτική οντότητα ή από εντεταλμένο τρίτο μέρος, σαφή δικαιώματα καταγγελίας και ειδικές στρατηγικές εξόδου. Επιπλέον, λαμβανομένου υπόψη ότι ορισμένα από αυτά τα συμβατικά στοιχεία μπορούν να τυποποιηθούν, ο κανονισμός προάγει την προαιρετική χρήση τυποποιημένων συμβατικών ρητρών που πρέπει να αναπτυχθούν για τη χρήση της υπηρεσίας υπολογιστικού νέφους από την Επιτροπή.

Τέλος, με τον παρόντα κανονισμό επιδιώκεται να προαχθεί η σύγκλιση των εποπτικών προσεγγίσεων όσον αφορά τον κίνδυνο τρίτων παρόχων ΤΠΕ στον χρηματοπιστωτικό τομέα με την υπαγωγή των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ σε πλαίσιο εποπτείας της Ένωσης. Μέσω ενός νέου εναρμονισμένου νομοθετικού πλαισίου, στην ΕΕΑ που ορίζεται ως κύριος εποπτικός φορέας για καθέναν από τους εν λόγω κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ ανατίθενται οι εξουσίες να διασφαλίζει ότι οι πάροχοι τεχνολογικών

υπηρεσιών που διαδραματίζουν κρίσιμο ρόλο στη λειτουργία του χρηματοπιστωτικού τομέα τελούν υπό κατάλληλη παρακολούθηση σε πανευρωπαϊκή κλίμακα. Το πλαίσιο εποπτείας που προβλέπεται στον παρόντα κανονισμό βασίζεται στην υφιστάμενη θεσμική αρχιτεκτονική του τομέα των χρηματοπιστωτικών υπηρεσιών, στο πλαίσιο της οποίας η μεικτή Επιτροπή των ΕΕΑ διασφαλίζει τον διατομεακό συντονισμό σε σχέση με όλα τα ζητήματα που αφορούν τον κίνδυνο ΤΠΕ, σύμφωνα με τα καθήκοντά της για την κυβερνοασφάλεια, με την υποστήριξη της σχετικής υποεπιτροπής (φόρουμ εποπτείας) που εκτελεί τις προπαρασκευαστικές εργασίες για μεμονωμένες αποφάσεις και συλλογικές συστάσεις που απευθύνονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ.

Ανταλλαγή πληροφοριών (άρθρο 40)

Για τους σκοπούς της αύξησης της ευαισθητοποίησης σχετικά με τον κίνδυνο ΤΠΕ, της ελαχιστοποίησης της εξάπλωσής του, της στήριξης των αμυντικών ικανοτήτων των χρηματοπιστωτικών οντοτήτων και των τεχνικών εντοπισμού απειλών, ο παρών κανονισμός παρέχει στις χρηματοπιστωτικές οντότητες τη δυνατότητα να θεσπίσουν ρυθμίσεις για να ανταλλάσσουν μεταξύ τους στοιχεία και πληροφορίες για κυβερνοαπειλές.

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[25],

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής[26],

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 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

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

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

χρηματοδότησης, τη χρηματοδότηση μεταξύ ομοτίμων, την αξιολόγηση πιστοληπτικής ικανότητας, την ανάληψη ασφαλιστικών κινδύνων, τη διαχείριση απαιτήσεων και τις υπηρεσίες υποστήριξης (back-office). 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[27], 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[28] 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 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.

(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

---

27 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.

28 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.

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[29] 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 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 τη διεύρυνση των εντολών των αρχών χρηματοπιστωτικής εποπτείας που είναι επιφορτισμένες με καθήκοντα παρακολούθησης και προστασίας της χρηματοπιστωτικής σταθερότητας και της ακεραιότητας της αγοράς.

(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

[29] 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.

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.

(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.

(13) Κατά την αντιμετώπιση του κινδύνου ΤΠΕ, οι χρηματοπιστωτικές οντότητες θα πρέπει να ακολουθούν την ίδια προσέγγιση και τους ίδιους κανόνες βάσει αρχών. Η συνοχή συμβάλλει στην ενίσχυση της εμπιστοσύνης στο χρηματοπιστωτικό σύστημα και στη διατήρηση της σταθερότητάς του, ιδίως σε περιόδους υπερβολικής χρήσης συστημάτων, πλατφορμών και υποδομών 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.

(15) Παράλληλα με τη νομοθεσία για τις χρηματοπιστωτικές υπηρεσίες, η οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[30] 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,

[30] 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).

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, 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 συνεργάζονται περαιτέρω με τα ενιαία κέντρα επαφής που ορίζονται βάσει της οδηγίας (ΕΕ) 2016/1148. 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.

(18) Είναι επίσης σημαντικό να διασφαλιστεί η συνοχή 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, 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

[31] 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).

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. 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. Το επίπεδο ψηφιακής επιχειρησιακής ανθεκτικότητας του χρηματοπιστωτικού συστήματος θα πρέπει να αυξηθεί, επιτρέποντας παράλληλα την αναλογική εφαρμογή των απαιτήσεων για τις χρηματοπιστωτικές οντότητες που αποτελούν πολύ μικρές επιχειρήσεις, όπως ορίζονται στη σύσταση 2003/361/ΕΚ της Επιτροπής[32].

(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)[33] 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.

(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 τη συμπλήρωση του καθεστώτος

---

32 Σύσταση της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων (ΕΕ L 124 της 20.5.2003, σ. 36).

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

αναφοράς συμβάντων που σχετίζονται με τις ΤΠΕ με τις απαιτήσεις που ελλείπουν επί του παρόντος από τη νομοθεσία για τον χρηματοπιστωτικό υποτομέα, 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 μόνο στις οικείες αρμόδιες αρχές. 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 δοκιμών ψηφιακής επιχειρησιακής ανθεκτικότητας στο πλαίσιο διαφόρων και 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 δυσχεραίνει 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[34], 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 είναι κρίσιμοι πάροχοι χρηματοπιστωτικών οντοτήτων.

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

(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 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.

(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.

(32) Επομένως, 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[35], 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[36], ιδίως στο πλαίσιο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα που είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, όπως αναφέρεται στο άρθρο 6 παράγραφος 1 στοιχείο στ) του εν λόγω κανονισμού.

---

35 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).

36 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).

(33) Παρά την ευρεία κάλυψη που επιδιώκεται με τον παρόντα κανονισμό, η εφαρμογή των κανόνων για την ψηφιακή επιχειρησιακή ανθεκτικότητα θα πρέπει να λαμβάνει υπόψη τις σημαντικές διαφορές μεταξύ των χρηματοπιστωτικών οντοτήτων όσον αφορά το μέγεθος, το επιχειρηματικό προφίλ ή την έκθεση σε ψηφιακό κίνδυνο. 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 και το επιχειρηματικό προφίλ τους, 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 δαπανών και ζημιών που προκαλούνται από διαταραχές των ΤΠΕ, καθώς και τα αποτελέσματα επανεξέτασης μετά από συμβάντα που επέρχονται λόγω σημαντικών διαταραχών των 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[37], 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 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,

---

37 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.

περιορίζοντας τις ζημίες και δίνοντας προτεραιότητα στην επανέναρξη των δραστηριοτήτων και στην ανάληψη δράσεων αποκατάστασης. 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, 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 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.

(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 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 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.

(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 η καταγγελία των συμβάσεων θα πρέπει να βασίζεται τουλάχιστον σε ένα σύνολο 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, ιδίως όταν συνάπτονται με τρίτους παρόχους υπηρεσιών ΤΠΕ που είναι εγκατεστημένοι σε τρίτη χώρα. Στο παρόν στάδιο, και για τους σκοπούς της επίτευξης δίκαιης ισορροπίας μεταξύ της επιτακτικής ανάγκης 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. Η ΕΕΑ που έχει οριστεί να ασκεί την εποπτεία για κάθε κρίσιμο τρίτο πάροχο ΤΠΕ (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[38].

(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,

[38] 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.

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 ή διακοπής των επιχειρηματικών δραστηριοτήτων του τρίτου παρόχου υπηρεσιών ΤΠΕ 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 χωρίς πρόσθετο κόστος ή με κόστος που καθορίζεται εκ των προτέρων.

(53) 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, η αρμόδια αρχή της χρηματοπιστωτικής οντότητας θα πρέπει να έχει τη δυνατότητα να ασκεί, βάσει προειδοποιήσεων, τα εν λόγω δικαιώματα επιθεώρησης και ελέγχου του τρίτου παρόχου υπηρεσιών ΤΠΕ, με την επιφύλαξη της τήρησης του απορρήτου.

(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 των εγκαταστάσεων, ανάλογα με την πολυπλοκότητα της παρεχόμενης υπηρεσίας.

(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.

(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 έχουν θεσπιστεί σε επίπεδο Ευρωσυστήματος με σκοπό την υποστήριξη των καθηκόντων που αναφέρονται στο άρθρο 127 παράγραφος 2 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης θα πρέπει, συνεπώς, να εξαιρούνται.

(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.

(59) Το πλαίσιο αυτό 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, με την υποστήριξη μιας νέας υποεπιτροπής (το φόρουμ εποπτείας) που εκτελεί τις προπαρασκευαστικές εργασίες τόσο για μεμονωμένες αποφάσεις που απευθύνονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ όσο και για 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, μία από τις ΕΕΑ θα πρέπει να οριστεί ως κύριος εποπτικός φορέας για κάθε κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ.

(62) Οι κύριοι εποπτικοί φορείς θα πρέπει να διαθέτουν τις απαραίτητες εξουσίες για τη διεξαγωγή ερευνών, επιτόπιων και μη 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.

Η ανάθεση στις ΕΕΑ της κύριας εποπτείας 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) Επιπροσθέτως, οι κύριοι εποπτικοί φορείς θα πρέπει να είναι σε θέση να υποβάλλουν συστάσεις σχετικά με θέματα κινδύνων ΤΠΕ και κατάλληλα διορθωτικά μέτρα, μεταξύ άλλων να εναντιώνονται 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 τους κύριους εποπτικούς φορείς θα πρέπει να λαμβάνεται δεόντως υπόψη από τις εθνικές αρμόδιες αρχές στο πλαίσιο των καθηκόντων τους που αφορούν την προληπτική εποπτεία των χρηματοπιστωτικών οντοτήτων.

(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 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[39], και η διαβούλευση με τις ΕΕΑ θα πρέπει να διασφαλίζονται μέσω της αμοιβαίας ανταλλαγής πληροφοριών και της παροχής συνδρομής στο πλαίσιο των εποπτικών δραστηριοτήτων.

(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 διεξαγάγει, κατά τις προπαρασκευαστικές της εργασίες, τις κατάλληλες διαβουλεύσεις, μεταξύ άλλων σε επίπεδο εμπειρογνωμόνων, και οι διαβουλεύσεις αυτές να πραγματοποιηθούν σύμφωνα με τις

[39] 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).

αρχές που ορίζονται στη διοργανική συμφωνία της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου[40]. Ειδικότερα, προκειμένου να διασφαλιστεί η ισότιμη 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 των κατ' εξουσιοδότηση πράξεων.

(69) Δεδομένου ότι ο παρών κανονισμός, σε συνδυασμό με την οδηγία (ΕΕ) 20xx/xx του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[41], 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.

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.

(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 το μέγεθος και την πολυπλοκότητα 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

[40] ΕΕ L 123 της 12.5.2016, σ. 1.

[41] [*Να προστεθεί πλήρης παραπομπή*]

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 Ι

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,

– 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.

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 κρυπτοστοιχείων, εκδότες ψηφιακών κερμάτων με εγγύηση περιουσιακών στοιχείων και εκδότες σημαντικών ψηφιακών κερμάτων με εγγύηση περιουσιακών στοιχείων,

στ) κεντρικά αποθετήρια 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,

ιε) ιδρύματα επαγγελματικών συνταξιοδοτικών παροχών,

ιστ) οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας,

ιζ) νόμιμους ελεγκτές και ελεγκτικά γραφεία,

ιη) διαχειριστές δεικτών αναφοράς κρίσιμης σημασίας,

ιθ) παρόχους υπηρεσιών πληθοχρηματοδότησης,

κ) αρχεία καταγραφής τιτλοποιήσεων,

κα) τρίτους παρόχους υπηρεσιών ΤΠΕ.

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

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 με γνώμονα την τεχνολογία διασφαλίζοντας, άμεσα ή έμμεσα, μέσω της χρήσης υπηρεσιών από τρίτους παρόχους ΤΠΕ, το πλήρες φάσμα των ικανοτήτων ΤΠΕ που απαιτούνται ώστε να ανταποκρίνεται στην ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιεί η χρηματοπιστωτική οντότητα και τα οποία υποστηρίζουν τη συνεχή παροχή χρηματοπιστωτικών υπηρεσιών και την ποιότητά τους·

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 —συμπεριλαμβανομένης τυχόν δυσλειτουργίας, υπέρβασης χωρητικότητας, αστοχίας, διαταραχής, υποβάθμισης, κατάχρησης, απώλειας ή άλλου είδους κακόβουλου ή μη κακόβουλου γεγονότος— η οποία, εάν επέλθει, ενδέχεται να θέσει σε κίνδυνο την ασφάλεια των συστημάτων δικτύου και πληροφοριών, κάθε εργαλείου ή διαδικασίας που εξαρτάται από την τεχνολογία, της λειτουργίας και της διεξαγωγής διαδικασιών ή της παροχής υπηρεσιών, υπονομεύοντας με αυτόν τον τρόπο την ακεραιότητα ή τη διαθεσιμότητα δεδομένων, λογισμικού ή οποιασδήποτε άλλης συνιστώσας των υπηρεσιών και των υποδομών ΤΠΕ, ή η οποία προκαλεί παραβίαση του απορρήτου, βλάβη στην υλική υποδομή ΤΠΕ ή άλλες δυσμενείς επιπτώσεις·

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

6) «συμβάν που σχετίζεται με τις ΤΠΕ»: απρόβλεπτο περιστατικό που διαπιστώνεται στα συστήματα δικτύου και πληροφοριών, το οποίο προκύπτει από κακόβουλη ή μη κακόβουλη δραστηριότητα και θέτει σε κίνδυνο την ασφάλεια των συστημάτων δικτύου και πληροφοριών, των πληροφοριών που τα συστήματα αυτά επεξεργάζονται, αποθηκεύουν ή διαβιβάζουν, ή έχει δυσμενείς επιπτώσεις στη διαθεσιμότητα, τον απόρρητο χαρακτήρα, τη συνέχεια ή τη γνησιότητα των χρηματοπιστωτικών υπηρεσιών που παρέχει η χρηματοπιστωτική οντότητα·

7) «σημαντικό συμβάν που σχετίζεται με τις ΤΠΕ»: συμβάν που σχετίζεται με τις ΤΠΕ που μπορεί να έχει εξαιρετικά δυσμενείς επιπτώσεις στα συστήματα δικτύου και

πληροφοριών τα οποία υποστηρίζουν κρίσιμες λειτουργίες της χρηματοπιστωτικής οντότητας·

8) «κυβερνοαπειλή»: η κυβερνοαπειλή όπως ορίζεται στο άρθρο 2 σημείο 8 του κανονισμού (ΕΕ) αριθ. 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[42]·

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 απειλή·

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 ψηφιακές υπηρεσίες και υπηρεσίες δεδομένων, συμπεριλαμβανομένων των παρόχων υπηρεσιών υπολογιστικού νέφους, λογισμικού, υπηρεσιών ανάλυσης δεδομένων, κέντρων δεδομένων, 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

[42] 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).

σημείο 4 της οδηγίας (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[43]·

16) «υπηρεσίες ΤΠΕ»: ψηφιακές υπηρεσίες και υπηρεσίες δεδομένων που παρέχονται μέσω των συστημάτων ΤΠΕ σε έναν ή περισσότερους εσωτερικούς ή εξωτερικούς χρήστες, συμπεριλαμβανομένης της παροχής δεδομένων, της εισαγωγής δεδομένων, της αποθήκευσης δεδομένων, των υπηρεσιών επεξεργασίας και αναφοράς δεδομένων, παρακολούθησης δεδομένων, καθώς και υποστήριξης δραστηριοτήτων και λήψης αποφάσεων βάσει δεδομένων·

17) «κρίσιμη ή σημαντική λειτουργία»: λειτουργία 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, ή τις οικονομικές της επιδόσεις ή την ευρωστία ή τη συνέχεια των υπηρεσιών και των δραστηριοτήτων της·

18) «κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ»: τρίτος πάροχος υπηρεσιών ΤΠΕ που ορίζεται σύμφωνα με το άρθρο 29 και υπόκειται στο πλαίσιο εποπτείας που αναφέρεται στα άρθρα 30 έως 37·

19) «τρίτος πάροχος υπηρεσιών ΤΠΕ εγκατεστημένος σε τρίτη χώρα»: τρίτος πάροχος υπηρεσιών ΤΠΕ ο οποίος είναι νομικό πρόσωπο εγκατεστημένο σε τρίτη χώρα, δεν έχει ιδρύσει επιχείρηση/δεν έχει παρουσία στην Ένωση 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, δεν έχει ιδρύσει επιχείρηση/δεν έχει παρουσία στην Ένωση 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 την ικανότητα της χρηματοπιστωτικής οντότητας, και εντέλει του χρηματοπιστωτικού συστήματος της Ένωσης συνολικά, να παρέχει κρίσιμες 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 άρθρο 3 παράγραφος 1 σημείο 20 του κανονισμού (ΕΕ) 2016/1011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[44], στο άρθρο 3

[43] 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).

[44] 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

παράγραφος 1 στοιχείο κα) του κανονισμού (ΕΕ) 20xx/xx του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[45] [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[46]·

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

25) «ίδρυμα πληρωμών»: ίδρυμα πληρωμών όπως ορίζεται στο άρθρο 1 παράγραφος 1 στοιχείο δ) 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[47]·

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·

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·

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).

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

46 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).

47 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).

36) «ασφαλιστικός διαμεσολαβητής»: ασφαλιστικός διαμεσολαβητής όπως ορίζεται στο άρθρο 2 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 σημείο 4 της οδηγίας (ΕΕ) 2016/97·

38) «αντασφαλιστικός διαμεσολαβητής»: αντασφαλιστικός διαμεσολαβητής όπως ορίζεται στο άρθρο 2 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*]·

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*]·

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 ι) του [*ΕΕ: Να συμπληρωθεί παραπομπή στον κανονισμό MICA*]·

47) «διαχειριστής δεικτών αναφοράς κρίσιμης σημασίας»: διαχειριστής δεικτών αναφοράς κρίσιμης σημασίας όπως ορίζεται στο άρθρο x στοιχείο x) του κανονισμού xx/202x [*ΕΕ: Να συμπληρωθεί παραπομπή στον κανονισμό για τους δείκτες αναφοράς*]·

48) «πάροχος υπηρεσιών πληθοχρηματοδότησης»: πάροχος υπηρεσιών πληθοχρηματοδότησης όπως ορίζεται στο άρθρο x στοιχείο x) του κανονισμού (ΕΕ) xx/202x [*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 επιχείρηση»: χρηματοπιστωτική οντότητα όπως ορίζεται στο άρθρο 2 παράγραφος 3 του παραρτήματος της σύστασης 2003/361/ΕΚ.

ΚΕΦΑΛΑΙΟ ΙΙ

ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΤΠΕ

ΤΜΗΜΑ Ι

Άρθρο 4

Διακυβέρνηση και οργάνωση

1. Οι χρηματοπιστωτικές οντότητες εφαρμόζουν πλαίσια εσωτερικής διακυβέρνησης και ελέγχου τα οποία διασφαλίζουν την αποτελεσματική και συνετή διαχείριση όλων των κινδύνων ΤΠΕ.

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·

   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 μετά από καταστροφή, όπως 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 κατάρτιση όλων των μελών του αρμόδιου 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 δεόντως ενήμερο για 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 με τρίτους παρόχους υπηρεσιών ΤΠΕ όσον αφορά τη χρήση των 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 παρακολουθούν τακτικά ειδικά προγράμματα κατάρτισης προκειμένου να αποκτήσουν επαρκείς γνώσεις και δεξιότητες και να τις επικαιροποιούν σε διαρκή βάση, ώστε να κατανοούν και να αξιολογούν τους κινδύνους ΤΠΕ και τις επιπτώσεις τους στις δραστηριότητες της χρηματοπιστωτικής οντότητας.

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 που ανταποκρίνεται στις επιχειρηματικές ανάγκες, το μέγεθος και την πολυπλοκότητά τους.

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, 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, το οποίο επανεξετάζουν τακτικά.

5. Οι χρηματοπιστωτικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, διασφαλίζουν τον κατάλληλο διαχωρισμό 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.

7. 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 και συνυπολογιζομένης δεόντως της φύσης, της κλίμακας και της πολυπλοκότητας των υπηρεσιών και των δραστηριοτήτων των χρηματοπιστωτικών οντοτήτων.

9. Το πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στην παράγραφο 1 περιλαμβάνει στρατηγική ψηφιακής 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 αναφοράς 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) καθορίζοντας μια ολιστική στρατηγική πολλαπλών προμηθευτών ΤΠΕ σε επίπεδο οντότητας η οποία αναδεικνύει τις βασικές εξαρτήσεις από τρίτους παρόχους υπηρεσιών ΤΠΕ και επεξηγεί το σκεπτικό στο οποίο βασίζεται ο συνδυασμός προμηθειών από τρίτους παρόχους υπηρεσιών·

   η) εφαρμόζοντας δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας·

   θ) περιγράφοντας μια στρατηγική επικοινωνίας σε περίπτωση συμβάντων που σχετίζονται με τις ΤΠΕ.

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

Άρθρο 6

Συστήματα, πρωτόκολλα και εργαλεία ΤΠΕ

1. Οι χρηματοπιστωτικές οντότητες χρησιμοποιούν και διατηρούν επικαιροποιημένα συστήματα, πρωτόκολλα και εργαλεία ΤΠΕ, τα οποία πληρούν τις ακόλουθες προϋποθέσεις:

   α) τα συστήματα και τα εργαλεία είναι κατάλληλα για τη φύση, την πολυμορφία, την πολυπλοκότητα και 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 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 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 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 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 πόρων ΤΠΕ, καθώς και τις συνδέσεις και τις αλληλεξαρτήσεις μεταξύ των διαφόρων πόρων ΤΠΕ.

5. Οι χρηματοπιστωτικές οντότητες προσδιορίζουν και τεκμηριώνουν όλες τις διαδικασίες που εξαρτώνται από τρίτους παρόχους υπηρεσιών ΤΠΕ και προσδιορίζουν τις διασυνδέσεις με τρίτους παρόχους υπηρεσιών ΤΠΕ.

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, ιδίως πριν και μετά τη σύνδεση παλαιότερων και νέων 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 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 τις πλέον σύγχρονες τεχνολογίες και διαδικασίες ΤΠΕ οι οποίες:

   α) εγγυώνται 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 κινδύνους πλημμελούς διοίκησης ή κινδύνους που σχετίζονται με την επεξεργασία, συμπεριλαμβανομένης της ανεπαρκούς τήρησης αρχείων.

4. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 5 παράγραφος 1, 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 που χρησιμοποιούν οι ίδιες και οι πελάτες τους, των δεδομένων και των πληροφοριακών πόρων·

β) ακολουθώντας μια προσέγγιση βάσει κινδύνων, θεσπίζουν ορθή διαχείριση δικτύων και υποδομών χρησιμοποιώντας κατάλληλες τεχνικές, μεθόδους και πρωτόκολλα, συμπεριλαμβανομένης της εφαρμογής αυτοματοποιημένων μηχανισμών για την απομόνωση των πληροφοριακών πόρων που επηρεάζονται σε περίπτωση κυβερνοεπιθέσεων·

γ) εφαρμόζουν πολιτικές 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 και θεσπίζουν, για τον σκοπό αυτόν, ένα σύνολο πολιτικών, διαδικασιών και ελέγχων που αφορούν τα δικαιώματα πρόσβασης και την ορθή διαχείρισή τους·

δ) εφαρμόζουν πολιτικές και πρωτόκολλα για ισχυρούς μηχανισμούς επαλήθευσης της ταυτότητας, βάσει σχετικών προτύπων και ειδικών συστημάτων ελέγχου με στόχο την αποτροπή της πρόσβασης σε κρυπτογραφικές κλείδες με τις οποίες κρυπτογραφούνται δεδομένα, βάσει αποτελεσμάτων εγκεκριμένων διαδικασιών ταξινόμησης δεδομένων και αξιολόγησης κινδύνων·

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 στιγμιαία 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 για τον προσδιορισμό 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 επιτρέπουν τη διεξαγωγή πολυεπίπεδου ελέγχου, καθορίζουν όρια προειδοποίησης και κριτήρια για την ενεργοποίηση διαδικασιών εντοπισμού και αντιμετώπισης συμβάντων που σχετίζονται με τις ΤΠΕ, και θέτουν σε εφαρμογή αυτόματους μηχανισμούς 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, λαμβάνοντας δεόντως υπόψη το μέγεθος, την επιχειρηματική δραστηριότητα και τα προφίλ κινδύνου τους, ώστε να παρακολουθούν τη δραστηριότητα των χρηστών, την εμφάνιση αντικανονικών δραστηριοτήτων ΤΠΕ και συμβάντων που σχετίζονται με τις ΤΠΕ, ιδίως όσον αφορά κυβερνοεπιθέσεις.

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 ειδική και ολοκληρωμένη πολιτική αδιάλειπτης λειτουργίας των ΤΠΕ ως αναπόσπαστο μέρος της πολιτικής αδιάλειπτης επιχειρησιακής λειτουργίας της χρηματοπιστωτικής οντότητας.

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:

   α) την καταγραφή όλων των συμβάντων που σχετίζονται με τις ΤΠΕ·

   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 στα 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, η οποία, 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 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 κόστους και των ζημιών που προκλήθηκαν από τις διαταραχές των ΤΠΕ και τα συμβάντα που σχετίζονται με τις ΤΠΕ.

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. 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 με διαφορετικό λειτουργικό περιβάλλον από το κύριο σύστημα, το οποίο δεν είναι άμεσα συνδεδεμένο με το τελευταίο και προστατεύεται 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 διατηρούν πλεονάζουσες χωρητικότητες ΤΠΕ εξοπλισμένες με επαρκείς και κατάλληλους πόρους, δυνατότητες και λειτουργίες για την κάλυψη των επιχειρηματικών αναγκών.

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 άμεσα προσβάσιμος από το προσωπικό της χρηματοπιστωτικής οντότητας, ώστε να διασφαλίζεται η αδιάλειπτη λειτουργία κρίσιμων υπηρεσιών 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 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 διενεργούν πολλαπλούς ελέγχους, μεταξύ άλλων της συμφωνίας μεταξύ των στοιχείων, προκειμένου να διασφαλίσουν ότι η ακεραιότητα των δεδομένων διατηρείται στο ανώτατο επίπεδο. Οι έλεγχοι αυτοί 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, ανάλογα με το μέγεθος, την επιχειρηματική δραστηριότητα και το προφίλ κινδύνου τους, 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 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, οι χρηματοπιστωτικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, κοινοποιούν τις αλλαγές αυτές στις αρμόδιες αρχές.

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, 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 αυτά ισχύουν για όλους τους υπαλλήλους και τα ανώτερα διοικητικά στελέχη.

Οι χρηματοπιστωτικές οντότητες 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 συμβάντων που σχετίζονται με τις

ΤΠΕ ή σημαντικών ευπαθειών σε πελάτες και αντισυμβαλλομένους, καθώς και στο κοινό, ανάλογα με την περίπτωση.

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 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·

β) να καθορίσουν τον τρόπο με τον οποίο οι πολιτικές, οι διαδικασίες και τα εργαλεία ασφάλειας των ΤΠΕ που αναφέρονται στο άρθρο 8 παράγραφος 2 ενσωματώνουν ελέγχους ασφαλείας στα συστήματα ήδη από τη σύλληψή τους (ασφάλεια εκ σχεδιασμού), να παράσχουν τη δυνατότητα προσαρμογών στο εξελισσόμενο τοπίο των απειλών και να προβλέψουν τη χρήση τεχνολογίας άμυνας σε βάθος·

γ) να προσδιορίσουν περαιτέρω τις κατάλληλες τεχνικές, μεθόδους και τα πρωτόκολλα που αναφέρονται στο άρθρο 8 παράγραφος 4 στοιχείο β)·

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.

ΚΕΦΑΛΑΙΟ ΙΙΙ

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 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 εξαλείφονται 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 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 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, και κατά πόσο το εν λόγω συμβάν έχει επιπτώσεις στη φήμη·

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

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

δ) τις απώλειες δεδομένων που συνεπάγεται το συμβάν που σχετίζεται με τις ΤΠΕ, 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 κατόπιν διαβούλευσης 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 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 υποβάλλουν στην Επιτροπή τα εν λόγω κοινά σχέδια ρυθμιστικών τεχνικών προτύπων έως τη(ν) [*Υπηρεσία Εκδόσεων: 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 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.

2. Όταν ένα σημαντικό συμβάν που σχετίζεται με τις ΤΠΕ έχει ή μπορεί να έχει επιπτώσεις στα οικονομικά συμφέροντα των χρηστών και των πελατών της υπηρεσίας, οι χρηματοπιστωτικές οντότητες ενημερώνουν, χωρίς αδικαιολόγητη καθυστέρηση, τους χρήστες και τους πελάτες της υπηρεσίας όσον αφορά το σημαντικό συμβάν που σχετίζεται με τις ΤΠΕ και τους ενημερώνουν το συντομότερο δυνατόν σχετικά με όλα τα μέτρα που έχουν ληφθεί για τον περιορισμό των αρνητικών επιπτώσεων του εν λόγω συμβάντος.

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

α) αρχική κοινοποίηση, χωρίς καθυστέρηση, και το αργότερο μέχρι το τέλος της εργάσιμης ημέρας ή, σε περίπτωση σημαντικού συμβάντος που σχετίζεται με τις ΤΠΕ το οποίο σημειώθηκε τουλάχιστον 2 ώρες πριν από το τέλος της εργάσιμης ημέρας, το αργότερο 4 ώρες από την αρχή της επόμενης εργάσιμης ημέρας ή, όταν δεν διατίθενται δίαυλοι αναφοράς, αμέσως μόλις αυτοί καταστούν διαθέσιμοι·

β) ενδιάμεση έκθεση, το αργότερο μία εβδομάδα 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 αποστολή της αρχικής έκθεσης

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.

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

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.

6. Η ΕΒΑ, η ESMA ή η ΕΙΟΡΑ και η ΕΚΤ 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·

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 στην παράγραφο 1 στοιχείο α) και τα κοινά σχέδια εκτελεστικών τεχνικών προτύπων που αναφέρονται στην παράγραφο 1 στοιχείο β) έως τον xx του 202x [*Υπηρεσία Εκδόσεων: Να συμπληρωθεί ημερομηνία 1 έτος μετά την ημερομηνία έναρξης ισχύος*].

Ανατίθεται στην Επιτροπή η εξουσία να συμπληρώνει τον παρόντα κανονισμό εγκρίνοντας τα κοινά ρυθμιστικά τεχνικά πρότυπα που αναφέρονται στην παράγραφο 1 στοιχείο α), 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 στην παράγραφο 1 στοιχείο β), σύμφωνα με το άρθρο 15 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1095/2010 και (ΕΕ) αριθ. 1094/2010, αντίστοιχα.

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 του εν λόγω κόμβου της ΕΕ·

β) οφέλη, περιορισμοί και πιθανοί κίνδυνοι·

γ) στοιχεία λειτουργικής διαχείρισης·

δ) όροι συμμετοχής·

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

στ) προκαταρκτική αξιολόγηση του οικονομικού κόστους που συνεπάγεται η σύσταση της επιχειρησιακής πλατφόρμας για την υποστήριξη του 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.

2. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, υποβάλλουν ετησίως έκθεση σε ανωνυμοποιημένη και συγκεντρωτική βάση σχετικά με τις κοινοποιήσεις 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 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.

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 θεσπίζουν, διατηρούν και επανεξετάζουν, λαμβανομένου δεόντως υπόψη του μεγέθους τους, της επιχειρηματικής δραστηριότητας και του προφίλ κινδύνου τους, 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.

5. Οι χρηματοπιστωτικές οντότητες θεσπίζουν διαδικασίες και πολιτικές για την ιεράρχηση, την ταξινόμηση και την επίλυση 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 υποβάλλουν σε δοκιμές 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, που 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 στην παράγραφο 4 πραγματοποιούν τουλάχιστον ανά 3 έτη προηγμένες δοκιμές μέσω δοκιμών διείσδυσης βάσει απειλών.

2. Οι δοκιμές διείσδυσης βάσει απειλών καλύπτουν τουλάχιστον τις κρίσιμες λειτουργίες και υπηρεσίες μιας χρηματοπιστωτικής οντότητας και διενεργούνται σε συστήματα ζωντανής παραγωγής που υποστηρίζουν τις εν λόγω λειτουργίες. Το ακριβές εύρος των δοκιμών διείσδυσης βάσει απειλών προσδιορίζεται από τις χρηματοπιστωτικές οντότητες με βάση την αξιολόγηση κρίσιμων λειτουργιών και υπηρεσιών και επικυρώνεται από τις αρμόδιες αρχές.

   Για τους σκοπούς του πρώτου εδαφίου, οι χρηματοπιστωτικές οντότητες προσδιορίζουν όλες τις σχετικές υποκείμενες διαδικασίες, συστήματα και τεχνολογίες ΤΠΕ που υποστηρίζουν κρίσιμες λειτουργίες και υπηρεσίες, συμπεριλαμβανομένων των 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 υπηρεσιών ΤΠΕ, η χρηματοπιστωτική οντότητα λαμβάνει τα απαραίτητα μέτρα για την εξασφάλιση της συμμετοχής των εν λόγω παρόχων.

Οι χρηματοπιστωτικές οντότητες εφαρμόζουν αποτελεσματικούς ελέγχους διαχείρισης κινδύνων με σκοπό τη μείωση των κινδύνων όσον αφορά τις πιθανές επιπτώσεις στα δεδομένα, την πρόκλησης ζημίας στα περιουσιακά στοιχεία και τη διαταραχή κρίσιμων υπηρεσιών 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 ελεγκτές παρέχουν στην αρμόδια αρχή τεκμηρίωση με την οποία βεβαιώνεται ότι η δοκιμή διείσδυσης βάσει απειλών διενεργήθηκε σύμφωνα με τις απαιτήσεις. Οι αρμόδιες αρχές επικυρώνουν την τεκμηρίωση και χορηγούν βεβαίωση.

3. Οι χρηματοπιστωτικές οντότητες συνάπτουν συμβάσεις με ελεγκτές σύμφωνα με το άρθρο 24 για τους σκοπούς της ανάληψης δοκιμών διείσδυσης βάσει απειλών.

Οι αρμόδιες αρχές προσδιορίζουν τις χρηματοπιστωτικές οντότητες που καλούνται να διενεργήσουν δοκιμές διείσδυσης βάσει απειλών κατά τρόπο αναλογικό προς το μέγεθος, την κλίμακα, τη δραστηριότητα και το συνολικό προφίλ κινδύνου της χρηματοπιστωτικής οντότητας, 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.

4. Η ΕΒΑ, η ESMA και η ΕΙΟΡΑ, κατόπιν διαβούλευσης με την ΕΚΤ και λαμβάνοντας υπόψη τα σχετικά πλαίσια στην Ένωση που εφαρμόζονται σε δοκιμές διείσδυσης βάσει στοιχείων, καταρτίζουν σχέδια ρυθμιστικών τεχνικών προτύπων για τον περαιτέρω προσδιορισμό:

α) των κριτηρίων που χρησιμοποιούνται για την εφαρμογή της παραγράφου 6 του παρόντος άρθρου·

β) των απαιτήσεων σχετικά με:

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

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

γ) τα αποτελέσματα, τα στάδια ολοκλήρωσης και επανόρθωσης στο πλαίσιο της δοκιμής·

γ) το είδος της εποπτικής συνεργασίας που απαιτείται για την εφαρμογή δοκιμών διείσδυσης βάσει απειλών στο πλαίσιο των χρηματοπιστωτικών οντοτήτων που δραστηριοποιούνται σε περισσότερα από ένα κράτη μέλη, ώστε να παρέχεται η

δυνατότητα κατάλληλου επιπέδου εποπτικής συμμετοχής, καθώς και η δυνατότητα ευέλικτης εφαρμογής για την κάλυψη των ιδιαίτερων χαρακτηριστικών επιμέρους 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 2 μήνες πριν 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, για την πραγματοποίηση δοκιμών διείσδυσης βάσει απειλών, χρησιμοποιούν 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·

   δ) σε περίπτωση χρήσης εξωτερικών φορέων δοκιμών, 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) σε περίπτωση χρήσης εξωτερικών φορέων δοκιμών, καλύπτονται δεόντως και πλήρως από σχετική ασφάλιση επαγγελματικής ευθύνης, μεταξύ άλλων έναντι κινδύνων παραπτωμάτων και αμέλειας.

2. Οι χρηματοπιστωτικές οντότητες διασφαλίζουν ότι οι συμφωνίες 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 Ι

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) 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.

3. Στο πλαίσιο της διαχείρισης κινδύνων ΤΠΕ, οι χρηματοπιστωτικές οντότητες εγκρίνουν και επανεξετάζουν τακτικά στρατηγική για τον κίνδυνο τρίτων παρόχων ΤΠΕ, λαμβάνοντας υπόψη τη στρατηγική πολλαπλών προμηθευτών που αναφέρεται στο άρθρο 5 παράγραφος 9 στοιχείο ζ). 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 παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ.

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

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

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 τα πλέον πρόσφατα πρότυπα ασφάλειας των πληροφοριών.

7. Κατά την άσκηση των δικαιωμάτων πρόσβασης, επιθεώρησης και ελέγχου έναντι του τρίτου παρόχου υπηρεσιών ΤΠΕ, 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 υψηλό επίπεδο τεχνολογικής πολυπλοκότητας, 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 καταγγέλλονται όταν συντρέχουν τουλάχιστον οι παρακάτω συνθήκες:

α) παραβίαση των εφαρμοστέων νομοθετικών, κανονιστικών διατάξεων ή συμβατικών όρων από τον 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 στη συνολική διαχείριση κινδύνων ΤΠΕ 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 δεν μπορεί πλέον να εποπτεύει αποτελεσματικά τη χρηματοπιστωτική οντότητα συνεπεία της αντίστοιχης συμβατικής ρύθμισης.

9. Οι χρηματοπιστωτικές οντότητες εφαρμόζουν στρατηγικές εξόδου προκειμένου να λαμβάνουν υπόψη τους κινδύνους που ενδέχεται να προκύψουν στο επίπεδο του τρίτου παρόχου υπηρεσιών ΤΠΕ, ιδίως όσον αφορά την πιθανότητα αθέτησης υποχρεώσεων εκ μέρους του, 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.

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) [*Υπηρεσία Εκδόσεων: 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 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 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 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 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, ιδίως σε περίπτωση υπεργολάβου ΤΠΕ εγκατεστημένου σε τρίτη χώρα.

Όταν οι συμβατικές ρυθμίσεις για τη χρήση υπηρεσιών ΤΠΕ συνάπτονται με τρίτο πάροχο υπηρεσιών ΤΠΕ εγκατεστημένο σε τρίτη χώρα, οι χρηματοπιστωτικές οντότητες εξετάζουν ως συναφείς τουλάχιστον τους ακόλουθους παράγοντες:

α) την τήρηση της προστασίας δεδομένων·

β) την αποτελεσματική επιβολή της νομοθεσίας·

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

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

Οι χρηματοπιστωτικές οντότητες αξιολογούν αν και με ποιον τρόπο μπορούν οι δυνητικά μεγάλες και πολύπλοκες αλυσίδες υπεργολαβικής ανάθεσης να επηρεάσουν την ικανότητά τους να παρακολουθούν πλήρως τις λειτουργίες που αποτελούν αντικείμενο ανάθεσης, καθώς και την ικανότητα της αρμόδιας αρχής να εποπτεύει αποτελεσματικά τη 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 με έγγραφο το οποίο τίθεται στη διάθεση των συμβαλλομένων σε έντυπη μορφή ή σε μορφή με δυνατότητα μεταφόρτωσης και πρόσβασης.

2. 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 στις οποίες πρέπει να παρέχονται οι λειτουργίες και υπηρεσίες που αποτελούν αντικείμενο ανάθεσης ή υπεργολαβίας και στις οποίες θα πραγματοποιείται η επεξεργασία δεδομένων, συμπεριλαμβανομένου του χώρου αποθήκευσης, και την απαίτηση 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 και την προστασία των δεδομένων προσωπικού χαρακτήρα, καθώς και 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 ή

διακοπής των επιχειρηματικών δραστηριοτήτων του τρίτου παρόχου υπηρεσιών ΤΠΕ·

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) 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·

στ) την υποχρέωση του τρίτου παρόχου υπηρεσιών ΤΠΕ να παρέχει συνδρομή σε περίπτωση συμβάντος ΤΠΕ 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 διασφαλίζουν επαρκές επίπεδο ασφαλούς παροχής υπηρεσιών από τη χρηματοπιστωτική οντότητα σύμφωνα με το κανονιστικό της πλαίσιο·

η) 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 λήψης αντιγράφων της σχετικής τεκμηρίωσης, η αποτελεσματική άσκηση των οποίων δεν εμποδίζεται ούτε περιορίζεται από άλλες συμβατικές ρυθμίσεις ή την εφαρμογή πολιτικών·

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

iii) τη δέσμευση πλήρους συνεργασίας κατά τις επιτόπιες επιθεωρήσεις που διενεργεί η χρηματοπιστωτική οντότητα και λεπτομέρειες σχετικά με το εύρος, τους τρόπους και τη συχνότητα διενέργειας των εξ αποστάσεων ελέγχων·

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·

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

α) 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·

β) 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.

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.

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).

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 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 φόρουμ εποπτείας που συγκροτείται βάσει του άρθρου 29 παράγραφος 1:

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.

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.

3. Η Επιτροπή εξουσιοδοτείται να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 50, με σκοπό τη συμπλήρωση των κριτηρίων που αναφέρονται στην παράγραφο 2.

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. Οι ΕΕΑ, μέσω της μεικτής επιτροπής, καταρτίζουν, δημοσιεύουν και επικαιροποιούν ετησίως 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 φόρουμ εποπτείας, το οποίο συγκροτείται σύμφωνα με το άρθρο 29. Το φόρουμ 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.

9. Οι χρηματοπιστωτικές οντότητες δεν κάνουν χρήση τρίτου παρόχου υπηρεσιών ΤΠΕ που είναι εγκατεστημένος σε τρίτη χώρα, ο οποίος θα χαρακτηριζόταν ως κρίσιμος, σύμφωνα με την παράγραφο 1 στοιχείο α), εάν ήταν εγκατεστημένος στην Ένωση.

Άρθρο 29

Δομή του πλαισίου εποπτείας

1. Η μεικτή επιτροπή συγκροτεί, σύμφωνα με το άρθρο 57 των κανονισμών (ΕΕ) αριθ. 1093/2010, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010, το φόρουμ εποπτείας ως υποεπιτροπή για τους σκοπούς της υποστήριξης των εργασιών της μεικτής επιτροπής και του κύριου εποπτικού φορέα που αναφέρεται στο άρθρο 28 παράγραφος 1 στοιχείο β) όσον αφορά τον κίνδυνο τρίτων παρόχων ΤΠΕ σε όλους τους χρηματοπιστωτικούς τομείς. Το φόρουμ εποπτείας καταρτίζει τα σχέδια κοινών θέσεων και κοινών πράξεων της μεικτής επιτροπής στο πεδίο αυτό.

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

2. Το φόρουμ εποπτείας προβαίνει ετησίως σε συλλογική αξιολόγηση των αποτελεσμάτων και των πορισμάτων των εποπτικών δραστηριοτήτων που διεξάγονται για όλους τους κρίσιμους τρίτους παρόχους 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.

3. Το φόρουμ 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.

4. Το φόρουμ εποπτείας απαρτίζεται από τους προέδρους των ΕΕΑ και έναν υψηλόβαθμο εκπρόσωπο από κάθε κράτος μέλος, προερχόμενο από το εν ενεργεία προσωπικό της οικείας αρμόδιας αρχής. Στο φόρουμ εποπτείας συμμετέχουν ως παρατηρητές οι εκτελεστικοί διευθυντές κάθε ΕΕΑ και ένας εκπρόσωπος από την Ευρωπαϊκή Επιτροπή, την ΕΕΣΚ, την ΕΚΤ και τον ENISA.

5. 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 σχετικά με τη συνεργασία μεταξύ των ΕΕΑ 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 των ΕΕΑ, καθώς και τις λεπτομέρειες σχετικά με την ανταλλαγή των πληροφοριών που χρειάζονται οι αρμόδιες αρχές προκειμένου να διασφαλιστεί ότι δίνεται συνέχεια στις συστάσεις που απευθύνουν οι κύριοι εποπτικοί φορείς, σύμφωνα με το άρθρο 31 παράγραφος 1 στοιχείο δ), σε κρίσιμους τρίτους παρόχους ΤΠΕ.

6. 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.

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

Άρθρο 30

Καθήκοντα του κύριου εποπτικού φορέα

1. 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.

2. Η αξιολόγηση που αναφέρεται στην παράγραφο 1 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 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 1, ο κύριος εποπτικός φορέας εγκρίνει σαφές, λεπτομερές και τεκμηριωμένο εξατομικευμένο σχέδιο εποπτείας για κάθε κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ. Το σχέδιο αυτό κοινοποιείται κάθε έτος στον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ.

4. Μόλις συμφωνηθούν 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 τον κύριο εποπτικό φορέα.

Άρθρο 31

Εξουσίες του κύριου εποπτικού φορέα

1. Για τους σκοπούς της εκτέλεσης των καθηκόντων που προβλέπονται στο παρόν τμήμα, ο κύριος εποπτικός φορέας διαθέτει τις ακόλουθες εξουσίες:

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

β) να διενεργεί γενικές έρευνες και 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 τρίτοι πάροχοι υπηρεσιών ΤΠΕ όσον αφορά τις συστάσεις που αναφέρονται στο στοιχείο δ) της παρούσας παραγράφου·

δ) να διατυπώνει συστάσεις για τους τομείς που αναφέρονται στο άρθρο 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 ο κύριος εποπτικός φορέας 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 ο κύριος εποπτικός φορέας θεωρεί συναφείς για την αποτροπή της δημιουργίας μοναδικών σημείων αποτυχίας, ή την ενίσχυσή τους, ή για την ελαχιστοποίηση των πιθανών συστημικών επιπτώσεων στον 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 ο κύριος εποπτικός φορέας 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·

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

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

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

4. Ο κύριος εποπτικός φορέας μπορεί να επιβάλει περιοδική χρηματική ποινή με σκοπό να υποχρεώσει τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ να συμμορφωθεί με τα στοιχεία α), β) και γ) της παραγράφου 1.

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 με το 1 % του μέσου ημερήσιου κύκλου εργασιών 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.

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) θέτει 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 αιτήματος παροχής πληροφοριών σύμφωνα με την παράγραφο 1, ο κύριος εποπτικός φορέας:

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

β) αναφέρει τον σκοπό του αιτήματος·

γ) προσδιορίζει τις πληροφορίες που ζητούνται·

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

ε) επισημαίνει τις περιοδικές χρηματικές ποινές που προβλέπονται στο άρθρο 31 παράγραφος 4 στην περίπτωση ελλιπούς παροχής των απαιτούμενων πληροφοριών·

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 34 παράγραφος 1, μπορεί να διεξαγάγει τις απαραίτητες έρευνες σε τρίτους παρόχους υπηρεσιών ΤΠΕ:

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 λαμβάνει ή να αποκτά 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 ΤΠΕ, όπως κεντρικά γραφεία, επιχειρησιακά κέντρα, δευτερεύοντες χώροι, καθώς και να διενεργεί επιθεωρήσεις εκτός λειτουργίας.

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 χρησιμοποιούνται ή συμβάλλουν στην παροχή υπηρεσιών προς χρηματοπιστωτικές οντότητες.

5. Πριν από κάθε προγραμματισμένη επιτόπια επίσκεψη, 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 πάροχο 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 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, κατόπιν διαβούλευσης με το φόρουμ εποπτείας, εγκρίνει συστάσεις τις οποίες πρέπει να απευθύνει ο κύριος εποπτικός φορέας 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 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 των αρμόδιων αρχών όσον αφορά τα μέτρα που έλαβε ο τρίτος πάροχος υπηρεσιών ΤΠΕ βάσει των συστάσεων του κύριου εποπτικού φορέα σύμφωνα με το άρθρο 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 εκδίδουν οι κύριοι εποπτικοί φορείς σύμφωνα με το άρθρο 31 παράγραφος 1 στοιχείο δ), οι κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ ενημερώνουν τον κύριο εποπτικό φορέα αν σκοπεύουν να ακολουθήσουν τις εν λόγω συστάσεις. Οι κύριοι εποπτικοί φορείς διαβιβάζουν αμέσως τις πληροφορίες αυτές στις αρμόδιες αρχές.

2. Οι αρμόδιες αρχές παρακολουθούν αν οι χρηματοπιστωτικές οντότητες λαμβάνουν υπόψη τους κινδύνους που προσδιορίζονται στις συστάσεις που απευθύνει ο κύριος εποπτικός φορέας σε κρίσιμους τρίτους παρόχους ΤΠΕ σύμφωνα με το άρθρο 31 παράγραφος 1 στοιχείο δ).

3. Οι αρμόδιες αρχές δύνανται, σύμφωνα με το άρθρο 44, να ζητήσουν από τις χρηματοπιστωτικές οντότητες να αναστείλουν προσωρινά, εν μέρει ή πλήρως, τη χρήση ή την ανάπτυξη μιας υπηρεσίας που παρέχεται από τον κρίσιμο τρίτο πάροχο ΤΠΕ, έως ότου αντιμετωπιστούν οι κίνδυνοι που προσδιορίζονται στις συστάσεις που απευθύνονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ. Εάν κρίνεται σκόπιμο, μπορούν να ζητήσουν από τις χρηματοπιστωτικές οντότητες να προβούν σε μερική ή ολική καταγγελία των σχετικών ρυθμίσεων που έχουν συναφθεί με τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ.

4. Κατά τη λήψη των αποφάσεων που αναφέρονται στην παράγραφο 3, οι αρμόδιες αρχές λαμβάνουν υπόψη το είδος και το μέγεθος του κινδύνου που δεν αντιμετωπίστηκε από τον κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ, καθώς και τη σοβαρότητα της μη συμμόρφωσης, λαμβάνοντας υπόψη τα ακόλουθα κριτήρια:

   α) τη βαρύτητα και τη διάρκεια της μη συμμόρφωσης·

   β) αν η μη συμμόρφωση αποκάλυψε σοβαρές αδυναμίες στις διαδικασίες, τα συστήματα διαχείρισης, τη διαχείριση κινδύνων και 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.

5. Οι αρμόδιες αρχές ενημερώνουν τακτικά τους κύριους εποπτικούς φορείς σχετικά με τις προσεγγίσεις και τα μέτρα που λαμβάνονται κατά την εκτέλεση των εποπτικών καθηκόντων τους σε σχέση με τις χρηματοπιστωτικές οντότητες, καθώς και σε σχέση με τα συμβατικά μέτρα που έχουν λάβει, σε περίπτωση που ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ δεν έχει εγκρίνει εν μέρει ή πλήρως τις συστάσεις που του απηύθυναν οι κύριοι εποπτικοί φορείς.

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 διοικητικές δαπάνες και είναι ανάλογο προς τον κύκλο εργασιών του.

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 μπορούν να ανταλλάσσουν μεταξύ τους 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, ιδίως μέσω της ευαισθητοποίησης σχετικά με τις κυβερνοαπειλές, του περιορισμού ή της παρεμπόδισης της ικανότητας διάδοσης των κυβερνοαπειλών, της υποστήριξης του φάσματος αμυντικών ικανοτήτων των χρηματοπιστωτικών οντοτήτων, των τεχνικών ανίχνευσης

απειλών, των στρατηγικών μετριασμού ή των σταδίων αντιμετώπισης και αποκατάστασης·

β. πραγματοποιείται στο πλαίσιο αξιόπιστων κοινοτήτων χρηματοπιστωτικών οντοτήτων·

γ. υλοποιείται μέσω ρυθμίσεων ανταλλαγής πληροφοριών που προστατεύουν τον δυνητικά ευαίσθητο χαρακτήρα των ανταλλασσόμενων πληροφοριών, και οι οποίες διέπονται από κανόνες δεοντολογίας, τηρουμένων πλήρως του επιχειρηματικού απορρήτου, της προστασίας των δεδομένων προσωπικού χαρακτήρα[48] και των κατευθυντήριων γραμμών για την πολιτική ανταγωνισμού[49].

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.

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·

[48] 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).

[49] 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).

(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 κρυπτοστοιχείων, εκδότες 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, 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 xx/202x*·

(ιη) για παρόχους υπηρεσιών πληθοχρηματοδότησης, την αρμόδια αρχή που ορίζεται σύμφωνα με το *άρθρο x του κανονισμού xx/202x*·

(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 δύνανται να ζητήσουν να συμμετέχουν στις δραστηριότητες της ομάδας συνεργασίας.

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.

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 και την ΕΕΣΚ, 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 σχετικής απειλής 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 και η ΕΚΤ 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 η αρμόδια αρχή θεωρεί ότι αντιβαίνει στις διατάξεις του παρόντος κανονισμού και να προλαμβάνουν την επανάληψη της εν λόγω πρακτικής ή συμπεριφοράς·

γ) να εγκρίνουν κάθε είδους μέτρα, μεταξύ άλλων χρηματικής φύσης, ώστε να διασφαλίζεται ότι οι 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 EBA και την EIOPA 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 1 έτος 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, 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].
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 δύο 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 δύο μήνες με πρωτοβουλία 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.

ΤΜΗΜΑ II

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].»·

4) στην παράγραφο 6, το πρώτο εδάφιο αντικαθίσταται από το ακόλουθο κείμενο:

«Το ΚΑΤ προσδιορίζει, παρακολουθεί και διαχειρίζεται τους κινδύνους που ενδέχεται να συνεπάγονται για τις δραστηριότητές του οι βασικοί συμμετέχοντες στα συστήματα διακανονισμού αξιογράφων που διαχειρίζεται, καθώς και οι πάροχοι υπηρεσιών και υπηρεσιών κοινής ωφελείας, άλλα ΚΑΤ ή άλλες υποδομές της αγοράς. Παρέχει πληροφορίες στις αρμόδιες και τις σχετικές αρχές, κατόπιν αιτήματος, σχετικά με οποιονδήποτε τέτοιον κίνδυνο εντοπιστεί. Ενημερώνει επίσης χωρίς καθυστέρηση την αρμόδια αρχή και τις σχετικές αρχές σχετικά με οποιαδήποτε περιστατικά που αφορούν τη λειτουργία του, εκτός των συμβάντων που σχετίζονται με κινδύνους ΤΠΕ, και οφείλονται στους εν λόγω κινδύνους.»·

5) στην παράγραφο 7, το πρώτο εδάφιο αντικαθίσταται από το ακόλουθο κείμενο:

«Η ΕΑΚΑΑ, σε στενή συνεργασία με τα μέλη του ΕΣΚΤ, καταρτίζει σχέδια ρυθμιστικών τεχνικών προτύπων για να εξειδικεύσει τους λειτουργικούς κινδύνους που αναφέρονται στις παραγράφους 1 και 6, πλην των κινδύνων ΤΠΕ, τις μεθόδους ελέγχου, αντιμετώπισης ή ελαχιστοποίησης των εν λόγω κινδύνων, συμπεριλαμβανομένων των πολιτικών αδιάλειπτης λειτουργίας και των σχεδίων αποκατάστασης λειτουργίας μετά από καταστροφή, που αναφέρονται στις παραγράφους 3 και 4, καθώς και των μεθόδων αξιολόγησής τους.».

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) 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 — 12 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.

Βρυξέλλες,

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

ΝΟΜΟΘΕΤΙΚΟ ΔΗΜΟΣΙΟΝΟΜΙΚΟ ΔΕΛΤΙΟ

1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

1.1. Τίτλος της πρότασης/πρωτοβουλίας

1.2. Σχετικοί τομείς πολιτικής

1.3. Χαρακτήρας της πρότασης/πρωτοβουλίας

1.4. Στόχοι

1.5. Αιτιολόγηση της πρότασης/πρωτοβουλίας

1.6. Διάρκεια και δημοσιονομικές επιπτώσεις της πρότασης/πρωτοβουλίας

1.7. Προβλεπόμενοι τρόποι διαχείρισης

2. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ

2.1. Κανόνες παρακολούθησης και υποβολής εκθέσεων

2.2. Συστήματα διαχείρισης και ελέγχου

2.3. Μέτρα για την πρόληψη περιπτώσεων απάτης και παρατυπίας

3. ΕΚΤΙΜΩΜΕΝΕΣ ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

3.1. Τομείς του πολυετούς δημοσιονομικού πλαισίου και γραμμές δαπανών του προϋπολογισμού που επηρεάζονται

3.2. Εκτιμώμενες επιπτώσεις στις δαπάνες

3.2.1. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις δαπάνες

3.2.2. Εκτιμώμενες επιπτώσεις στις πιστώσεις

3.2.3. Εκτιμώμενες επιπτώσεις στους ανθρώπινους πόρους

3.2.4. Συμβατότητα με το ισχύον πολυετές δημοσιονομικό πλαίσιο

3.2.5. Συμμετοχή τρίτων στη χρηματοδότηση

3.3. Εκτιμώμενες επιπτώσεις στα έσοδα

Παράρτημα

Γενικές παραδοχές

Εποπτικές εξουσίες

ΝΟΜΟΘΕΤΙΚΟ ΔΗΜΟΣΙΟΝΟΜΙΚΟ ΔΕΛΤΙΟ «ΟΡΓΑΝΙΣΜΟΙ»

1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

1.1. Τίτλος της πρότασης/πρωτοβουλίας

Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα.

1.2. Σχετικοί τομείς πολιτικής

Τομέας πολιτικής: Χρηματοπιστωτική σταθερότητα, χρηματοπιστωτικές υπηρεσίες και ένωση κεφαλαιαγορών

Δραστηριότητα: Ψηφιακή επιχειρησιακή ανθεκτικότητα

1.3. Η πρόταση αφορά

☑ **νέα δράση**

☐ **νέα δράση μετά από πιλοτικό έργο / προπαρασκευαστική ενέργεια**[50]

☐ **την παράταση υφιστάμενης δράσης**

☐ **συγχώνευση μίας ή περισσότερων δράσεων προς άλλη/νέα δράση**

1.4. Στόχοι

1.4.1. Γενικοί στόχοι

Ο γενικός στόχος της πρωτοβουλίας είναι η ενίσχυση της ψηφιακής επιχειρησιακής ανθεκτικότητας των οντοτήτων του χρηματοπιστωτικού τομέα της ΕΕ με τον εξορθολογισμό και την αναβάθμιση των υφιστάμενων κανόνων και την εισαγωγή νέων απαιτήσεων όπου υπάρχουν κενά. Με τον τρόπο αυτόν θα ενισχυθεί επίσης το ενιαίο εγχειρίδιο κανόνων ως προς την ψηφιακή του διάσταση.

Ο γενικός στόχος μπορεί να έχει τη δομή τριών γενικών στόχων: 1) μείωση του κινδύνου χρηματοπιστωτικών κλυδωνισμών και αστάθειας, 2) μείωση της διοικητικής επιβάρυνσης και αύξηση της αποτελεσματικότητας της εποπτείας και 3) αύξηση της προστασίας των καταναλωτών και των επενδυτών.

1.4.2. Ειδικοί στόχοι

Η πρόταση έχει τους ακόλουθους ειδικούς στόχους:

αντιμετώπιση των κινδύνων των τεχνολογιών των πληροφοριών και των επικοινωνιών (στο εξής: ΤΠΕ) με πιο ολοκληρωμένο τρόπο και ενίσχυση του συνολικού επιπέδου ψηφιακής ανθεκτικότητας του χρηματοπιστωτικού τομέα·

εξορθολογισμός της αναφοράς συμβάντων που σχετίζονται με τις ΤΠΕ και αντιμετώπιση της αλληλεπικάλυψης των απαιτήσεων αναφοράς·

δυνατότητα πρόσβασης των αρχών χρηματοπιστωτικής εποπτείας σε πληροφορίες για συμβάντα που σχετίζονται με τις ΤΠΕ·

[50] Όπως αναφέρεται στο άρθρο 58 παράγραφος 2 στοιχείο α) ή β) του δημοσιονομικού κανονισμού.

διασφάλιση ότι οι χρηματοπιστωτικές οντότητες που καλύπτονται από την παρούσα πρόταση αξιολογούν την αποτελεσματικότητα των μέτρων πρόληψης και ανθεκτικότητάς τους και προσδιορίζουν τις ευπάθειες που σχετίζονται με τις ΤΠΕ·

μείωση του κατακερματισμού της αγοράς και δυνατότητα αποδοχής των αποτελεσμάτων των δοκιμών σε διασυνοριακό επίπεδο·

ενίσχυση των συμβατικών διασφαλίσεων που ισχύουν για χρηματοπιστωτικές οντότητες κατά τη χρήση υπηρεσιών ΤΠΕ, συμπεριλαμβανομένων των κανόνων εξωτερικής ανάθεσης (που διέπουν την παρακολούθηση τρίτων παρόχων ΤΠΕ·

δυνατότητα εποπτείας των δραστηριοτήτων κρίσιμων τρίτων παρόχων ΤΠΕ·

παροχή κινήτρων για την ανταλλαγή πληροφοριών για απειλές στον χρηματοπιστωτικό τομέα.

1.4.3. Αναμενόμενα αποτελέσματα και επιπτώσεις

Να προσδιοριστούν τα αποτελέσματα που θα πρέπει να έχει η πρόταση/πρωτοβουλία όσον αφορά τους στοχοθετημένους δικαιούχους / τις στοχοθετημένες ομάδες.

Η πράξη για την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα θα διασφαλίσει ένα ολοκληρωμένο πλαίσιο το οποίο θα καλύπτει όλες τις πτυχές της ψηφιακής επιχειρησιακής ανθεκτικότητας και θα είναι αποτελεσματικό ως προς τη βελτίωση της συνολικής επιχειρησιακής ανθεκτικότητας του χρηματοπιστωτικού τομέα. Θα διασφαλίζει τη σαφήνεια και τη συνοχή στο πλαίσιο του ενιαίου εγχειριδίου κανόνων.

Επιπλέον, θα καταστήσει την αλληλεπίδραση με την οδηγία NIS και την αναθεώρησή της περισσότερο σαφή και συνεκτική. Θα προσφέρει στις χρηματοπιστωτικές οντότητες σαφήνεια ως προς τους διαφορετικούς κανόνες σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα με τους οποίους πρέπει να συμμορφώνονται, ιδίως όσον αφορά τις χρηματοπιστωτικές οντότητες που κατέχουν περισσότερες από μία άδειες λειτουργίας και δραστηριοποιούνται σε διάφορες αγορές εντός της ΕΕ.

1.4.4. Δείκτες επιδόσεων

Να προσδιοριστούν οι δείκτες για την παρακολούθηση της προόδου και των επιτευγμάτων.

Πιθανοί δείκτες:

Αριθμός συμβάντων που σχετίζονται με τις ΤΠΕ στον χρηματοπιστωτικό τομέα της ΕΕ και οι επιπτώσεις τους

Αριθμός σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ και αναφέρονται σε αρχές προληπτικής εποπτείας

Αριθμός χρηματοπιστωτικών οντοτήτων οι οποίες καλούνται να διεξαγάγουν δοκιμές διείσδυσης βάσει απειλών

Αριθμός χρηματοπιστωτικών οντοτήτων που χρησιμοποιούν τυποποιημένες συμβατικές ρήτρες για τη σύναψη συμβατικών ρυθμίσεων με τρίτους παρόχους ΤΠΕ

Αριθμός κρίσιμων τρίτων παρόχων ΤΠΕ τους οποίους εποπτεύουν οι ΕΕΑ/αρχές προληπτικής εποπτείας

Αριθμός χρηματοπιστωτικών οντοτήτων που συμμετέχουν σε λύσεις ανταλλαγής πληροφοριών για απειλές

Αριθμός αρχών που είναι αποδέκτες αναφορών σχετικά με το ίδιο συμβάν που σχετίζεται με τις ΤΠΕ

Αριθμός διασυνοριακών δοκιμών διείσδυσης βάσει απειλών

1.5. Αιτιολόγηση της πρότασης/πρωτοβουλίας

1.5.1. Βραχυπρόθεσμη ή μακροπρόθεσμη κάλυψη αναγκών, συμπεριλαμβανομένου λεπτομερούς χρονοδιαγράμματος για τη σταδιακή υλοποίηση της πρωτοβουλίας

Ο χρηματοπιστωτικός τομέας βασίζεται σε μεγάλο βαθμό στις τεχνολογίες των πληροφοριών και των επικοινωνιών (ΤΠΕ). Παρά τη σημαντική πρόοδο που σημειώθηκε με τη θέσπιση εθνικών και ευρωπαϊκών στοχευμένων πολιτικών και νομοθετικών πρωτοβουλιών, οι κίνδυνοι ΤΠΕ εξακολουθούν να συνιστούν πρόκληση για την επιχειρησιακή ανθεκτικότητα, τις επιδόσεις και τη σταθερότητα του χρηματοπιστωτικού συστήματος της ΕΕ. Η μεταρρύθμιση που ακολούθησε τη χρηματοπιστωτική κρίση του 2008 ενίσχυσε πρωτίστως τη χρηματοπιστωτική ανθεκτικότητα του χρηματοπιστωτικού τομέα της ΕΕ και είχε ως στόχο τη

διασφάλιση της ανταγωνιστικότητας και της σταθερότητας της ΕΕ από την οπτική γωνία της οικονομίας, της προληπτικής εποπτείας και της δεοντολογίας της αγοράς. Η ασφάλεια των ΤΠΕ και η συνολική ψηφιακή επιχειρησιακή ανθεκτικότητα αποτελούν μέρος του επιχειρησιακού κινδύνου, αλλά δεν έχουν τοποθετηθεί επαρκώς στο επίκεντρο του κανονιστικού θεματολογίου μετά την κρίση, ενώ έχουν αναπτυχθεί μόνο σε ορισμένους τομείς των πολιτικών και των κανονισμών για τις χρηματοπιστωτικές αγορές της ΕΕ ή μόνο σε λίγα κράτη μέλη. Η κατάσταση αυτή συνεπάγεται τις ακόλουθες προκλήσεις, τις οποίες καλείται να αντιμετωπίσει η πρόταση:

Το νομικό πλαίσιο της ΕΕ που καλύπτει τον κίνδυνο ΤΠΕ και την επιχειρησιακή ανθεκτικότητα σε ολόκληρο τον χρηματοπιστωτικό τομέα είναι κατακερματισμένο και δεν χαρακτηρίζεται από πλήρη συνοχή.

Η έλλειψη συνεκτικών απαιτήσεων αναφοράς συμβάντων που σχετίζονται με τις ΤΠΕ έχει ως αποτέλεσμα οι εποπτικές αρχές να σχηματίζουν ελλιπή εικόνα της φύσης, της συχνότητας, της σημασίας και των επιπτώσεων των συμβάντων.

Ορισμένες χρηματοπιστωτικές οντότητες αντιμετωπίζουν πολύπλοκες, αλληλεπικαλυπτόμενες και πιθανώς αντιφατικές απαιτήσεις αναφοράς για το ίδιο συμβάν που σχετίζεται με τις ΤΠΕ.

Η ανεπαρκής ανταλλαγή πληροφοριών και η ελλιπής συνεργασία όσον αφορά πληροφορίες για κυβερνοαπειλές σε επίπεδο στρατηγικής, τακτικής και επιχειρησιακής λειτουργίας συνιστά αποτρεπτικό παράγοντα για την επαρκή αξιολόγηση, παρακολούθηση, άμυνα και αντιμετώπιση κυβερνοαπειλών από μεμονωμένες χρηματοπιστωτικές οντότητες.

Σε ορισμένους χρηματοπιστωτικούς υποτομείς ενδέχεται να υπάρχουν πολλαπλά και μη συντονισμένα πλαίσια δοκιμών διείσδυσης και ανθεκτικότητας, σε συνδυασμό με τη μη διασυνοριακή αναγνώριση των αποτελεσμάτων, ενώ άλλοι επιμέρους τομείς δεν διαθέτουν πλαίσια δοκιμών αυτού του είδους.

Η έλλειψη εποπτικών πληροφοριακών στοιχείων σχετικά με τις δραστηριότητες των χρηματοπιστωτικών οντοτήτων που παρέχονται από τρίτους παρόχους ΤΠΕ εκθέτει σε επιχειρησιακούς κινδύνους τόσο τις χρηματοπιστωτικές οντότητες μεμονωμένα όσο και το χρηματοπιστωτικό σύστημα στο σύνολό του.

Οι αρχές χρηματοπιστωτικής εποπτείας δεν διαθέτουν επαρκή εντολή ούτε εργαλεία για την παρακολούθηση και τη διαχείριση κινδύνων συγκέντρωσης και συστημικών κινδύνων που απορρέουν από την εξάρτηση των χρηματοπιστωτικών οντοτήτων από τρίτους παρόχους ΤΠΕ.

1.5.2. Προστιθέμενη αξία της ενωσιακής παρέμβασης (που μπορεί να προκύπτει από διάφορους παράγοντες, π.χ. οφέλη από τον συντονισμό, ασφάλεια δικαίου, μεγαλύτερη αποτελεσματικότητα ή συμπληρωματικότητα). Για τους σκοπούς του παρόντος σημείου, «προστιθέμενη αξία της ενωσιακής παρέμβασης» είναι η αξία που απορρέει από την ενωσιακή παρέμβαση και η οποία προστίθεται στην αξία που θα είχε δημιουργηθεί αν τα κράτη μέλη ενεργούσαν μεμονωμένα.

Λόγοι για ανάληψη δράσης σε ευρωπαϊκό επίπεδο (εκ των προτέρων):

Η ψηφιακή επιχειρησιακή ανθεκτικότητα αποτελεί ζήτημα κοινού συμφέροντος των χρηματοπιστωτικών αγορών της ΕΕ. Η δράση σε επίπεδο ΕΕ θα αποφέρει περισσότερα πλεονεκτήματα και μεγαλύτερη αξία συγκριτικά με την ανάληψη μεμονωμένης δράσης σε εθνικό επίπεδο. Χωρίς την προσθήκη των εν λόγω επιχειρησιακών διατάξεων σχετικά με τον κίνδυνο ΤΠΕ, το ενιαίο εγχειρίδιο κανόνων θα παρέχει τα εργαλεία για την αντιμετώπιση όλων των άλλων ειδών κινδύνου σε ευρωπαϊκό επίπεδο, αλλά θα παραλείπει τις πτυχές της

ψηφιακής επιχειρησιακής ανθεκτικότητας ή θα τις υποβάλει σε κατακερματισμένες και μη συντονισμένες πρωτοβουλίες σε εθνικό επίπεδο. Η πρόταση θα παράσχει νομική σαφήνεια σχετικά με το αν και με ποιον τρόπο εφαρμόζονται οι διατάξεις για την ψηφιακή επιχειρησιακή ανθεκτικότητα, ιδίως σε διασυνοριακές χρηματοπιστωτικές οντότητες, και θα εξαλείψει την ανάγκη των κρατών μελών να βελτιώσουν σε μεμονωμένη βάση τους κανόνες, τα πρότυπα και τις προσδοκίες σχετικά με την επιχειρησιακή ανθεκτικότητα και την κυβερνοασφάλεια, ανταποκρινόμενα στην τρέχουσα περιορισμένη κάλυψη των κανόνων της ΕΕ και του γενικού χαρακτήρα της οδηγίας NIS.

Αναμενόμενη προστιθέμενη αξία της Ένωσης (εκ των υστέρων):

Η παρέμβαση της Ένωσης θα αυξήσει σημαντικά την αποτελεσματικότητα της πολιτικής, ενώ θα περιορίσει ταυτόχρονα την πολυπλοκότητα και θα μειώσει την οικονομική και διοικητική επιβάρυνση για όλες τις χρηματοπιστωτικές οντότητες. Θα εναρμονίσει έναν τομέα της οικονομίας που είναι σε μεγάλο βαθμό διασυνδεδεμένος και ενοποιημένος και επωφελείται ήδη από ένα ενιαίο σύνολο κανόνων και εποπτείας. Όσον αφορά την αναφορά συμβάντων που σχετίζονται με τις ΤΠΕ, η πρόταση θα μειώσει την επιβάρυνση της υποβολής αναφορών —και τις έμμεσες δαπάνες— όταν το ίδιο συμβάν που σχετίζεται με τις ΤΠΕ αναφέρεται σε διαφορετικές αρχές της ΕΕ και/ή εθνικές αρχές. Θα διευκολύνει επίσης την αμοιβαία αναγνώριση/αποδοχή των αποτελεσμάτων των δοκιμών από οντότητες που δραστηριοποιούνται σε διασυνοριακό επίπεδο και υπόκεινται σε πολλαπλά πλαίσια δοκιμών σε διάφορα κράτη μέλη.

1.5.3. Διδάγματα από ανάλογες εμπειρίες του παρελθόντος

Νέα πρωτοβουλία

1.5.4. Συμβατότητα με το πολυετές δημοσιονομικό πλαίσιο και ενδεχόμενες συνέργειες με άλλα κατάλληλα μέσα

Ο στόχος της παρούσας πρότασης συνάδει με ορισμένες άλλες πολιτικές και υπό εξέλιξη πρωτοβουλίες της ΕΕ, και ειδικότερα την οδηγία για την ασφάλεια δικτύων και πληροφοριών (NIS) και την οδηγία για τις ευρωπαϊκές υποδομές ζωτικής σημασίας (ECI). Η πρόταση θα διατηρήσει τα οφέλη που συνδέονται με το οριζόντιο πλαίσιο για την κυβερνοασφάλεια, διατηρώντας τους τρεις επιμέρους χρηματοπιστωτικούς τομείς εντός του πεδίου εφαρμογής της οδηγίας NIS. Χάρη στη διατήρηση της συνάφειας με το οικοσύστημα της οδηγίας NIS, οι αρχές χρηματοπιστωτικής εποπτείας θα είναι σε θέση να ανταλλάσσουν σχετικές πληροφορίες με τις αρχές NIS και να συμμετέχουν στην ομάδα συνεργασίας NIS. Η πρόταση δεν επηρεάζει την οδηγία NIS, αλλά βασίζεται σε αυτήν και αντιμετωπίζει πιθανές αλληλοεπικαλύψεις με τη θέσπιση εξαίρεσης lex specialis. Η αλληλεπίδραση μεταξύ του κανονισμού για τις χρηματοπιστωτικές υπηρεσίες και της οδηγίας NIS θα συνεχίσει να διέπεται από ρήτρα lex specialis, με την οποία θα διασφαλίζεται η εξαίρεση των χρηματοπιστωτικών οντοτήτων από ουσιώδεις απαιτήσεις της οδηγίας NIS και να αποφεύγονται οι αλληλεπικαλύψεις μεταξύ των δύο πράξεων. Επιπλέον, η πρόταση συνάδει με την οδηγία για τις ευρωπαϊκές υποδομές ζωτικής σημασίας (ECI), η οποία βρίσκεται επί του παρόντος στο στάδιο της αναθεώρησης, με σκοπό τη βελτίωση της προστασίας και της ανθεκτικότητας των υποδομών ζωτικής σημασίας έναντι κυβερνοαπειλών.

Η παρούσα πρόταση δεν έχει επιπτώσεις στο πολυετές δημοσιονομικό πλαίσιο (ΠΔΠ). Πρώτον, το πλαίσιο εποπτείας κρίσιμων τρίτων παρόχων ΤΠΕ θα χρηματοδοτηθεί πλήρως από τα τέλη που θα επιβληθούν στους εν λόγω παρόχους· δεύτερον, τα πρόσθετα ρυθμιστικά καθήκοντα που συνδέονται με την ψηφιακή επιχειρησιακή ανθεκτικότητα και ανατίθενται στις ΕΕΑ, θα διασφαλίζονται με την εσωτερική ανακατανομή του υφιστάμενου προσωπικού.

Τούτο συνεπάγεται την πρόταση για την αύξηση του εξουσιοδοτημένου προσωπικού του οργανισμού κατά τη μελλοντική ετήσια διαδικασία του προϋπολογισμού. Ο οργανισμός θα συνεχίσει να καταβάλλει προσπάθειες με σκοπό τη μεγιστοποίηση των συνεργειών και τη βελτίωση της αποδοτικότητας (μεταξύ άλλων μέσω συστημάτων ΤΠΕ) και θα παρακολουθεί στενά τον πρόσθετο φόρτο εργασίας που σχετίζεται με την παρούσα πρόταση, ο οποίος θα αντικατοπτρίζεται στο επίπεδο του εξουσιοδοτημένου προσωπικού που ζητεί ο οργανισμός κατά την ετήσια διαδικασία του προϋπολογισμού.

1.5.5. Αξιολόγηση των διάφορων διαθέσιμων επιλογών χρηματοδότησης, συμπεριλαμβανομένων των δυνατοτήτων ανακατανομής

Εξετάστηκαν διάφορες επιλογές χρηματοδότησης:

Πρώτον, οι πρόσθετες δαπάνες θα μπορούσαν να χρηματοδοτηθούν από τον συνήθη μηχανισμό χρηματοδότησης των ΕΕΑ. Ωστόσο, η επιλογή αυτή συνεπάγεται σημαντική αύξηση της συνεισφοράς της ΕΕ στους χρηματοδοτικούς πόρους των ΕΕΑ.

Η επιλογή αυτή προκρίνεται για τις δαπάνες που αφορούν τα ρυθμιστικά καθήκοντα που συνδέονται με την παρούσα πρόταση. Πράγματι, οι ΕΕΑ θα κληθούν να ανακατανείμουν το υφιστάμενο προσωπικό ώστε να είναι δυνατή η κατάρτιση διαφόρων τεχνικών προτύπων. Ωστόσο, οι πρόσθετες δαπάνες που αφορούν την εποπτεία κρίσιμων τρίτων παρόχων ΤΠΕ δεν μπορούν να καλυφθούν από την ανακατανομή πόρων εντός των ΕΕΑ, οι οποίες θα έχουν επίσης άλλα καθήκοντα επιπλέον των προβλεπόμενων καθηκόντων στην παρούσα πρόταση, καθώς και βάσει άλλων νομοθετικών πράξεων της Ένωσης. Επιπλέον, τα εποπτικά καθήκοντα που αφορούν την ψηφιακή επιχειρησιακή ανθεκτικότητα προϋποθέτουν ειδικές τεχνικές

γνώσεις και εμπειρογνωσία. Δεδομένου ότι το υφιστάμενο επίπεδο των εν λόγω πόρων των ΕΕΑ είναι ανεπαρκές, απαιτούνται πρόσθετοι πόροι.

Τέλος, σύμφωνα με την πρόταση, θα επιβληθούν τέλη σε κρίσιμους τρίτους παρόχους ΤΠΕ που υπόκεινται σε εποπτεία. Τα τέλη αυτά αναμένεται να καλύπτουν όλους τους πρόσθετους πόρους που απαιτούνται ώστε οι ΕΕΑ να είναι σε θέση να εκτελούν τα καθήκοντα και τις εξουσίες τους.

1.6. Διάρκεια και δημοσιονομικές επιπτώσεις της πρότασης/πρωτοβουλίας

☐ **περιορισμένη διάρκεια**

☐ Πρόταση/πρωτοβουλία με ισχύ από [ΗΗ/ΜΜ]ΕΕΕΕ έως [ΗΗ/ΜΜ]ΕΕΕΕ

☐ Δημοσιονομικές επιπτώσεις από το ΕΕΕΕ έως το ΕΕΕΕ

☑ **απεριόριστη διάρκεια**

Περίοδος σταδιακής εφαρμογής από το 2021

και στη συνέχεια πλήρης εφαρμογή.

1.7. Προβλεπόμενοι τρόποι διαχείρισης[51]

Άμεση διαχείριση από την Επιτροπή

☐ από τους εκτελεστικούς οργανισμούς

☐ **Επιμερισμένη διαχείριση** με τα κράτη μέλη

☑ **Έμμεση διαχείριση** με ανάθεση καθηκόντων εκτέλεσης του προϋπολογισμού:

☐ σε διεθνείς οργανισμούς και στις οργανώσεις τους (να προσδιοριστούν)·

☐ στην ΕΤΕπ και στο Ευρωπαϊκό Ταμείο Επενδύσεων·

☑ στους οργανισμούς που αναφέρονται στα άρθρα 70 και 71·

☐ σε οργανισμούς δημοσίου δικαίου·

☐ σε οργανισμούς που διέπονται από ιδιωτικό δίκαιο και έχουν αποστολή δημόσιας υπηρεσίας, στον βαθμό που παρέχουν επαρκείς οικονομικές εγγυήσεις·

☐ σε οργανισμούς που διέπονται από το ιδιωτικό δίκαιο κράτους μέλους, στους οποίους έχει ανατεθεί η εκτέλεση σύμπραξης δημόσιου και ιδιωτικού τομέα και οι οποίοι παρέχουν επαρκείς οικονομικές εγγυήσεις·

☐ σε πρόσωπα επιφορτισμένα με την υλοποίηση συγκεκριμένων δράσεων στην ΚΕΠΠΑ βάσει του τίτλου V της ΣΕΕ και τα οποία προσδιορίζονται στην αντίστοιχη βασική πράξη.

Παρατηρήσεις

Άνευ αντικειμένου

[51] Οι λεπτομέρειες σχετικά με τους τρόπους διαχείρισης και οι παραπομπές στον δημοσιονομικό κανονισμό είναι διαθέσιμες στον ιστότοπο BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EL/man/budgmanag/Pages/budgmanag.aspx.

2. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ

2.1. Κανόνες παρακολούθησης και υποβολής εκθέσεων

Να προσδιοριστούν η συχνότητα και οι όροι.

Σύμφωνα με τις ήδη υφιστάμενες ρυθμίσεις, οι ΕΕΑ εκπονούν τακτικά εκθέσεις σχετικά με τη δραστηριότητά τους (συμπεριλαμβανομένων των εσωτερικών εκθέσεων προς τα ανώτερα διοικητικά στελέχη, των εκθέσεων προς τα συμβούλια και της σύνταξης ετήσιας έκθεσης), και υπόκεινται σε ελέγχους από το Ελεγκτικό Συνέδριο και την Υπηρεσία Εσωτερικού Ελέγχου της Επιτροπής όσον αφορά τη χρήση των πόρων και τις επιδόσεις τους. Η παρακολούθηση και η υποβολή εκθέσεων σχετικά με τις δράσεις που περιλαμβάνονται στην πρόταση θα συμμορφώνονται με τις ήδη υφιστάμενες απαιτήσεις, καθώς και με οποιεσδήποτε νέες απαιτήσεις προκύψουν από την παρούσα πρόταση.

2.2. Συστήματα διαχείρισης και ελέγχου

2.2.1. Αιτιολόγηση των τρόπων διαχείρισης, των μηχανισμών εκτέλεσης της χρηματοδότησης, των όρων πληρωμής και της προτεινόμενης στρατηγικής ελέγχου

Η διαχείριση θα πραγματοποιείται έμμεσα από τις ΕΕΑ. Ο μηχανισμός χρηματοδότησης θα εκτελείται με τέλη τα οποία θα επιβληθούν στους οικείους κρίσιμους τρίτους παρόχους ΤΠΕ.

2.2.2. Πληροφορίες σχετικά με τους κινδύνους που έχουν εντοπιστεί και τα συστήματα εσωτερικού ελέγχου που έχουν δημιουργηθεί για τον μετριασμό τους

Όσον αφορά τη νόμιμη, οικονομική, αποδοτική και αποτελεσματική χρήση των πιστώσεων για την εφαρμογή της παρούσας πρότασης, η πρόταση δεν αναμένεται να δημιουργήσει σημαντικούς νέους κινδύνους που να μην καλύπτονται από το υφιστάμενο πλαίσιο εσωτερικού ελέγχου. Ωστόσο, ενδέχεται να προκύψει μια νέα πρόκληση όσον αφορά τη διασφάλιση της έγκαιρης είσπραξης τελών από τους οικείους κρίσιμους παρόχους ΤΠΕ.

2.2.3. Εκτίμηση και αιτιολόγηση της οικονομικής αποδοτικότητας των ελέγχων (λόγος του κόστους του ελέγχου προς την αξία των σχετικών κονδυλίων που αποτελούν αντικείμενο διαχείρισης) και αξιολόγηση του εκτιμώμενου επιπέδου κινδύνου σφάλματος (κατά την πληρωμή και κατά το κλείσιμο)

Έχουν τεθεί ήδη σε εφαρμογή τα συστήματα διαχείρισης και ελέγχου που προβλέπονται στους κανονισμούς των ΕΕΑ. Οι ΕΕΑ συνεργάζονται στενά με την Υπηρεσία Εσωτερικού Λογιστικού Ελέγχου της Επιτροπής για να διασφαλίσουν την τήρηση των κατάλληλων προτύπων σε όλους τους τομείς του πλαισίου εσωτερικού ελέγχου. Οι ρυθμίσεις αυτές θα ισχύουν και όσον αφορά τον ρόλο των ΕΕΑ σύμφωνα με την παρούσα πρόταση. Επιπλέον, κάθε οικονομικό έτος, το Ευρωπαϊκό Κοινοβούλιο, κατόπιν σύστασης του Συμβουλίου, χορηγεί σε κάθε ΕΕΑ απαλλαγή για τη εκτέλεση του προϋπολογισμού της.

2.3. Μέτρα για την πρόληψη περιπτώσεων απάτης και παρατυπίας

Να προσδιοριστούν τα ισχύοντα ή τα προβλεπόμενα μέτρα πρόληψης και προστασίας, π.χ. στη στρατηγική για την καταπολέμηση της απάτης.

Για την καταπολέμηση της απάτης, της διαφθοράς και άλλων παράνομων δραστηριοτήτων, ισχύουν για τις ΕΕΑ, άνευ περιορισμών, οι διατάξεις του κανονισμού (ΕΕ, Ευρατόμ) αριθ. 883/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Σεπτεμβρίου 2013, σχετικά με τις έρευνες που πραγματοποιούνται από την Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF).

Οι ΕΕΑ διαθέτουν ειδική στρατηγική για την καταπολέμηση της απάτης και συνακόλουθο σχέδιο δράσης. Οι ενισχυμένες δράσεις των ΕΕΑ στον τομέα της καταπολέμησης της απάτης θα συμμορφώνονται με τους κανόνες και τις κατευθύνσεις που παρέχονται στον δημοσιονομικό κανονισμό (μέτρα για την καταπολέμηση της απάτης στο πλαίσιο της χρηστής δημοσιονομικής διαχείρισης), στις πολιτικές της OLAF για την πρόληψη της απάτης, στις διατάξεις που προβλέπονται στη στρατηγική της Επιτροπής για την καταπολέμηση της απάτης [COM(2011) 376], καθώς και στις διατάξεις που προβλέπονται στην κοινή προσέγγιση για τους αποκεντρωμένους οργανισμούς της ΕΕ (Ιούλιος 2012) και στον σχετικό χάρτη πορείας.

Επιπλέον, οι κανονισμοί για τη σύσταση των ΕΕΑ, καθώς και οι δημοσιονομικοί κανονισμοί των ΕΕΑ καθορίζουν τις διατάξεις για την εκτέλεση και τον έλεγχο των προϋπολογισμών των ΕΕΑ και τους εφαρμοστέους δημοσιονομικούς κανόνες, συμπεριλαμβανομένων εκείνων που αποσκοπούν στην πρόληψη της απάτης και των παρατυπιών.

3. ΕΚΤΙΜΩΜΕΝΕΣ ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

3.1. Τομείς του πολυετούς δημοσιονομικού πλαισίου και γραμμές δαπανών του προϋπολογισμού που επηρεάζονται

Υφιστάμενες γραμμές του προϋπολογισμού

Κατά σειρά τομέων του πολυετούς δημοσιονομικού πλαισίου και γραμμών του προϋπολογισμού

Τομέας του πολυετούς δημοσιονομικού πλαισίου	Γραμμή του προϋπολογισμού	Είδος δαπάνης	Συμμετοχή			
	Αριθμός	ΔΠ/ΜΔΠ[52]	χωρών ΕΖΕΣ[53]	υποψηφίων για ένταξη χωρών[54]	τρίτων χωρών	κατά την έννοια του άρθρου 21 παράγραφος 2 στοιχείο β) του δημοσιονομικού κανονισμού

Νέες γραμμές του προϋπολογισμού, των οποίων έχει ζητηθεί η δημιουργία

Κατά σειρά τομέων του πολυετούς δημοσιονομικού πλαισίου και γραμμών του προϋπολογισμού

[52] ΔΠ = Διαχωριζόμενες πιστώσεις / ΜΔΠ = Μη διαχωριζόμενες πιστώσεις.

[53] ΕΖΕΣ: Ευρωπαϊκή Ζώνη Ελεύθερων Συναλλαγών.

[54] Υποψήφιες χώρες και, κατά περίπτωση, δυνάμει υποψήφια μέλη των Δυτικών Βαλκανίων.

Τομέας του πολυετούς δημοσιονομικού πλαισίου	Γραμμή του προϋπολογισμού	Είδος δαπάνης	Συμμετοχή			
	Αριθμός	ΔΠ/ΜΔΠ	χωρών ΕΖΕΣ	υποψηφίων για ένταξη χωρών	τρίτων χωρών	κατά την έννοια του άρθρου 21 παράγραφος 2 στοιχείο β) του δημοσιονομικού κανονισμού

3.2. Εκτιμώμενες επιπτώσεις στις δαπάνες

3.3. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις δαπάνες

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

Τομέας του πολυετούς δημοσιονομικού πλαισίου	Αριθμός	Τομέας

ΓΔ: <..>			2020	2021	2022	2023	2024	2025	2026	2027	**ΣΥΝΟΛΟ**
	Αναλήψεις υποχρεώσεων	(1)									
	Πληρωμές	(2)									
ΣΥΝΟΛΟ πιστώσεων για τη ΓΔ <…….>	Αναλήψεις υποχρεώσεων										
	Πληρωμές										

Τομέας του πολυετούς δημοσιονομικού πλαισίου		

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

		2022	2023	2024	2025	2026	2027	**ΣΥΝΟΛΟ**
ΓΔ:								
• Ανθρώπινοι πόροι								
• Άλλες διοικητικές δαπάνες <>								
ΣΥΝΟΛΟ ΓΔ	Πιστώσεις							

ΣΥΝΟΛΟ πιστώσεων του ΤΟΜΕΑ <….> του πολυετούς δημοσιονομικού πλαισίου	(Σύνολο αναλήψεων υποχρεώσεων = Σύνολο πληρωμών)							

σε εκατ. EUR (με τρία δεκαδικά ψηφία) σε σταθερές τιμές

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**ΣΥΝΟΛΟ**
ΣΥΝΟΛΟ πιστώσεων του ΤΟΜΕΑ 1 του πολυετούς δημοσιονομικού πλαισίου	Αναλήψεις υποχρεώσεων							
	Πληρωμές							

3.3.1. Εκτιμώμενες επιπτώσεις στις πιστώσεις

☑ Η πρόταση/πρωτοβουλία δεν συνεπάγεται τη χρησιμοποίηση επιχειρησιακών πιστώσεων

☐ Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση επιχειρησιακών πιστώσεων, όπως εξηγείται κατωτέρω:

Πιστώσεις ανάληψης υποχρεώσεων σε εκατ. EUR (με τρία δεκαδικά ψηφία) σε σταθερές τιμές

Να προσδιοριστούν οι στόχοι και τα αποτελέσματα ⇩			2022		2023		2024		2025		2026		2027		**ΣΥΝΟΛΟ**	
	ΑΠΟΤΕΛΕΣΜΑΤΑ															
	Είδος[55]	Μέσο κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Συνολικός αριθ.	Συνολικό κόστος
ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ αριθ. 1[56] …																
-																
Μερικό σύνολο για τον ειδικό στόχο αριθ. 1																
ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ αριθ. 2 …																
-																
Μερικό σύνολο για τον ειδικό στόχο αριθ. 2																
ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ																

[55] Τα αποτελέσματα είναι τα προϊόντα και οι υπηρεσίες που θα παρασχεθούν (π.χ.: αριθμός ανταλλαγών φοιτητών που θα χρηματοδοτηθούν, αριθμός χλμ. οδών που θα κατασκευαστούν κ.λπ.).

[56] Όπως περιγράφεται στο σημείο 1.4.2. «Ειδικοί στόχοι …»

3.3.2. Εκτιμώμενες επιπτώσεις στους ανθρώπινους πόρους

3.3.2.1. Συνοπτική παρουσίαση

☐ Η πρόταση/πρωτοβουλία δεν συνεπάγεται τη χρησιμοποίηση πιστώσεων διοικητικού χαρακτήρα

☑ Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση πιστώσεων διοικητικού χαρακτήρα, όπως εξηγείται κατωτέρω:

σε εκατ. EUR (με τρία δεκαδικά ψηφία) σε σταθερές τιμές

EBA, EIOPA, ESMA	2022	2023	2024	2025	2026	2027	**ΣΥΝΟΛΟ**
Έκτακτοι υπάλληλοι (βαθμοί AD)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Έκτακτοι υπάλληλοι (βαθμοί AST)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Συμβασιούχοι υπάλληλοι							
Αποσπασμένοι εθνικοί εμπειρογνώμονες							
ΣΥΝΟΛΟ	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Απαιτήσεις προσωπικού (ΙΠΑ):

EBA, EIOPA, ESMA και EOX	2022	2023	2024	2025	2026	2027	**ΣΥΝΟΛΟ**
Έκτακτοι υπάλληλοι (βαθμοί AD) EBA=5, EIOPA= 5, ESMA= 5	15	15	15	15	15	15	15
Έκτακτοι υπάλληλοι (βαθμοί AST) EBA=1, EIOPA=1, EOX=1	3	3	3	3	3	3	3
Συμβασιούχοι υπάλληλοι							
Αποσπασμένοι εθνικοί εμπειρογνώμονες							

ΣΥΝΟΛΟ	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Εκτιμώμενες ανάγκες σε ανθρώπινους πόρους για τις (αρμόδιες) ΓΔ

☑ Η πρόταση/πρωτοβουλία δεν συνεπάγεται τη χρησιμοποίηση ανθρώπινων πόρων

☐ Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση ανθρώπινων πόρων, όπως εξηγείται κατωτέρω:

Εκτίμηση η οποία πρέπει να εκφράζεται σε ακέραιο αριθμό (ή το πολύ με ένα δεκαδικό ψηφίο)

		2022	2023	2024	2025	2026	2027
• **Θέσεις απασχόλησης του πίνακα προσωπικού (θέσεις μόνιμων και έκτακτων υπαλλήλων)**							
• **Εξωτερικό προσωπικό (σε μονάδα ισοδυνάμου πλήρους απασχόλησης: ΙΠΑ)**[57]							
XX 01 02 01 (AC, END, INT από το συνολικό κονδύλιο)							
XX 01 02 02 (AC, AL, END, INT και JPD στις αντιπροσωπείες της ΕΕ)							
XX 01 04 ***yy***[58]	– στην έδρα[59]						
	– στις αντιπροσωπείες της ΕΕ						
XX 01 05 02 (AC, END, INT – έμμεση έρευνα)							
10 01 05 02 (AC, END, INT – άμεση έρευνα)							
Άλλες γραμμές του προϋπολογισμού (να προσδιοριστούν)							
ΣΥΝΟΛΟ							

XX είναι ο σχετικός τομέας πολιτικής ή ο σχετικός τίτλος του προϋπολογισμού.

Οι ανάγκες σε ανθρώπινους πόρους θα καλυφθούν από το προσωπικό της ΓΔ που έχει ήδη διατεθεί για τη διαχείριση της δράσης και/ή έχει ανακατανεμηθεί στο εσωτερικό της ΓΔ, το οποίο θα συμπληρωθεί, αν χρειαστεί, με τυχόν πρόσθετους πόρους που μπορεί να διατεθούν στην αρμόδια για τη διαχείριση ΓΔ στο πλαίσιο της ετήσιας διαδικασίας κατανομής και λαμβανομένων υπόψη των υφιστάμενων δημοσιονομικών περιορισμών.

Περιγραφή των προς εκτέλεση καθηκόντων:

Μόνιμοι και έκτακτοι υπάλληλοι	

[57] AC = Συμβασιούχος υπάλληλος· AL = Τοπικός υπάλληλος· END = Αποσπασμένος εθνικός εμπειρογνώμονας· INT = Προσωρινό προσωπικό· JPD = Νέος επαγγελματίας σε αντιπροσωπεία της ΕΕ.

[58] Επιμέρους ανώτατο όριο εξωτερικού προσωπικού που καλύπτεται από επιχειρησιακές πιστώσεις (πρώην γραμμές «ΒΑ»).

[59] Κυρίως για τα διαρθρωτικά ταμεία, το Ευρωπαϊκό Γεωργικό Ταμείο Αγροτικής Ανάπτυξης (ΕΓΤΑΑ) και το Ευρωπαϊκό Ταμείο Αλιείας (ΕΤΑ).

Εξωτερικό προσωπικό	

Η περιγραφή του υπολογισμού του κόστους των μονάδων ΙΠΑ θα πρέπει να συμπεριληφθεί στο τμήμα 3 του παραρτήματος V.

3.3.3. Συμβατότητα με το ισχύον πολυετές δημοσιονομικό πλαίσιο

☑ Η πρόταση/πρωτοβουλία είναι συμβατή με το ισχύον πολυετές δημοσιονομικό πλαίσιο.

☐ Η πρόταση/πρωτοβουλία απαιτεί αναπρογραμματισμό του σχετικού τομέα του πολυετούς δημοσιονομικού πλαισίου.

☐ Η πρόταση/πρωτοβουλία απαιτεί τη χρησιμοποίηση του μέσου ευελιξίας ή την αναθεώρηση του πολυετούς δημοσιονομικού πλαισίου[60].

Να εξηγηθούν οι απαιτούμενες ενέργειες και να προσδιοριστούν οι σχετικοί τομείς και οι σχετικές γραμμές του προϋπολογισμού, καθώς και τα αντίστοιχα ποσά. […]

3.3.4. Συμμετοχή τρίτων στη χρηματοδότηση

☐ Η πρόταση/πρωτοβουλία δεν προβλέπει συγχρηματοδότηση από τρίτους.

☑ Η πρόταση/πρωτοβουλία προβλέπει τη συγχρηματοδότηση που εκτιμάται παρακάτω:

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

ΕΒΑ

	2022	2023	2024	2025	2026	2027	Σύνολο
Οι δαπάνες θα καλυφθούν κατά 100 % από τέλη που θα επιβληθούν στις εποπτευόμενες οντότητες[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
ΣΥΝΟΛΟ συγχρηματοδοτούμενων πιστώσεων	1,373	1,948	1,748	1,748	1,748	1,748	10,313

ΕΙΟΡΑ

	2022	2023	2024	2025	2026	2027	Σύνολο
Οι δαπάνες θα καλυφθούν κατά 100 % από τέλη που θα επιβληθούν στις εποπτευόμενες οντότητες[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
ΣΥΝΟΛΟ συγχρηματοδοτούμενων πιστώσεων	1,305	1,811	1,611	1,611	1,611	1,611	9,560

60 Βλ. άρθρα 11 και 17 του κανονισμού (ΕΕ, Ευρατόμ) αριθ. 1311/2013 του Συμβουλίου για τον καθορισμό του πολυετούς δημοσιονομικού πλαισίου για την περίοδο 2014-2020.

61 100 % των συνολικών εκτιμώμενων δαπανών συν τις πλήρεις συνταξιοδοτικές εισφορές του εργοδότη

62 100 % των συνολικών εκτιμώμενων δαπανών συν τις πλήρεις συνταξιοδοτικές εισφορές του εργοδότη

	2022	2023	2024	2025	2026	2027	Σύνολο
Οι δαπάνες θα καλυφθούν κατά 100 % από τέλη που θα επιβληθούν στις εποπτευόμενες οντότητες[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
ΣΥΝΟΛΟ συγχρηματοδοτούμενων πιστώσεων	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Εκτιμώμενες επιπτώσεις στα έσοδα

☑ Η πρόταση/πρωτοβουλία δεν έχει δημοσιονομικές επιπτώσεις στα έσοδα.

☐ Η πρόταση/πρωτοβουλία έχει τις δημοσιονομικές επιπτώσεις που περιγράφονται κατωτέρω:

☐ στους ιδίους πόρους

☐ στα λοιπά έσοδα

☐ Να αναφερθεί αν τα έσοδα προορίζονται για γραμμές δαπανών

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

Γραμμή εσόδων του προϋπολογισμού:	Διαθέσιμες πιστώσεις για το τρέχον οικονομικό έτος	Επιπτώσεις της πρότασης/πρωτοβουλίας[64]						
		Έτος **N**	Έτος **N+1**	Έτος **N+2**	Έτος **N+3**	Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6)		
Άρθρο …….								

Ως προς τα διάφορα έσοδα «για ειδικό προορισμό», να προσδιοριστούν οι γραμμές δαπανών του προϋπολογισμού που επηρεάζονται.

[…]

Να προσδιοριστεί η μέθοδος υπολογισμού των επιπτώσεων στα έσοδα.

[…]

63 100 % των συνολικών εκτιμώμενων δαπανών συν τις πλήρεις συνταξιοδοτικές εισφορές του εργοδότη

64 Όσον αφορά τους παραδοσιακούς ιδίους πόρους (δασμούς, εισφορές ζάχαρης), τα αναγραφόμενα ποσά πρέπει να είναι καθαρά ποσά, δηλ. τα ακαθάριστα ποσά μετά την αφαίρεση του 20 % για έξοδα είσπραξης.

ΠΑΡΑΡΤΗΜΑ

Γενικές παραδοχές

Τίτλος I — Δαπάνες προσωπικού

Οι ακόλουθες ειδικές παραδοχές εφαρμόστηκαν στον υπολογισμό των δαπανών προσωπικού με βάση τις διαπιστωθείσες ανάγκες προσωπικού που αναλύονται κατωτέρω:

- Το κόστος του πρόσθετου προσωπικού που θα προσληφθεί το 2022 υπολογίζεται για 6 μήνες δεδομένου του χρόνου που προβλέπεται ότι απαιτείται για την πρόσληψη του πρόσθετου προσωπικού
- Το μέσο ετήσιο κόστος έκτακτου υπαλλήλου ανέρχεται σε 150 000 EUR, στο οποίο περιλαμβάνονται περιφερειακές δαπάνες (habillage) ύψους 25 000 EUR (κτίρια, ΤΠ κ.λπ.)
- Οι διορθωτικοί συντελεστές που ισχύουν για τους μισθούς υπαλλήλων στο Παρίσι (EBA και ESMA) και στη Φρανκφούρτη (EIOPA) είναι 117,7 και 99,4 αντίστοιχα
- Οι συνταξιοδοτικές εισφορές του εργοδότη για έκτακτους υπαλλήλους βασίστηκαν στους τυποποιημένους βασικούς μισθούς που περιλαμβάνονται στον τυποποιημένο μέσο όρο ετήσιου κόστους, ήτοι 95 660 EUR
- Οι πρόσθετοι έκτακτοι υπάλληλοι είναι βαθμών AD5 και AST.

Τίτλος II — Δαπάνες υποδομών και λειτουργίας

Οι δαπάνες βασίζονται στο γινόμενο του αριθμού του προσωπικού επί το ποσοστό του έτους που απασχολήθηκε πολλαπλασιαζόμενο με τις τυποποιημένες περιφερειακές δαπάνες (habillage), ήτοι 25 000 EUR.

Τίτλος III — Λειτουργικές δαπάνες

Οι δαπάνες υπολογίζονται βάσει των ακόλουθων παραδοχών:

- Οι δαπάνες μετάφρασης ορίζονται σε 350 000 EUR ετησίως για κάθε ΕΕΑ
- Οι εφάπαξ δαπάνες ΤΠ ύψους 500 000 EUR ανά ΕΕΑ υπολογίζεται να υλοποιηθούν κατά τη διάρκεια της διετίας 2022-2023 με αναλογία 50 % – 50 %. Οι ετήσιες δαπάνες συντήρησης από το 2024 υπολογίζονται σε 50 000 EUR ανά ΕΕΑ
- Οι δαπάνες επιτόπιων ετήσιων επιθεωρήσεων υπολογίζονται σε 200 000 EUR ανά ΕΕΑ.

Οι εκτιμήσεις που παρατίθενται ανωτέρω συνεπάγονται τις ακόλουθες δαπάνες ανά έτος:

Τομέας του πολυετούς δημοσιονομικού πλαισίου	Αριθμός	

Σταθερές τιμές

ΕΒΑ:			2022	2023	2024	2025	2026	2027	**ΣΥΝΟΛΟ**
Τίτλος 1:	Αναλήψεις υποχρεώσεων	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Πληρωμές	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Τίτλος 2:	Αναλήψεις υποχρεώσεων	(1α)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Πληρωμές	(2α)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Τίτλος 3:	Αναλήψεις υποχρεώσεων	(3α)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Πληρωμές	(3β)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
ΣΥΝΟΛΟ πιστώσεων για την ΕΒΑ	Αναλήψεις υποχρεώσεων	=1+1α +3α	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Πληρωμές	=2+2α +3β	1,373	1,948	1,748	1,748	1,748	1,748	10,313

ΕΙΟΡΑ:			2022	2023	2024	2025	2026	2027	**ΣΥΝΟΛΟ**
Τίτλος 1:	Αναλήψεις υποχρεώσεων	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Πληρωμές	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Τίτλος 2:	Αναλήψεις υποχρεώσεων	(1α)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Πληρωμές	(2α)	0,075	0,150	0,150	0,150	0,150	0,150	0,825

Τίτλος 3:	Αναλήψεις υποχρεώσεων	(3α)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Πληρωμές	(3β)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
ΣΥΝΟΛΟ πιστώσεων για την EIOPA	Αναλήψεις υποχρεώσεων	=1+1α +3α	1,305	1,811	1,611	1,611	1,611	1,611	9,560
	Πληρωμές	=2+2α +3β	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA:			2022	2023	2024	2025	2026	2027	**ΣΥΝΟΛΟ**
Τίτλος 1:	Αναλήψεις υποχρεώσεων	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Πληρωμές	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Τίτλος 2:	Αναλήψεις υποχρεώσεων	(1α)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Πληρωμές	(2α)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Τίτλος 3:	Αναλήψεις υποχρεώσεων	(3α)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Πληρωμές	(3β)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
ΣΥΝΟΛΟ πιστώσεων για την ESMA	Αναλήψεις υποχρεώσεων	=1+1α +3α	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Πληρωμές	=2+2α +3β	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Η πρόταση συνεπάγεται τη χρησιμοποίηση επιχειρησιακών πιστώσεων, όπως εξηγείται κατωτέρω:

Πιστώσεις ανάληψης υποχρεώσεων σε εκατ. EUR (με τρία δεκαδικά ψηφία) σε σταθερές τιμές

ΕΒΑ

Να προσδιοριστούν οι στόχοι και τα αποτελέσματα ⇩			2022		2023		2024		2025		2026		2027			
	ΑΠΟΤΕΛΕΣΜΑΤΑ															
	Είδος[65]	Μέσο κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Συνολικός αριθ.	Συνολικό κόστος
ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ αριθ. 1[66] Άμεση εποπτεία κρίσιμων τρίτων παρόχων ΤΠΕ																
-				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Μερικό σύνολο για τον ειδικό στόχο αριθ. 1																
ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ αριθ. 2 ...																
-																
Μερικό σύνολο για τον ειδικό στόχο αριθ. 2																
ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ΕΙΟΡΑ

Να προσδιοριστούν οι στόχοι και τα αποτελέσματα ⇩			2022		2023		2024		2025		2026		2027			
	ΑΠΟΤΕΛΕΣΜΑΤΑ															
	Είδος[67]	Μέσο κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Συνολικός αριθ.	Συνολικό κόστος
ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ αριθ. 1[68] Άμεση εποπτεία																

[65] Τα αποτελέσματα είναι τα προϊόντα και οι υπηρεσίες που θα παρασχεθούν (π.χ.: αριθμός ανταλλαγών φοιτητών που θα χρηματοδοτηθούν, αριθμός χλμ. οδών που θα κατασκευαστούν κ.λπ.).

[66] Όπως περιγράφεται στο σημείο 1.4.2. «Ειδικοί στόχοι …»

[67] Τα αποτελέσματα είναι τα προϊόντα και οι υπηρεσίες που θα παρασχεθούν (π.χ.: αριθμός ανταλλαγών φοιτητών που θα χρηματοδοτηθούν, αριθμός χλμ. οδών που θα κατασκευαστούν κ.λπ.).

κρίσιμων τρίτων παρόχων ΤΠΕ															
-				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Μερικό σύνολο για τον ειδικό στόχο αριθ. 1															
ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ αριθ. 2 ...															
-															
Μερικό σύνολο για τον ειδικό στόχο αριθ. 2															
ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ESMA

Να προσδιοριστούν οι στόχοι και τα αποτελέσματα ⇩			2022		2023		2024		2025		2026		2027			
	ΑΠΟΤΕΛΕΣΜΑΤΑ															
	Είδος[69]	Μέσο κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Συνολικός αριθ.	Συνολικό κόστος
ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ αριθ. 1[70] Άμεση εποπτεία κρίσιμων τρίτων παρόχων ΤΠΕ																
-				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Μερικό σύνολο για τον ειδικό στόχο αριθ. 1																
ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ αριθ. 2 ...																
-																
Μερικό σύνολο για τον ειδικό στόχο αριθ. 2																
ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

[68] Όπως περιγράφεται στο σημείο 1.4.2. «Ειδικοί στόχοι …»

[69] Τα αποτελέσματα είναι τα προϊόντα και οι υπηρεσίες που θα παρασχεθούν (π.χ.: αριθμός ανταλλαγών φοιτητών που θα χρηματοδοτηθούν, αριθμός χλμ. οδών που θα κατασκευαστούν κ.λπ.).

[70] Όπως περιγράφεται στο σημείο 1.4.2. «Ειδικοί στόχοι …»

Οι δραστηριότητες εποπτείας θα χρηματοδοτηθούν πλήρως από τέλη που θα επιβληθούν στις εποπτευόμενες οντότητες ως εξής:

EBA

	2022	2023	2024	2025	2026	2027	Σύνολο
Οι δαπάνες θα καλυφθούν κατά 100 % από τέλη που θα επιβληθούν στις εποπτευόμενες οντότητες[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
ΣΥΝΟΛΟ συγχρηματοδοτούμενων πιστώσεων	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Σύνολο
Οι δαπάνες θα καλυφθούν κατά 100 % από τέλη που θα επιβληθούν στις εποπτευόμενες οντότητες[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
ΣΥΝΟΛΟ συγχρηματοδοτούμενων πιστώσεων	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Σύνολο

[71] 100 % των συνολικών εκτιμώμενων δαπανών συν τις πλήρεις συνταξιοδοτικές εισφορές του εργοδότη

[72] 100 % των συνολικών εκτιμώμενων δαπανών συν τις πλήρεις συνταξιοδοτικές εισφορές του εργοδότη

Οι δαπάνες θα καλυφθούν κατά 100 % από τέλη που θα επιβληθούν στις εποπτευόμενες οντότητες[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
ΣΥΝΟΛΟ συγχρηματοδοτούμενων πιστώσεων	1,373	1,948	1,748	1,748	1,748	1,748	10,313

ΕΙΔΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ

Εξουσίες άμεσης εποπτείας

Εισαγωγικά, υπενθυμίζεται ότι οι οντότητες που υπόκεινται στην άμεση εποπτεία της ESMA θα πρέπει να καταβάλλουν τέλη στην ESMA (εφάπαξ δαπάνες εγγραφής και επαναλαμβανόμενες δαπάνες διαρκούς εποπτείας). Αυτό ισχύει για τους οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας [βλ. κατ' εξουσιοδότηση κανονισμό (ΕΕ) αριθ. 272/2012 της Επιτροπής] και τα αρχεία καταγραφής συναλλαγών [κατ' εξουσιοδότηση κανονισμός (ΕΕ) αριθ. 1003/2013 της Επιτροπής].

Βάσει της παρούσας νομοθετικής πρότασης, θα ανατεθούν στις ΕΕΑ νέα καθήκοντα που αποσκοπούν στην προώθηση της σύγκλισης των εποπτικών προσεγγίσεων για τον κίνδυνο τρίτων παρόχων ΤΠΕ στον χρηματοπιστωτικό τομέα, με την υπαγωγή των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ στο πλαίσιο εποπτείας της Ένωσης.

Το πλαίσιο εποπτείας που προβλέπεται στην παρούσα πρόταση βασίζεται στην υφιστάμενη θεσμική αρχιτεκτονική του τομέα των χρηματοπιστωτικών υπηρεσιών, στο πλαίσιο της οποίας η μεικτή επιτροπή των ΕΕΑ διασφαλίζει τον διατομεακό συντονισμό σε σχέση με όλα τα ζητήματα που αφορούν τον κίνδυνο ΤΠΕ, σύμφωνα με τα καθήκοντά της για την κυβερνοασφάλεια, με την υποστήριξη της σχετικής υποεπιτροπής (φόρουμ εποπτείας) που εκτελεί τις προπαρασκευαστικές εργασίες για μεμονωμένες αποφάσεις και συλλογικές συστάσεις που απευθύνονται σε κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ.

Μέσω του πλαισίου αυτού, οι ΕΕΑ που ορίζονται ως κύριοι εποπτικοί φορείς για κάθε κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ αναλαμβάνουν εξουσίες ώστε να διασφαλίζεται ότι οι πάροχοι υπηρεσιών τεχνολογίας που διαδραματίζουν κρίσιμο ρόλο στη λειτουργία του χρηματοπιστωτικού τομέα παρακολουθούνται επαρκώς σε πανευρωπαϊκή κλίμακα. Τα καθήκοντα εποπτείας καθορίζονται στην πρόταση και διευκρινίζονται περαιτέρω στην αιτιολογική έκθεση. Περιλαμβάνουν το δικαίωμα να ζητούν όλες τις σχετικές πληροφορίες και έγγραφα τεκμηρίωσης για τη διεξαγωγή γενικών ερευνών και επιθεωρήσεων, για τη διατύπωση συστάσεων και, στη συνέχεια, την υποβολή εκθέσεων σχετικά με τις ενέργειες που έχουν αναληφθεί ή τα διορθωτικά μέτρα που εφαρμόστηκαν για την υλοποίηση των εν λόγω συστάσεων.

Ως εκ τούτου, για την εκτέλεση των νέων καθηκόντων που προβλέπονται στην παρούσα πρόταση, οι ΕΕΑ προσλαμβάνουν πρόσθετο εξειδικευμένο προσωπικό σε θέματα κινδύνων ΤΠΕ και δίνουν έμφαση στην αξιολόγηση των εξαρτήσεων τρίτων.

Οι ανάγκες σε ανθρώπινους πόρους μπορούν να εκτιμηθούν σε 6 ΙΠΑ για κάθε αρχή (5 στον βαθμό AD και 1 στον βαθμό AST για την υποστήριξη του βαθμού AD). Οι ΕΕΑ θα επιβαρυνθούν επίσης με πρόσθετες δαπάνες ΤΠ, εκτιμώμενου ύψους 500 000 EUR (εφάπαξ δαπάνες), καθώς και με δαπάνες

[73] 100 % των συνολικών εκτιμώμενων δαπανών συν τις πλήρεις συνταξιοδοτικές εισφορές του εργοδότη

συντήρησης ύψους 50 000 EUR ετησίως για καθεμία από τις τρεις ΕΕΑ. Ένα σημαντικό στοιχείο για την εκπλήρωση των νέων καθηκόντων είναι οι αποστολές για τη διεξαγωγή επιτόπιων επιθεωρήσεων και ελέγχων, οι οποίες ανέρχονται κατ' εκτίμηση σε 200 000 EUR ετησίως για κάθε ΕΕΑ. Οι δαπάνες μετάφρασης των διαφόρων εγγράφων που θα λαμβάνουν οι ΕΕΑ από τους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ περιλαμβάνονται επίσης στη γραμμή των λειτουργικών δαπανών και ανέρχονται σε 350 000 EUR ετησίως.

Όλες οι διοικητικές δαπάνες που αναφέρονται ανωτέρω θα χρηματοδοτηθούν πλήρως από τα ετήσια τέλη που επιβάλλουν οι ΕΕΑ στους εποπτευόμενους κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ (χωρίς επιπτώσεις στον προϋπολογισμό της ΕΕ).