Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2024/1773

25.6.2024

ΚΑΤ' ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2024/1773 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 13ης Μαρτίου 2024

για τη συμπλήρωση του κανονισμού (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τα ρυθμιστικά τεχνικά πρότυπα για τον προσδιορισμό των λεπτομερειών του περιεχομένου της πολιτικής σε σχέση με τις συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ οι οποίες υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη τον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 ([1]), και ιδίως το άρθρο 28 παράγραφος 10 τρίτο εδάφιο,

Εκτιμώντας τα ακόλουθα:

(1) Το πλαίσιο για την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα που θεσπίστηκε με τον κανονισμό (ΕΕ) 2022/2554 απαιτεί από τις χρηματοοικονομικές οντότητες να καθορίζουν συγκεκριμένες βασικές αρχές για τη διαχείριση του κινδύνου τρίτων παρόχων ΤΠΕ, οι οποίες είναι ιδιαίτερα σημαντικές όταν οι χρηματοοικονομικές οντότητες συνεργάζονται με τρίτους παρόχους υπηρεσιών ΤΠΕ για την υποστήριξη των κρίσιμων ή σημαντικών λειτουργιών τους.

(2) Οι χρηματοοικονομικές οντότητες, στο πλαίσιο της οικείας διαχείρισης κινδύνου ΤΠΕ, πρέπει να εγκρίνουν και να επανεξετάζουν τακτικά τη στρατηγική για τους κινδύνους τρίτων παρόχων ΤΠΕ. Σύμφωνα με το άρθρο 28 παράγραφος 2 του κανονισμού (ΕΕ) 2022/2554, η εν λόγω στρατηγική πρέπει να περιλαμβάνει πολιτική για τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες οι οποίες παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ. Η στρατηγική αυτή εφαρμόζεται σε μεμονωμένη βάση και, ανάλογα με την περίπτωση, σε υποενοποιημένη και ενοποιημένη βάση.

(3) Οι χρηματοοικονομικές οντότητες διαφέρουν σημαντικά ως προς το μέγεθος, τη δομή και την εσωτερική οργάνωση, καθώς και ως προς τη φύση και την πολυπλοκότητα των δραστηριοτήτων και των λειτουργιών τους. Είναι αναγκαίο να ληφθεί υπόψη η εν λόγω πολυμορφία, ενώ παράλληλα πρέπει να επιβληθούν συγκεκριμένες θεμελιώδεις κανονιστικές απαιτήσεις που είναι κατάλληλες για όλες τις χρηματοοικονομικές οντότητες κατά την κατάρτιση της πολιτικής για τις συμβατικές ρυθμίσεις σχετικά με τη χρήση υπηρεσιών ΤΠΕ οι οποίες υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ (στο εξής: πολιτική), και να διασφαλιστεί ότι οι εν λόγω απαιτήσεις εφαρμόζονται κατά τρόπο αναλογικό.

(4) Όταν οι χρηματοοικονομικές οντότητες ανήκουν σε όμιλο, η μητρική επιχείρηση που είναι υπεύθυνη για την παροχή των ενοποιημένων ή υποενοποιημένων οικονομικών καταστάσεων για τον όμιλο θα πρέπει συνεπώς να διασφαλίζει ότι η πολιτική εφαρμόζεται με συνεπή και συνεκτικό τρόπο εντός του ομίλου.

(5) Κατά την εφαρμογή της πολιτικής, οι ενδοομιλικοί πάροχοι υπηρεσιών ΤΠΕ, συμπεριλαμβανομένων εκείνων που ανήκουν εξολοκλήρου ή συλλογικά σε χρηματοοικονομικές οντότητες εντός του ίδιου θεσμικού συστήματος προστασίας, θα πρέπει να θεωρούνται τρίτοι πάροχοι υπηρεσιών ΤΠΕ. Οι κίνδυνοι που ενέχουν οι ενδοομιλικοί πάροχοι υπηρεσιών ΤΠΕ μπορεί να διαφέρουν, αλλά οι απαιτήσεις που ισχύουν γι' αυτούς είναι οι ίδιες σύμφωνα με τον κανονισμό (ΕΕ) 2022/2554. Κατά τον ίδιο τρόπο, η πολιτική θα πρέπει να εφαρμόζεται σε υπεργολάβους που παρέχουν υπηρεσίες ΤΠΕ οι οποίες υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες ή σημαντικά μέρη αυτών σε τρίτους παρόχους υπηρεσιών ΤΠΕ, όταν υπάρχει αλυσίδα τρίτων παρόχων υπηρεσιών ΤΠΕ.

(6) Η τελική ευθύνη του διοικητικού οργάνου για τη διαχείριση του κινδύνου ΤΠΕ μιας χρηματοοικονομικής οντότητας αποτελεί γενική αρχή η οποία εφαρμόζεται επίσης όσον αφορά τη χρήση τρίτων παρόχων υπηρεσιών ΤΠΕ. Η ευθύνη αυτή θα πρέπει να μετουσιώνεται περαιτέρω στη διαρκή συμμετοχή του διοικητικού οργάνου στον έλεγχο και στην παρακολούθηση της διαχείρισης κινδύνου ΤΠΕ, συμπεριλαμβανομένης της έγκρισης και επανεξέτασης, τουλάχιστον μία φορά ετησίως, της πολιτικής.

([1]) ΕΕ L 333 της 27.12.2022, σ. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(7) Για τη διασφάλιση της κατάλληλης υποβολής εκθέσεων στο διοικητικό όργανο, στην πολιτική θα πρέπει να προσδιορίζονται και να υποδεικνύονται σαφώς οι εσωτερικές αρμοδιότητες για την έγκριση, τη διαχείριση, τον έλεγχο και την τεκμηρίωση των συμβατικών ρυθμίσεων σχετικά με τη χρήση υπηρεσιών ΤΠΕ οι οποίες υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ (στο εξής: συμβατικές ρυθμίσεις), συμπεριλαμβανομένων των υπηρεσιών ΤΠΕ που παρέχονται βάσει συμβατικών ρυθμίσεων που αναφέρονται στο άρθρο 28 παράγραφος 1 στοιχείο α) του κανονισμού (ΕΕ) 2022/2554.

(8) Προκειμένου να λαμβάνονται υπόψη όλοι οι πιθανοί κίνδυνοι που ενδέχεται να προκύψουν κατά τη σύναψη συμβάσεων για υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμη ή σημαντική λειτουργία, η δομή της πολιτικής θα πρέπει να ακολουθεί όλα τα στάδια κάθε κύριας φάσης του κύκλου ζωής για τις συμβατικές ρυθμίσεις με τρίτους παρόχους.

(9) Για τον μετριασμό των κινδύνων που εντοπίζονται, η πολιτική θα πρέπει να προσδιορίζει τον σχεδιασμό των συμβατικών ρυθμίσεων, συμπεριλαμβανομένης της αξιολόγησης κινδύνων, της δέουσας επιμέλειας και της διαδικασίας έγκρισης νέων ή σημαντικών αλλαγών των εν λόγω συμβατικών ρυθμίσεων. Για τη διαχείριση των κινδύνων που ενδέχεται να προκύψουν πριν από τη σύναψη συμβατικής ρύθμισης με τρίτο πάροχο υπηρεσιών ΤΠΕ, η πολιτική θα πρέπει να προσδιορίζει κατάλληλη και αναλογική διαδικασία για την επιλογή και την αξιολόγηση της καταλληλότητας των υποψήφιων τρίτων παρόχων υπηρεσιών ΤΠΕ και να επιβάλλει στη χρηματοοικονομική οντότητα την υποχρέωση να λαμβάνει υπόψη μη εξαντλητικό κατάλογο στοιχείων που θα πρέπει να διαθέτουν οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ. Ο κατάλογος θα πρέπει να περιλαμβάνει στοιχεία σε σχέση με την επιχειρηματική φήμη των παρόχων υπηρεσιών, τους οικονομικούς, ανθρώπινους και τεχνικούς πόρους τους, την ασφάλεια των πληροφοριών τους, την οργανωτική δομή τους, συμπεριλαμβανομένης της διαχείρισης κινδύνων, και τους εσωτερικούς ελέγχους τους.

(10) Για τη διασφάλιση της χρηστής διαχείρισης κινδύνων κατά την παροχή υπηρεσιών ΤΠΕ οι οποίες υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες από τρίτους παρόχους υπηρεσιών ΤΠΕ, η πολιτική θα πρέπει να περιλαμβάνει πληροφορίες σχετικά με την εφαρμογή, την παρακολούθηση και τη διαχείριση των συμβατικών ρυθμίσεων, μεταξύ άλλων σε ενοποιημένο και υποενοποιημένο επίπεδο, κατά περίπτωση. Αυτό περιλαμβάνει απαιτήσεις για τις συμβατικές ρήτρες σχετικά με τις αμοιβαίες υποχρεώσεις των χρηματοοικονομικών οντοτήτων και των τρίτων παρόχων υπηρεσιών ΤΠΕ, οι οποίες θα πρέπει να καθορίζονται γραπτώς. Προκειμένου να διασφαλιστεί η αποτελεσματική εποπτεία και να ενισχυθεί η ανθεκτικότητα σε περίπτωση αλλαγών στο επιχειρηματικό μοντέλο ή στο επιχειρηματικό περιβάλλον, η πολιτική θα πρέπει να διασφαλίζει τα δικαιώματα των χρηματοοικονομικών οντοτήτων ή των διορισμένων τρίτων φορέων και των αρμόδιων αρχών όσον αφορά τις επιθεωρήσεις και την πρόσβαση σε πληροφορίες, και θα πρέπει επίσης να προσδιορίζει περαιτέρω τις στρατηγικές εξόδου και τις διαδικασίες καταγγελίας.

(11) Στον βαθμό που τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία από τρίτους παρόχους υπηρεσιών ΤΠΕ, η πολιτική αυτή και τυχόν συμβατικές ρυθμίσεις δεν θίγουν και θα πρέπει να συμπληρώνουν τις υποχρεώσεις που απορρέουν από τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([2]), όπως η σύναψη γραπτής σύμβασης στην οποία περιγράφεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα, η απαίτηση διασφάλισης της ασφάλειας της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και ο καθορισμός όλων των άλλων στοιχείων που απαιτούνται σύμφωνα με τον εν λόγω κανονισμό.

([2]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Η μεικτή επιτροπή των Ευρωπαϊκών Εποπτικών Αρχών που αναφέρεται στο άρθρο 54 του κανονισμού (ΕΕ) αριθ. 1093/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([3]), στο άρθρο 54 του κανονισμού (ΕΕ) αριθ. 1094/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([4]) και στο άρθρο 54 του κανονισμού (ΕΕ) αριθ. 1095/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([5]) διενήργησε ανοικτές δημόσιες διαβουλεύσεις σχετικά με τα σχέδια ρυθμιστικών τεχνικών προτύπων στα οποία βασίζεται ο παρών κανονισμός, ανέλυσε το δυνητικό κόστος και τα οφέλη των προτεινόμενων προτύπων και ζήτησε συμβουλές από την ομάδα τραπεζικών συμφεροντούχων που συστάθηκε σύμφωνα με το άρθρο 37 του κανονισμού (ΕΕ) αριθ. 1093/2010, την ομάδα συμφεροντούχων ασφαλίσεων και αντασφαλίσεων και την ομάδα συμφεροντούχων ταμείων επαγγελματικών συνταξιοδοτικών παροχών που συστάθηκαν σύμφωνα με το άρθρο 37 του κανονισμού (ΕΕ) αριθ. 1094/2010 και την ομάδα συμφεροντούχων κινητών αξιών και αγορών που συστάθηκε σύμφωνα με το άρθρο 37 του κανονισμού (ΕΕ) αριθ. 1095/2010,

(13) Ζητήθηκε η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6]), ο οποίος γνωμοδότησε στις 24 Ιανουαρίου 2024,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Άρθρο 1

Συνολικό προφίλ κινδύνου και πολυπλοκότητα

Η πολιτική σχετικά με τη χρήση υπηρεσιών ΤΠΕ οι οποίες υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ (στο εξής: πολιτική) λαμβάνει υπόψη το μέγεθος και το συνολικό προφίλ κινδύνου της χρηματοοικονομικής οντότητας, καθώς και τη φύση, την κλίμακα και τα στοιχεία αυξημένης ή μειωμένης πολυπλοκότητας των υπηρεσιών, των δραστηριοτήτων και των λειτουργιών της, συμπεριλαμβανομένων των στοιχείων που αφορούν:

α) το είδος των υπηρεσιών ΤΠΕ που περιλαμβάνονται στη συμβατική ρύθμιση σχετικά με τη χρήση υπηρεσιών ΤΠΕ οι οποίες υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ (στο εξής: συμβατική ρύθμιση) μεταξύ της χρηματοοικονομικής οντότητας και του τρίτου παρόχου υπηρεσιών ΤΠΕ·

β) την τοποθεσία του τρίτου παρόχου υπηρεσιών ΤΠΕ ή την τοποθεσία της μητρικής εταιρείας του·

γ) αν οι υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες παρέχονται από τρίτο πάροχο υπηρεσιών ΤΠΕ ο οποίος βρίσκεται σε κράτος μέλος ή σε τρίτη χώρα, λαμβάνοντας επίσης υπόψη την τοποθεσία από την οποία παρέχονται οι υπηρεσίες ΤΠΕ και την τοποθεσία στην οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται τα δεδομένα·

δ) τη φύση των δεδομένων που κοινοποιούνται στον τρίτο πάροχο υπηρεσιών ΤΠΕ·

ε) αν ο τρίτος πάροχος υπηρεσιών ΤΠΕ είναι μέλος του ίδιου ομίλου με τη χρηματοοικονομική οντότητα στην οποία παρέχονται οι υπηρεσίες·

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

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

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

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

στ) τη χρήση τρίτων παρόχων υπηρεσιών ΤΠΕ που έχουν λάβει άδεια λειτουργίας, είναι εγγεγραμμένες οντότητες ή υπόκεινται σε εποπτεία ή επίβλεψη από αρμόδια αρχή κράτους μέλους ή υπόκεινται στο πλαίσιο εποπτείας σύμφωνα με το κεφάλαιο V τμήμα II του κανονισμού (ΕΕ) 2022/2554, και τη χρήση τρίτων παρόχων υπηρεσιών ΤΠΕ που δεν εμπίπτουν στις παραπάνω περιπτώσεις·

ζ) τη χρήση τρίτων παρόχων υπηρεσιών ΤΠΕ που έχουν λάβει άδεια λειτουργίας, είναι εγγεγραμμένες οντότητες ή υπόκεινται σε εποπτεία ή επίβλεψη από εποπτική αρχή τρίτης χώρας και τη χρήση τρίτων παρόχων υπηρεσιών ΤΠΕ που δεν εμπίπτουν στις παραπάνω περιπτώσεις·

η) αν η παροχή υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες συγκεντρώνεται σε έναν μόνο τρίτο πάροχο υπηρεσιών ΤΠΕ ή σε μικρό αριθμό τέτοιων παρόχων υπηρεσιών·

θ) τη δυνατότητα μεταφοράς των υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες σε άλλον τρίτο πάροχο υπηρεσιών ΤΠΕ, μεταξύ άλλων λόγω τεχνολογικών ιδιαιτεροτήτων·

ι) τον δυνητικό αντίκτυπο των διαταραχών της παροχής των υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες στη συνέχεια των δραστηριοτήτων της χρηματοοικονομικής οντότητας και στη διαθεσιμότητα των υπηρεσιών της.

Άρθρο 2

Εφαρμογή σε επίπεδο ομίλου

Όταν ο παρών κανονισμός εφαρμόζεται σε υποενοποιημένη ή ενοποιημένη βάση, η μητρική επιχείρηση που είναι υπεύθυνη για την παροχή των ενοποιημένων ή υποενοποιημένων οικονομικών καταστάσεων του ομίλου διασφαλίζει ότι η πολιτική εφαρμόζεται με συνέπεια σε όλες τις χρηματοοικονομικές οντότητες που είναι μέλη του ομίλου και είναι επαρκής για την αποτελεσματική εφαρμογή του παρόντος κανονισμού σε όλα τα σχετικά επίπεδα του ομίλου.

Άρθρο 3

Ρυθμίσεις διακυβέρνησης

1. Το διοικητικό όργανο επανεξετάζει την πολιτική τουλάχιστον μία φορά ετησίως και την επικαιροποιεί, εφόσον κρίνεται αναγκαίο. Οι αλλαγές που επέρχονται στην πολιτική εφαρμόζονται εγκαίρως και το συντομότερο δυνατό στο πλαίσιο των σχετικών συμβατικών ρυθμίσεων. Η χρηματοοικονομική οντότητα τεκμηριώνει το προβλεπόμενο χρονοδιάγραμμα για την εφαρμογή.

2. Στην πολιτική καθορίζεται ή αναφέρεται η μεθοδολογία για τον προσδιορισμό των υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες. Στην πολιτική προσδιορίζεται επίσης πότε πρέπει να διενεργείται και να επανεξετάζεται η εν λόγω αξιολόγηση.

3. Η πολιτική περιλαμβάνει σαφή ανάθεση των εσωτερικών αρμοδιοτήτων για την έγκριση, τη διαχείριση, τον έλεγχο και την τεκμηρίωση των σχετικών συμβατικών ρυθμίσεων και διασφαλίζει τη διατήρηση κατάλληλων δεξιοτήτων, πείρας και γνώσεων εντός της χρηματοοικονομικής οντότητας για την αποτελεσματική εποπτεία των σχετικών συμβατικών ρυθμίσεων, συμπεριλαμβανομένων των υπηρεσιών ΤΠΕ που παρέχονται στο πλαίσιο των εν λόγω ρυθμίσεων.

4. Με την επιφύλαξη της τελικής ευθύνης της χρηματοοικονομικής οντότητας όσον αφορά την αποτελεσματική επίβλεψη των σχετικών συμβατικών ρυθμίσεων, η πολιτική απαιτεί να αξιολογείται ο τρίτος πάροχος υπηρεσιών ΤΠΕ ως προς το αν διαθέτει επαρκείς πόρους ώστε να διασφαλίζεται ότι η χρηματοοικονομική οντότητα συμμορφώνεται με όλες τις νομικές και κανονιστικές απαιτήσεις της όσον αφορά τις παρεχόμενες υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες.

5. Η πολιτική προσδιορίζει σαφώς τον ρόλο ή το ανώτερο διοικητικό στέλεχος που είναι αρμόδιο για την παρακολούθηση των σχετικών συμβατικών ρυθμίσεων. Η πολιτική διευκρινίζει τον τρόπο συνεργασίας μεταξύ του εν λόγω ρόλου ή του ανώτερου διοικητικού στελέχους και των λειτουργιών ελέγχου, εκτός αν είναι μέρος αυτών, και καθορίζει τους διαύλους αναφοράς προς το διοικητικό όργανο, συμπεριλαμβανομένης της φύσης των πληροφοριών που πρέπει να υποβάλλονται και των εγγράφων που πρέπει να παρέχονται. Καθορίζει επίσης τη συχνότητα των αναφορών αυτών.

6. Η πολιτική διασφαλίζει ότι οι συμβατικές ρυθμίσεις συνάδουν με:

α) το πλαίσιο διαχείρισης κινδύνων ΤΠΕ που αναφέρεται στο άρθρο 6 του κανονισμού (ΕΕ) 2022/2554·

β) την πολιτική ασφάλειας των πληροφοριών που αναφέρεται στο άρθρο 9 παράγραφος 4 του κανονισμού (ΕΕ) 2022/2554·

γ) την πολιτική επιχειρησιακής συνέχειας των ΤΠΕ που αναφέρεται στο άρθρο 11 του κανονισμού (ΕΕ) 2022/2554·

δ) τις απαιτήσεις για την αναφορά συμβάντων που ορίζονται στο άρθρο 19 του κανονισμού (ΕΕ) 2022/2554.

7. Η πολιτική ορίζει ότι οι υπηρεσίες ΤΠΕ οι οποίες υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ πρέπει να υπόκεινται σε ανεξάρτητη επανεξέταση και να περιλαμβάνονται στο σχέδιο ελέγχου.

8. Στην πολιτική διευκρινίζεται ρητά ότι οι συμβατικές ρυθμίσεις:

α) δεν απαλλάσσουν τη χρηματοοικονομική οντότητα και το διοικητικό της όργανο από τις κανονιστικές υποχρεώσεις και τις ευθύνες της χρηματοοικονομικής οντότητας έναντι των πελατών της·

β) δεν εμποδίζουν την αποτελεσματική εποπτεία μιας χρηματοοικονομικής οντότητας και δεν παραβιάζουν τυχόν εποπτικούς περιορισμούς στις υπηρεσίες και τις δραστηριότητες·

γ) επιβάλλουν στους τρίτους παρόχους υπηρεσιών ΤΠΕ να συνεργάζονται με τις αρμόδιες αρχές·

δ) απαιτούν η χρηματοοικονομική οντότητα, οι ελεγκτές της και οι αρμόδιες αρχές να έχουν αποτελεσματική πρόσβαση σε δεδομένα και εγκαταστάσεις που σχετίζονται με τη χρήση υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες.

Άρθρο 4

Κύριες φάσεις του κύκλου ζωής για την έγκριση και τη χρήση των συμβατικών ρυθμίσεων

Η πολιτική προσδιορίζει τις απαιτήσεις, συμπεριλαμβανομένων των κανόνων, των αρμοδιοτήτων και των διαδικασιών, για κάθε κύρια φάση του κύκλου ζωής της συμβατικής ρύθμισης, καλύπτοντας τουλάχιστον τα ακόλουθα:

α) τις αρμοδιότητες του διοικητικού οργάνου, συμπεριλαμβανομένης της συμμετοχής του, κατά περίπτωση, στη διαδικασία λήψης αποφάσεων σχετικά με τη χρήση υπηρεσιών ΤΠΕ οι οποίες υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ·

β) τον σχεδιασμό των συμβατικών ρυθμίσεων, συμπεριλαμβανομένης της αξιολόγησης κινδύνου, της δέουσας επιμέλειας όπως ορίζεται στα άρθρα 5 και 6 και της διαδικασίας έγκρισης όσον αφορά νέες ή σημαντικές αλλαγές στις συμβατικές ρυθμίσεις, όπως ορίζεται στο άρθρο 8 παράγραφος 4·

γ) τη συμμετοχή επιχειρηματικών μονάδων, μονάδων εσωτερικών ελέγχων και άλλων σχετικών μονάδων όσον αφορά τις συμβατικές ρυθμίσεις·

δ) την εφαρμογή, την παρακολούθηση και τη διαχείριση των συμβατικών ρυθμίσεων που αναφέρονται στα άρθρα 7, 8 και 9, μεταξύ άλλων σε ενοποιημένο και υποενοποιημένο επίπεδο, κατά περίπτωση·

ε) την τεκμηρίωση και την τήρηση αρχείων, λαμβάνοντας υπόψη τις απαιτήσεις όσον αφορά το μητρώο πληροφοριών που προβλέπεται στο άρθρο 28 παράγραφος 3 του κανονισμού (ΕΕ) 2022/2554·

στ) τις στρατηγικές εξόδου και τις διαδικασίες καταγγελίας, όπως ορίζονται στο άρθρο 10.

Άρθρο 5

Εκ των προτέρων αξιολόγηση κινδύνων

1. Η πολιτική απαιτεί τον καθορισμό των επιχειρηματικών αναγκών της χρηματοοικονομικής οντότητας πριν από τη σύναψη συμβατικής ρύθμισης.

2. Η πολιτική απαιτεί τη διενέργεια αξιολόγησης κινδύνων σε επίπεδο χρηματοοικονομικής οντότητας και, κατά περίπτωση, σε ενοποιημένο και υποενοποιημένο επίπεδο πριν από τη σύναψη συμβατικής ρύθμισης.

Κατά την αξιολόγηση των κινδύνων λαμβάνονται υπόψη όλες οι σχετικές απαιτήσεις που ορίζονται στον κανονισμό (ΕΕ) 2022/2554 και στην ισχύουσα τομεακή νομοθεσία της Ένωσης. Ειδικότερα, εξετάζονται οι επιπτώσεις της παροχής υπηρεσιών ΤΠΕ οι οποίες υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες που παρέχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ στη χρηματοοικονομική οντότητα και όλοι οι κίνδυνοι που ενέχει η παροχή των εν λόγω υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες από τρίτους παρόχους υπηρεσιών ΤΠΕ, συμπεριλαμβανομένων των ακόλουθων:

α) λειτουργικών κινδύνων·

β) νομικών κινδύνων·

γ) κινδύνων ΤΠΕ·

δ) κινδύνων φήμης·

ε) κινδύνων που συνδέονται με την προστασία των εμπιστευτικών δεδομένων ή των δεδομένων προσωπικού χαρακτήρα·

στ) κινδύνων που συνδέονται με τη διαθεσιμότητα των δεδομένων·

ζ) κινδύνων που συνδέονται με την τοποθεσία στην οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται τα δεδομένα·

η) κινδύνων που συνδέονται με την τοποθεσία του τρίτου παρόχου υπηρεσιών ΤΠΕ·

θ) κινδύνων συγκέντρωσης ΤΠΕ σε επίπεδο οντότητας.

Άρθρο 6

Δέουσα επιμέλεια

1. Η πολιτική καθορίζει κατάλληλη και αναλογική διαδικασία για την επιλογή και την αξιολόγηση των υποψήφιων τρίτων παρόχων υπηρεσιών ΤΠΕ, λαμβάνοντας υπόψη αν ο τρίτος πάροχος υπηρεσιών ΤΠΕ είναι ενδοομιλικός πάροχος υπηρεσιών ΤΠΕ ή όχι, και απαιτεί από τη χρηματοοικονομική οντότητα να αξιολογεί, πριν από τη σύναψη συμβατικής ρύθμισης, αν ο τρίτος πάροχος υπηρεσιών ΤΠΕ:

α) διαθέτει την επιχειρηματική φήμη, επαρκείς ικανότητες, εμπειρογνωσία και επαρκείς οικονομικούς, ανθρώπινους και τεχνικούς πόρους, πρότυπα ασφάλειας των πληροφοριών, κατάλληλη οργανωτική δομή, διαχείριση κινδύνων και εσωτερικούς ελέγχους και, κατά περίπτωση, τις απαιτούμενες άδειες ή καταχωρίσεις για την παροχή υπηρεσιών ΤΠΕ που υποστηρίζουν την κρίσιμη ή σημαντική λειτουργία με αξιόπιστο και επαγγελματικό τρόπο·

β) έχει την ικανότητα να παρακολουθεί τις σχετικές τεχνολογικές εξελίξεις και να εντοπίζει πρωτοπόρες πρακτικές στον τομέα της ασφάλειας ΤΠΕ και να τις εφαρμόζει, κατά περίπτωση, ώστε να διαθέτει αποτελεσματικό και άρτιο πλαίσιο ψηφιακής επιχειρησιακής ανθεκτικότητας·

γ) χρησιμοποιεί ή προτίθεται να χρησιμοποιήσει υπεργολάβους ΤΠΕ για την εκτέλεση των υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες ή σημαντικά μέρη αυτών·

δ) βρίσκεται, ή επεξεργάζεται ή αποθηκεύει τα δεδομένα σε τρίτη χώρα και, στην περίπτωση αυτή, αν η συγκεκριμένη πρακτική επηρεάζει το επίπεδο του λειτουργικού κινδύνου ή του κινδύνου φήμης ή τον κίνδυνο να επηρεαστεί από περιοριστικά μέτρα, συμπεριλαμβανομένων εμπάργκο και κυρώσεων, που ενδέχεται να επηρεάσουν την ικανότητα του τρίτου παρόχου υπηρεσιών ΤΠΕ να παρέχει τις υπηρεσίες ΤΠΕ ή της χρηματοοικονομικής οντότητας να λαμβάνει τις εν λόγω υπηρεσίες ΤΠΕ·

ε) εγκρίνει συμβατικές ρυθμίσεις που διασφαλίζουν ότι είναι πρακτικά δυνατή η διενέργεια ελέγχων στον τρίτο πάροχο υπηρεσιών ΤΠΕ, μεταξύ άλλων επιτόπου, από την ίδια τη χρηματοοικονομική οντότητα, από διορισμένους τρίτους και τις αρμόδιες αρχές·

στ) ενεργεί με δεοντολογικό και κοινωνικά υπεύθυνο τρόπο, σέβεται τα ανθρώπινα δικαιώματα και τα δικαιώματα των παιδιών, συμπεριλαμβανομένης της απαγόρευσης της παιδικής εργασίας, σέβεται τις εφαρμοστέες αρχές για την προστασία του περιβάλλοντος και διασφαλίζει κατάλληλες συνθήκες εργασίας.

2. Η πολιτική προσδιορίζει το απαιτούμενο επίπεδο διασφάλισης όσον αφορά την αποτελεσματικότητα του πλαισίου διαχείρισης κινδύνων τρίτων παρόχων υπηρεσιών ΤΠΕ για τις υπηρεσίες ΤΠΕ οι οποίες υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες που πρόκειται να παρασχεθούν από τρίτο πάροχο υπηρεσιών ΤΠΕ. Η πολιτική απαιτεί η διαδικασία δέουσας επιμέλειας να περιλαμβάνει αξιολόγηση της ύπαρξης μέτρων μετριασμού του κινδύνου και επιχειρησιακής συνέχειας, καθώς και του τρόπου με τον οποίο διασφαλίζεται η λειτουργία τους εντός του τρίτου παρόχου υπηρεσιών ΤΠΕ.

3. Η πολιτική καθορίζει τη διαδικασία δέουσας επιμέλειας για την επιλογή και την αξιολόγηση των υποψήφιων τρίτων παρόχων υπηρεσιών ΤΠΕ και αναφέρει ποια από τα ακόλουθα στοιχεία πρόκειται να χρησιμοποιηθούν για το απαιτούμενο επίπεδο διασφάλισης των επιδόσεων του τρίτου παρόχου υπηρεσιών ΤΠΕ:

α) έλεγχοι ή ανεξάρτητες αξιολογήσεις που διενεργούνται από την ίδια τη χρηματοοικονομική οντότητα ή για λογαριασμό της·

β) η χρήση εκθέσεων ανεξάρτητου ελέγχου που υποβάλλονται κατόπιν αιτήματος από τον τρίτο πάροχο υπηρεσιών ΤΠΕ·

γ) η χρήση εκθέσεων ελέγχου που υποβάλλονται από τη λειτουργία εσωτερικού ελέγχου του τρίτου παρόχου υπηρεσιών ΤΠΕ·

δ) η χρήση κατάλληλων πιστοποιήσεων από τρίτους·

ε) η χρήση άλλων σχετικών πληροφοριών που έχει στη διάθεσή της η χρηματοοικονομική οντότητα ή άλλων πληροφοριών που παρέχονται από τον τρίτο πάροχο υπηρεσιών ΤΠΕ.

4. Οι χρηματοοικονομικές οντότητες μεριμνούν για το κατάλληλο επίπεδο διασφάλισης των επιδόσεων του τρίτου παρόχου υπηρεσιών ΤΠΕ, λαμβάνοντας υπόψη τα στοιχεία που απαριθμούνται στην παράγραφο 3 στοιχεία α) έως ε). Κατά περίπτωση, χρησιμοποιούνται περισσότερα από ένα στοιχεία από αυτά που παρατίθενται ανωτέρω.

Άρθρο 7

Συγκρούσεις συμφερόντων

1. Η πολιτική προσδιορίζει τα κατάλληλα μέτρα για τον εντοπισμό, την πρόληψη και τη διαχείριση πραγματικών ή δυνητικών συγκρούσεων συμφερόντων που προκύπτουν από τη χρήση τρίτων παρόχων υπηρεσιών ΤΠΕ, τα οποία λαμβάνονται πριν από τη σύναψη σχετικών συμβατικών ρυθμίσεων, και προβλέπει τη συνεχή παρακολούθηση των εν λόγω συγκρούσεων συμφερόντων.

2. Όταν οι υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες παρέχονται από ενδοομιλικούς παρόχους υπηρεσιών ΤΠΕ, η πολιτική διευκρινίζει ότι οι αποφάσεις σχετικά με τους όρους, συμπεριλαμβανομένων των οικονομικών όρων, για τις υπηρεσίες ΤΠΕ πρέπει να λαμβάνονται αντικειμενικά.

Άρθρο 8

Συμβατικές ρήτρες

1. Στην πολιτική διευκρινίζεται ότι η σχετική συμβατική ρύθμιση πρέπει να είναι γραπτή και να περιλαμβάνει όλα τα στοιχεία που αναφέρονται στο άρθρο 30 παράγραφοι 2 και 3 του κανονισμού (ΕΕ) 2022/2554. Η πολιτική περιλαμβάνει επίσης στοιχεία σχετικά με τις απαιτήσεις που αναφέρονται στο άρθρο 1 παράγραφος 1 στοιχείο α) του κανονισμού (ΕΕ) 2022/2554, καθώς και στη λοιπή σχετική ενωσιακή και εθνική νομοθεσία, κατά περίπτωση.

2. Η πολιτική διευκρινίζει ότι οι σχετικές συμβατικές ρυθμίσεις πρέπει να περιλαμβάνουν το δικαίωμα της χρηματοοικονομικής οντότητας να έχει πρόσβαση σε πληροφορίες, να διενεργεί επιθεωρήσεις και ελέγχους και να εκτελεί δοκιμές σε ΤΠΕ. Για τον σκοπό αυτό, η πολιτική απαιτεί από τη χρηματοοικονομική οντότητα να χρησιμοποιεί τις ακόλουθες μεθόδους, με την επιφύλαξη της τελικής ευθύνης της χρηματοοικονομικής οντότητας:

α) δικό της εσωτερικό έλεγχο ή έλεγχο από διορισμένο τρίτο·

β) κατά περίπτωση, ομαδικούς ελέγχους και ομαδικές δοκιμές ΤΠΕ, συμπεριλαμβανομένων δοκιμών διείσδυσης βάσει απειλών, που διοργανώνονται από κοινού με άλλες αναθέτουσες χρηματοοικονομικές οντότητες ή εταιρείες που χρησιμοποιούν υπηρεσίες ΤΠΕ του ίδιου τρίτου παρόχου υπηρεσιών ΤΠΕ και εκτελούνται από τις εν λόγω αναθέτουσες χρηματοοικονομικές οντότητες ή εταιρείες ή από τρίτο που διορίζεται από αυτές·

γ) κατά περίπτωση, πιστοποιήσεις τρίτων·

δ) κατά περίπτωση, εκθέσεις εσωτερικού ελέγχου ή εκθέσεις ελέγχου από τρίτους που διατίθενται από τον τρίτο πάροχο υπηρεσιών ΤΠΕ.

3. Η χρηματοοικονομική οντότητα διαχρονικά δεν βασίζεται αποκλειστικά στις πιστοποιήσεις που αναφέρονται στην παράγραφο 2 στοιχείο γ) ή στις εκθέσεις ελέγχου που αναφέρονται στο στοιχείο δ) της εν λόγω παραγράφου. Η πολιτική επιτρέπει τη χρήση των μεθόδων που αναφέρονται στην παράγραφο 2 στοιχεία γ) και δ) μόνο όταν η χρηματοοικονομική οντότητα:

α) είναι ικανοποιημένη με το σχέδιο ελέγχου του τρίτου παρόχου υπηρεσιών ΤΠΕ για τις σχετικές συμβατικές ρυθμίσεις·

β) διασφαλίζει ότι το πεδίο εφαρμογής των πιστοποιήσεων ή των εκθέσεων ελέγχου καλύπτει τα συστήματα και τους βασικούς ελέγχους που προσδιορίζει η ίδια, και διασφαλίζει τη συμμόρφωση με τις σχετικές κανονιστικές απαιτήσεις·

γ) αξιολογεί διεξοδικά το περιεχόμενο των πιστοποιήσεων ή των εκθέσεων ελέγχου σε συνεχή βάση και επαληθεύει ότι οι εκθέσεις ή οι πιστοποιήσεις δεν είναι παρωχημένες·

δ) διασφαλίζει ότι τα βασικά συστήματα και οι έλεγχοι καλύπτονται σε μελλοντικές εκδόσεις της πιστοποίησης ή της έκθεσης ελέγχου·

ε) είναι ικανοποιημένη με την ικανότητα του μέρους που εκδίδει την πιστοποίηση ή διενεργεί τον έλεγχο·

στ) είναι ικανοποιημένη με το γεγονός ότι οι πιστοποιήσεις εκδίδονται και οι έλεγχοι διενεργούνται με βάση ευρέως αναγνωρισμένα σχετικά επαγγελματικά πρότυπα και περιλαμβάνουν δοκιμή της επιχειρησιακής αποτελεσματικότητας των βασικών ελέγχων που εφαρμόζονται·

ζ) έχει το συμβατικό δικαίωμα να ζητεί, με συχνότητα που είναι εύλογη και δικαιολογημένη από την άποψη της διαχείρισης κινδύνων, τροποποιήσεις του πεδίου εφαρμογής των πιστοποιήσεων ή των εκθέσεων ελέγχου σε άλλα σχετικά συστήματα και ελέγχους·

η) έχει το συμβατικό δικαίωμα να διενεργεί μεμονωμένους και ομαδικούς ελέγχους κατά τη διακριτική της ευχέρεια όσον αφορά τις συμβατικές ρυθμίσεις και να ασκεί τα εν λόγω δικαιώματα σύμφωνα με τη συμφωνηθείσα συχνότητα.

4. Η πολιτική διασφαλίζει ότι οι σημαντικές αλλαγές στη συμβατική συμφωνία πρέπει να επισημοποιούνται σε έγγραφο το οποίο φέρει ημερομηνία και υπογραφή όλων των μερών και προσδιορίζει τη διαδικασία ανανέωσης των συμβατικών ρυθμίσεων.

Άρθρο 9

Παρακολούθηση των συμβατικών ρυθμίσεων

1. Η πολιτική απαιτεί οι συμβατικές ρυθμίσεις να προσδιορίζουν τα μέτρα και τους βασικούς δείκτες για την παρακολούθηση, σε συνεχή βάση, των επιδόσεων τρίτων παρόχων υπηρεσιών ΤΠΕ, συμπεριλαμβανομένων μέτρων για την παρακολούθηση της συμμόρφωσης με τις απαιτήσεις όσον αφορά την εμπιστευτικότητα, τη διαθεσιμότητα, την ακεραιότητα και τη γνησιότητα των δεδομένων και των πληροφοριών, καθώς και της συμμόρφωσης των τρίτων παρόχων υπηρεσιών ΤΠΕ με τις σχετικές πολιτικές και διαδικασίες της χρηματοοικονομικής οντότητας. Η πολιτική προσδιορίζει επίσης μέτρα που εφαρμόζονται όταν δεν πληρούνται οι συμφωνίες για το επίπεδο των υπηρεσιών, συμπεριλαμβανομένων των συμβατικών κυρώσεων, κατά περίπτωση.

2. Η πολιτική προσδιορίζει τον τρόπο με τον οποίο η χρηματοοικονομική οντότητα πρέπει να αξιολογεί αν οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ που χρησιμοποιούνται για τις υπηρεσίες ΤΠΕ οι οποίες υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες πληρούν κατάλληλα πρότυπα επιδόσεων και ποιότητας σύμφωνα με τη συμβατική ρύθμιση και τις πολιτικές της ίδιας της χρηματοοικονομικής οντότητας. Ειδικότερα, η πολιτική διασφαλίζει τα ακόλουθα:

α) ότι οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ παρέχουν στη χρηματοοικονομική οντότητα, κατάλληλες εκθέσεις σχετικά με τις δραστηριότητες και τις υπηρεσίες τους συμπεριλαμβανομένων περιοδικών εκθέσεων, αναφορών συμβάντων, εκθέσεων παροχής υπηρεσιών, εκθέσεων σχετικά με την ασφάλεια ΤΠΕ και εκθέσεων σχετικά με τα μέτρα επιχειρησιακής συνέχειας και τις δοκιμές·

β) ότι οι επιδόσεις των τρίτων παρόχων υπηρεσιών ΤΠΕ αξιολογούνται με βασικούς δείκτες επιδόσεων, βασικούς δείκτες ελέγχου, λογιστικούς ελέγχους, αυτοπιστοποιήσεις και ανεξάρτητες αξιολογήσεις σύμφωνα με το πλαίσιο διαχείρισης κινδύνων ΤΠΕ της χρηματοοικονομικής οντότητας·

γ) ότι η χρηματοοικονομική οντότητα λαμβάνει άλλες σχετικές πληροφορίες από τους τρίτους παρόχους υπηρεσιών ΤΠΕ·

δ) ότι η χρηματοοικονομική οντότητα ενημερώνεται, κατά περίπτωση, για συμβάντα που σχετίζονται με τις ΤΠΕ και λειτουργικά συμβάντα ή συμβάντα ασφάλειας που σχετίζονται με πληρωμές·

ε) ότι διενεργούνται ανεξάρτητη αξιολόγηση και έλεγχοι για την επαλήθευση της συμμόρφωσης με τις νομικές και κανονιστικές απαιτήσεις και πολιτικές.

3. Η πολιτική διευκρινίζει ότι η αξιολόγηση που αναφέρεται στην παράγραφο 2 πρέπει να τεκμηριώνεται και τα αποτελέσματά της να χρησιμοποιούνται για την επικαιροποίηση της αξιολόγησης κινδύνων της χρηματοοικονομικής οντότητας που αναφέρεται στο άρθρο 6.

4. Η πολιτική καθορίζει τα κατάλληλα μέτρα που πρέπει να λάβει η χρηματοοικονομική οντότητα εάν εντοπίσει ελλείψεις των τρίτων παρόχων υπηρεσιών ΤΠΕ, συμπεριλαμβανομένων των συμβάντων που σχετίζονται με τις ΤΠΕ και των λειτουργικών συμβάντων ή των συμβάντων ασφάλειας που σχετίζονται με πληρωμές, στην παροχή των υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες ή στη συμμόρφωση με συμβατικές ρυθμίσεις ή νομικές απαιτήσεις. Προσδιορίζει επίσης τον τρόπο με τον οποίο πρέπει να παρακολουθείται η εφαρμογή των εν λόγω μέτρων, ώστε να διασφαλίζεται η αποτελεσματική συμμόρφωσή τους εντός καθορισμένου χρονοδιαγράμματος, λαμβάνοντας υπόψη τη σημαντικότητα των ελλείψεων.

Άρθρο 10

Έξοδος και καταγγελία των συμβατικών ρυθμίσεων

Η πολιτική περιλαμβάνει απαιτήσεις για τεκμηριωμένο σχέδιο εξόδου για κάθε συμβατική ρύθμιση και για την περιοδική επανεξέταση και δοκιμή του τεκμηριωμένου σχεδίου εξόδου. Κατά την κατάρτιση του σχεδίου εξόδου, λαμβάνονται υπόψη τα ακόλουθα:

α) απρόβλεπτες και επίμονες διακοπές παροχής της υπηρεσίας·

β) ακατάλληλη παροχή υπηρεσιών ή αδυναμία παροχής τους·

γ) η μη αναμενόμενη καταγγελία της συμβατικής ρύθμισης.

Το σχέδιο εξόδου είναι ρεαλιστικό, εφικτό, βασίζεται σε ευλογοφανή σενάρια και εύλογες παραδοχές και προβλέπει προγραμματισμένο χρονοδιάγραμμα υλοποίησης το οποίο συνάδει με τους όρους εξόδου και καταγγελίας που καθορίζονται στις συμβατικές ρυθμίσεις.

Άρθρο 11

Έναρξη ισχύος

Ο παρών κανονισμός αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

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

Βρυξέλλες, 13 Μαρτίου 2024.

Για την Επιτροπή
Η Πρόεδρος
Ursula VON DER LEYEN