EIOPA-BoS-20-002

Κατευθυντήριες γραμμές σχετικά με την εξωτερική ανάθεση δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους

Πίνακας περιεχομένων

Εισαγωγή

1. Σύμφωνα με το άρθρο 16 του κανονισμού (ΕΕ) αριθ. 1094/2010[1], η Ευρωπαϊκή Αρχή Ασφαλίσεων και Επαγγελματικών Συντάξεων (EIOPA) εκδίδει κατευθυντήριες γραμμές προκειμένου να παρέχει καθοδήγηση σε ασφαλιστικές και αντασφαλιστικές επιχειρήσεις όσον αφορά τον τρόπο με τον οποίο πρέπει να εφαρμόζονται οι διατάξεις περί εξωτερικής ανάθεσης που προβλέπονται στην οδηγία 2009/138/ΕΚ[2] («οδηγία Φερεγγυότητα ΙΙ») και στον κατ' εξουσιοδότηση κανονισμό (ΕΕ) 2015/35[3] («κατ' εξουσιοδότηση κανονισμός) σε περίπτωση εξωτερικής ανάθεσης δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους.

2. Οι παρούσες κατευθυντήριες γραμμές βασίζονται στο άρθρο 13 παράγραφος 28 και στα άρθρα 38 και 49 της οδηγίας Φερεγγυότητα ΙΙ, καθώς και στο άρθρο 274 του κατ' εξουσιοδότηση κανονισμού. Επιπλέον, οι συγκεκριμένες κατευθυντήριες γραμμές στηρίζονται επίσης στις οδηγίες των κατευθυντήριων γραμμών της EIOPA σχετικά με το σύστημα διακυβέρνησης (EIOPA-BoS-14/253).

3. Οι παρούσες κατευθυντήριες γραμμές απευθύνονται στις αρμόδιες αρχές, με στόχο να παράσχουν καθοδήγηση σχετικά τον τρόπο με τον οποίο οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις [αποκαλούμενες από κοινού «επιχείρηση(-εις)»] θα πρέπει να εφαρμόζουν τις προβλεπόμενες στις προαναφερθείσες νομικές πράξεις απαιτήσεις εξωτερικής ανάθεσης, στο πλαίσιο της εξωτερικής ανάθεσης δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους.

4. Οι κατευθυντήριες γραμμές εφαρμόζονται σε μεμονωμένες επιχειρήσεις και, κατ' αναλογίαν, σε ομίλους[4].

   Οι οντότητες που ανήκουν σε έναν όμιλο και υπόκεινται σε άλλες τομεακές απαιτήσεις εξαιρούνται από το πεδίο εφαρμογής των συγκεκριμένων κατευθυντήριων γραμμών σε μεμονωμένη βάση, δεδομένου ότι οφείλουν να τηρούν τις ειδικές τομεακές απαιτήσεις, καθώς και τη σχετική καθοδήγηση που εκδίδει η Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών και η Ευρωπαϊκή Αρχή Τραπεζών.

5. Σε περίπτωση ενδοομιλικής εξωτερικής ανάθεσης και υπεργολαβικής ανάθεσης σε παρόχους υπηρεσιών υπολογιστικού νέφους, οι παρούσες κατευθυντήριες γραμμές θα πρέπει να εφαρμόζονται σε συνδυασμό με τις διατάξεις των κατευθυντήριων γραμμών της EIOPA σχετικά με το σύστημα διακυβέρνησης για την ενδοομιλική εξωτερική ανάθεση.

6. Στο πλαίσιο της συμμόρφωσης ή της εποπτείας της συμμόρφωσης με τις παρούσες κατευθυντήριες γραμμές, οι επιχειρήσεις και οι αρμόδιες αρχές θα πρέπει να λαμβάνουν υπόψη την αρχή της αναλογικότητας[5] και τον κρίσιμο ή σημαντικό χαρακτήρα της υπηρεσίας που αποτελεί αντικείμενο εξωτερικής ανάθεσης σε παρόχους υπηρεσιών υπολογιστικού νέφους. Η αρχή της αναλογικότητας θα πρέπει να διασφαλίζει ότι οι ρυθμίσεις διακυβέρνησης, συμπεριλαμβανομένων εκείνων που αφορούν την εξωτερική ανάθεση δραστηριοτήτων σε παρόχους υπηρεσιών

[1] 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).

[2] Οδηγία 2009/138/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2019, σχετικά με την ανάληψη και την άσκηση δραστηριοτήτων ασφάλισης και αντασφάλισης (Φερεγγυότητα ΙΙ) (ΕΕ L 335 της 17.12.2009, σ. 1).

[3] Κατ' εξουσιοδότηση κανονισμός (ΕΕ) 2015/35 της Επιτροπής, της 10ης Οκτωβρίου 2014, για τη συμπλήρωση της οδηγίας 2009/138/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ανάληψη και την άσκηση δραστηριοτήτων ασφάλισης και αντασφάλισης (Φερεγγυότητα ΙΙ) (ΕΕ L 12 της 17.1.2015, σ. 1).

[4] Άρθρο 212 παράγραφος 1 της οδηγίας Φερεγγυότητα ΙΙ.

[5] Άρθρο 29 παράγραφος 3 της οδηγίας Φερεγγυότητα ΙΙ.

υπολογιστικού νέφους, εφαρμόζονται κατά τρόπο ανάλογο προς τη φύση, την κλίμακα και την πολυπλοκότητα των υποκείμενων κινδύνων.

7. Οι παρούσες κατευθυντήριες γραμμές θα πρέπει να ερμηνεύονται σε συνδυασμό και με την επιφύλαξη των κατευθυντήριων γραμμών της ΕΙΟΡΑ σχετικά με το σύστημα διακυβέρνησης και των κανονιστικών υποχρεώσεων που παρατίθενται στην παράγραφο 1.

Ορισμοί

8. Εάν δεν παρέχεται ορισμός στις παρούσες κατευθυντήριες γραμμές, οι όροι έχουν την έννοια που τους αποδίδεται στις νομικές πράξεις που αναφέρονται στην εισαγωγή.

9. Επιπλέον, για τους σκοπούς του παρόντος εγγράφου ισχύουν οι ακόλουθοι ορισμοί:

Πάροχος υπηρεσιών	τρίτη οντότητα που αναλαμβάνει μια διαδικασία, παρέχει μια υπηρεσία ή εκτελεί μια δραστηριότητα, ή μέρος της, στο πλαίσιο συμφωνίας εξωτερικής ανάθεσης.
Πάροχος υπηρεσιών υπολογιστικού νέφους	πάροχος υπηρεσιών, όπως ορίζεται ανωτέρω, υπεύθυνος για την παροχή υπηρεσιών υπολογιστικού νέφους στο πλαίσιο συμφωνίας εξωτερικής ανάθεσης.
Υπηρεσίες υπολογιστικού νέφους	υπηρεσίες που παρέχονται με τη χρήση υπολογιστικού νέφους, δηλαδή ενός μοντέλου για τη διευκόλυνση της από οπουδήποτε, εύκολης, κατ' αίτηση δικτυακής πρόσβασης σε κοινή ομάδα διαμορφώσιμων υπολογιστικών πόρων (π.χ. δικτύων, διακομιστών, αποθηκευτικών χώρων, εφαρμογών και υπηρεσιών) που μπορούν να παρασχεθούν και να διατεθούν ταχέως, με ελάχιστη διαχειριστική προσπάθεια ή αλληλεπίδραση με τον πάροχο υπηρεσίας.
Δημόσιο υπολογιστικό νέφος	υποδομή υπολογιστικού νέφους η οποία είναι διαθέσιμη για ανοικτή χρήση από το ευρύ κοινό.
Ιδιωτικό υπολογιστικό νέφος	υποδομή υπολογιστικού νέφους η οποία είναι διαθέσιμη για αποκλειστική χρήση από μία και μόνο επιχείρηση.
Κοινοτικό υπολογιστικό νέφος	υποδομή υπολογιστικού νέφους η οποία είναι διαθέσιμη για αποκλειστική χρήση από συγκεκριμένη κοινότητα επιχειρήσεων, όπως, για παράδειγμα, διάφορες επιχειρήσεις ενός και μόνο ομίλου.
Υβριδικό υπολογιστικό νέφος	υποδομή υπολογιστικού νέφους η οποία περιλαμβάνει δύο ή περισσότερες διακριτές υποδομές υπολογιστικού νέφους.

Ημερομηνία εφαρμογής

10. Οι παρούσες κατευθυντήριες γραμμές εφαρμόζονται από την 1η Ιανουαρίου 2021 σε όλες τις συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους που συνάπτονται ή τροποποιούνται από την εν λόγω ημερομηνία και εξής.

11. Οι επιχειρήσεις θα πρέπει να επανεξετάσουν και να τροποποιήσουν αναλόγως τις υφιστάμενες συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους που σχετίζονται με κρίσιμες ή σημαντικές επιχειρησιακές λειτουργίες ή

δραστηριότητες, ώστε να διασφαλίσουν τη συμμόρφωση με τις παρούσες κατευθυντήριες γραμμές έως τις 31 Δεκεμβρίου 2022.

12. Εάν η επανεξέταση των συμφωνιών εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους που σχετίζονται με κρίσιμες ή σημαντικές επιχειρησιακές λειτουργίες ή δραστηριότητες δεν οριστικοποιηθεί έως τις 31 Δεκεμβρίου 2022, η επιχείρηση θα πρέπει να ενημερώσει την εποπτική της αρχή[6] σχετικά με το γεγονός αυτό και τα μέτρα που έχει προγραμματίσει για να ολοκληρώσει την επανεξέταση ή την πιθανή στρατηγική εξόδου. Η εποπτική αρχή δύναται, κατά περίπτωση, να συμφωνήσει με την επιχείρηση στην επέκταση της προθεσμίας για την ολοκλήρωση της εν λόγω επανεξέτασης.

13. Η επικαιροποίηση (εφόσον απαιτείται) των πολιτικών και των εσωτερικών διαδικασιών της επιχείρησης θα πρέπει να πραγματοποιηθεί έως την 1η Ιανουαρίου 2021, ενώ οι απαιτήσεις τεκμηρίωσης για συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους που σχετίζονται με κρίσιμες ή σημαντικές επιχειρησιακές λειτουργίες ή δραστηριότητες θα πρέπει να εφαρμοστούν έως τις 31 Δεκεμβρίου 2022.

[6] Άρθρο 13 παράγραφος 10 της οδηγίας Φερεγγυότητα ΙΙ.

Κατευθυντήρια γραμμή 1 – Υπηρεσίες υπολογιστικού νέφους και εξωτερική ανάθεση

14. Η επιχείρηση θα πρέπει να διαπιστώσει αν μια συμφωνία με έναν πάροχο υπηρεσιών υπολογιστικού νέφους εμπίπτει στον ορισμό της εξωτερικής ανάθεσης δυνάμει της οδηγίας Φερεγγυότητα ΙΙ. Στο πλαίσιο της αξιολόγησης, θα πρέπει να εξετάζεται:

a. αν η επιχειρησιακή λειτουργία ή δραστηριότητα (ή μέρος της) που αποτελεί αντικείμενο εξωτερικής ανάθεσης εκτελείται σε επαναλαμβανόμενη ή διαρκή βάση· και

b. αν η εν λόγω επιχειρησιακή λειτουργία ή δραστηριότητα (ή μέρος της) θα ενέπιπτε κανονικά στο πεδίο εφαρμογής των επιχειρησιακών λειτουργιών ή δραστηριοτήτων που εκτελούνται ή θα μπορούσαν να εκτελούνται από την επιχείρηση στο πλαίσιο των συνήθων επιχειρηματικών της δραστηριοτήτων, ακόμη και αν η επιχείρηση δεν έχει εκτελέσει τη συγκεκριμένη επιχειρησιακή λειτουργία ή δραστηριότητα στο παρελθόν.

15. Όταν μια συμφωνία με έναν πάροχο υπηρεσιών καλύπτει πολλαπλές επιχειρησιακές λειτουργίες ή δραστηριότητες, η επιχείρηση θα πρέπει να εξετάζει όλες τις πτυχές της συμφωνίας στο πλαίσιο της αξιολόγησής της.

16. Σε περιπτώσεις στις οποίες η επιχείρηση προβαίνει σε εξωτερική ανάθεση επιχειρησιακών λειτουργιών ή δραστηριοτήτων σε παρόχους υπηρεσιών οι οποίοι δεν παρέχουν υπηρεσίες υπολογιστικού νέφους αλλά εξαρτώνται σε σημαντικό βαθμό από υποδομές υπολογιστικού νέφους για την προσφορά των υπηρεσιών τους (για παράδειγμα, όταν ο πάροχος υπηρεσιών υπολογιστικού νέφους αποτελεί μέρος μιας υπεργολαβικής αλυσίδας), η συμφωνία για τέτοιου είδους εξωτερική ανάθεση εμπίπτει στο πεδίο εφαρμογής του παρόντος εγγράφου.

Κατευθυντήρια γραμμή 2 – Γενικές αρχές διακυβέρνησης σχετικά με την εξωτερική ανάθεση δραστηριοτήτων υπολογιστικού νέφους

17. Με την επιφύλαξη του άρθρου 274 παράγραφος 3 του κατ' εξουσιοδότηση κανονισμού, το διοικητικό, διαχειριστικό ή εποπτικό όργανο της επιχείρησης θα πρέπει να διασφαλίζει ότι κάθε απόφαση για εξωτερική ανάθεση κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους βασίζεται σε εμπεριστατωμένη αξιολόγηση κινδύνων, μεταξύ των οποίων οι σχετικοί κίνδυνοι που συνεπάγεται η συμφωνία, όπως ο κίνδυνος τεχνολογίας πληροφοριών και επικοινωνιών («ΤΠΕ»), ο κίνδυνος για την επιχειρησιακή συνέχεια, ο νομικός κίνδυνος και ο κίνδυνος συμμόρφωσης, ο κίνδυνος συγκέντρωσης, άλλοι λειτουργικοί κίνδυνοι, καθώς και κίνδυνοι που σχετίζονται με τη μετάπτωση δεδομένων και/ή το στάδιο υλοποίησης, κατά περίπτωση.

18. Στην περίπτωση εξωτερικής ανάθεσης κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους, η επιχείρηση θα πρέπει, εφόσον απαιτείται, να αποτυπώνει τις αλλαγές που επέρχονται στο προφίλ κινδύνου της και οφείλονται στις συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους, στο πλαίσιο της αξιολόγησης κινδύνου και φερεγγυότητας που διενεργεί.

19. Η χρήση υπηρεσιών υπολογιστικού νέφους θα πρέπει να συνάδει με τις στρατηγικές της επιχείρησης (για παράδειγμα, με τη στρατηγική ΤΠΕ, τη στρατηγική ασφάλειας των πληροφοριών, τη στρατηγική διαχείρισης επιχειρησιακών κινδύνων), καθώς και με τις εσωτερικές πολιτικές και διαδικασίες, οι οποίες θα πρέπει να επικαιροποιούνται, εφόσον απαιτείται.

Κατευθυντήρια γραμμή 3 – Επικαιροποίηση της γραπτής πολιτικής εξωτερικής ανάθεσης

20. Στην περίπτωση εξωτερικής ανάθεσης σε παρόχους υπηρεσιών υπολογιστικού νέφους, η επιχείρηση θα πρέπει να επικαιροποιεί τη γραπτή πολιτική εξωτερικής ανάθεσης (για παράδειγμα, μέσω της επανεξέτασής της, της προσθήκης ξεχωριστού προσαρτήματος ή της ανάπτυξης νέων ειδικών πολιτικών), καθώς και τις άλλες εσωτερικές πολιτικές (για παράδειγμα, την ασφάλεια των πληροφοριών), λαμβάνοντας υπόψη τις ιδιαιτερότητες της εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους, τουλάχιστον όσον αφορά τα ακόλουθα πεδία:

a. τους ρόλους και τις αρμοδιότητες των σχετικών τμημάτων της επιχείρησης, ιδίως του διοικητικού, διαχειριστικού ή εποπτικού οργάνου, και των τμημάτων που είναι επιφορτισμένα με την ΤΠΕ, την ασφάλεια των πληροφοριών, τη συμμόρφωση, τη διαχείριση κινδύνων και τον εσωτερικό έλεγχο·

b. τις διεργασίες και τις διαδικασίες υποβολής εκθέσεων που απαιτούνται για την έγκριση, την εφαρμογή, την παρακολούθηση, τη διαχείριση και την ανανέωση, κατά περίπτωση, των συμφωνιών εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους που σχετίζονται με κρίσιμες ή σημαντικές επιχειρησιακές λειτουργίες ή δραστηριότητες·

c. την εποπτεία των υπηρεσιών υπολογιστικού νέφους κατά τρόπο αναλογικό προς τη φύση, το μέγεθος και την πολυπλοκότητα των κινδύνων που είναι εγγενείς στις παρεχόμενες υπηρεσίες, η οποία περιλαμβάνει i) αξιολόγηση κινδύνων των συμφωνιών εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους και έλεγχο δέουσας επιμέλειας των παρόχων υπηρεσιών υπολογιστικού νέφους, συμπεριλαμβανομένης της συχνότητας διενέργειας της αξιολόγησης κινδύνων· ii) ελέγχους παρακολούθησης και διαχείρισης (για παράδειγμα, έλεγχος της συμφωνίας επιπέδου υπηρεσιών)· iii) πρότυπα και ελέγχους ασφάλειας·

d. αναφορικά με την εξωτερική ανάθεση κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους, θα πρέπει να γίνει παραπομπή στις συμβατικές απαιτήσεις που περιγράφονται στην κατευθυντήρια γραμμή 10·

e. τις απαιτήσεις τεκμηρίωσης και τη γραπτή κοινοποίηση προς την εποπτική αρχή σχετικά με την εξωτερική ανάθεση κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους·

f. στο πλαίσιο κάθε συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους που αφορούν κρίσιμες ή σημαντικές επιχειρησιακές λειτουργίες ή δραστηριότητες, την απαίτηση για τεκμηριωμένη και, κατά περίπτωση, επαρκώς δοκιμασμένη «στρατηγική εξόδου», κατά τρόπο αναλογικό προς τη φύση, το μέγεθος και την πολυπλοκότητα των κινδύνων που είναι εγγενείς στις παρεχόμενες υπηρεσίες. Η στρατηγική εξόδου ενδέχεται να συνεπάγεται ένα φάσμα διαδικασιών καταγγελίας, οι οποίες περιλαμβάνουν, μεταξύ άλλων, τη διακοπή, την επανενσωμάτωση ή τη μεταφορά των υπηρεσιών που προβλέπονται στη συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους.

Κατευθυντήρια γραμμή 4 – Γραπτή κοινοποίηση προς την εποπτική αρχή

21. Οι απαιτήσεις γραπτής κοινοποίησης που ορίζονται στο άρθρο 49 παράγραφος 3 της οδηγίας Φερεγγυότητα ΙΙ και αναλύονται λεπτομερέστερα στις κατευθυντήριες γραμμές της EIOPA σχετικά με το σύστημα διακυβέρνησης είναι εφαρμοστέες σε όλες τις εξωτερικές αναθέσεις κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους. Η επιχείρηση θα

πρέπει να ενημερώνει την εποπτική αρχή σε περίπτωση που μια επιχειρησιακή λειτουργία ή δραστηριότητα που αποτελεί αντικείμενο εξωτερικής ανάθεσης και προηγουμένως είχε χαρακτηριστεί ως μη κρίσιμη ή μη σημαντική καθίσταται κρίσιμη ή σημαντική.

22. Η γραπτή κοινοποίηση της επιχείρησης θα πρέπει να περιλαμβάνει, λαμβανομένης υπόψη της αρχής της αναλογικότητας, τουλάχιστον τις ακόλουθες πληροφορίες:

a. συνοπτική περιγραφή της επιχειρησιακής λειτουργίας ή δραστηριότητας που αποτελεί αντικείμενο εξωτερικής ανάθεσης·

b. την ημερομηνία έναρξης και, κατά περίπτωση, την επόμενη ημερομηνία ανανέωσης της σύμβασης, την ημερομηνία λήξης και/ή τις περιόδους προειδοποίησης για τον πάροχο υπηρεσιών υπολογιστικού νέφους και για την επιχείρηση·

c. το εφαρμοστέο δίκαιο που διέπει τη σύμβαση εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους·

d. το όνομα του παρόχου υπηρεσιών υπολογιστικού νέφους, τον εταιρικό αριθμό μητρώου, τον αναγνωριστικό κωδικό νομικής οντότητας (εάν είναι διαθέσιμος), την έδρα και άλλα συναφή στοιχεία επικοινωνίας, καθώς και την επωνυμία της μητρικής εταιρείας (εάν υπάρχει)· στην περίπτωση ομίλων, εάν ο πάροχος υπηρεσιών υπολογιστικού νέφους ανήκει ή όχι στον όμιλο·

e. τα μοντέλα υπηρεσιών και εφαρμογής υπολογιστικού νέφους (δηλαδή δημόσιο/ιδιωτικό/υβριδικό/κοινοτικό) και τον ειδικό χαρακτήρα των δεδομένων που θα διατηρούνται, καθώς και τις τοποθεσίες (δηλαδή τις χώρες ή περιφέρειες) στις οποίες θα αποθηκεύονται τα εν λόγω δεδομένα·

f. συνοπτική παράθεση των λόγων για τους οποίους η επιχειρησιακή λειτουργία ή δραστηριότητα που αποτελεί αντικείμενο εξωτερικής ανάθεσης θεωρείται κρίσιμη ή σημαντική·

g. την ημερομηνία της τελευταίας αξιολόγησης του κρίσιμου ή σημαντικού χαρακτήρα της επιχειρησιακής λειτουργίας ή δραστηριότητας που αποτελεί αντικείμενο εξωτερικής ανάθεσης.

Κατευθυντήρια γραμμή 5 – Απαιτήσεις τεκμηρίωσης

23. Στο πλαίσιο του συστήματος διακυβέρνησης και διαχείρισης κινδύνων που εφαρμόζει, η επιχείρηση θα πρέπει να τηρεί μητρώο των συμφωνιών εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους που σύνηψε, με τη μορφή, για παράδειγμα, ενός ειδικού μητρώου το οποίο επικαιροποιεί σε βάθος χρόνου. Υπό την επιφύλαξη του εθνικού δικαίου, η επιχείρηση θα πρέπει επίσης να διατηρεί μητρώο με τις συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους που έχουν λήξει για επαρκές χρονικό διάστημα.

24. Σε περίπτωση εξωτερικής ανάθεσης κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων, η επιχείρηση θα πρέπει να καταχωρίζει όλες τις ακόλουθες πληροφορίες:

a. τις πληροφορίες που πρέπει να κοινοποιούνται στην εποπτική αρχή και αναφέρονται στην κατευθυντήρια γραμμή 4·

b. στην περίπτωση ομίλων, τις ασφαλιστικές ή αντασφαλιστικές επιχειρήσεις, καθώς και άλλες επιχειρήσεις εντός του πεδίου εφαρμογής της εποπτικής ενοποίησης οι οποίες χρησιμοποιούν υπηρεσίες υπολογιστικού νέφους·

c. την ημερομηνία της τελευταίας αξιολόγησης κινδύνων και συνοπτική παρουσίαση των κυριότερων αποτελεσμάτων·

d. το πρόσωπο ή το όργανο λήψης αποφάσεων (π.χ. το διοικητικό, διαχειριστικό ή εποπτικό όργανο) εντός της επιχείρησης που ενέκρινε τη συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους·

e. τις ημερομηνίες του τελευταίου και του επόμενου προγραμματισμένου ελέγχου, κατά περίπτωση·

f. τα ονόματα τυχόν υπεργολάβων στους οποίους ανατίθενται με υπεργολαβία ουσιώδη μέρη κρίσιμης ή σημαντικής επιχειρησιακής λειτουργίας ή δραστηριότητας, συμπεριλαμβανομένων των χωρών στις οποίες είναι καταχωρισμένοι οι υπεργολάβοι, στις οποίες θα παρέχεται η υπηρεσία και, κατά περίπτωση, τις τοποθεσίες (δηλαδή χώρες ή περιφέρειες) στις οποίες θα αποθηκεύονται τα δεδομένα·

g. το αποτέλεσμα της αξιολόγησης της δυνατότητας υποκατάστασης του παρόχου υπηρεσιών υπολογιστικού νέφους (π.χ., εύκολη, δύσκολη ή αδύνατη)·

h. αν η κρίσιμη ή σημαντική επιχειρησιακή λειτουργία ή δραστηριότητα που αποτελεί αντικείμενο εξωτερικής ανάθεσης υποστηρίζει επιχειρηματικές δραστηριότητες για τις οποίες ο παράγοντας του χρόνου είναι καίριας σημασίας·

i. το εκτιμώμενο ετήσιο κόστος για τον προϋπολογισμό·

j. κατά πόσον η επιχείρηση διαθέτει στρατηγική εξόδου σε περίπτωση μονομερούς καταγγελίας της σύμβασης ή διακοπής της παροχής υπηρεσιών από τον πάροχο υπηρεσιών υπολογιστικού νέφους·

25. Σε περίπτωση εξωτερικής ανάθεσης μη κρίσιμων ή μη σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων, η επιχείρηση θα πρέπει να προσδιορίζει τις πληροφορίες που πρέπει να καταχωριστούν, αναλόγως της φύσης, του μεγέθους και της πολυπλοκότητας των κινδύνων που είναι εγγενείς στις παρεχόμενες υπηρεσίες από τον πάροχο υπηρεσιών υπολογιστικού νέφους.

26. Η επιχείρηση θα πρέπει, κατόπιν αιτήματος, να θέτει στη διάθεση της εποπτικής αρχής όλες τις απαραίτητες πληροφορίες που καθιστούν εφικτή την άσκηση εποπτείας της επιχείρησης από την εποπτική αρχή, συμπεριλαμβανομένου ενός αντιγράφου της σύμβασης εξωτερικής ανάθεσης.

Κατευθυντήρια γραμμή 6 – Ανάλυση πριν από την εξωτερική ανάθεση δραστηριοτήτων

27. Πριν από τη σύναψη κάθε συμφωνίας με παρόχους υπηρεσιών υπολογιστικού νέφους, η επιχείρηση θα πρέπει:

a. να αξιολογεί αν η συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους αφορά κρίσιμη ή σημαντική επιχειρησιακή λειτουργία ή δραστηριότητα σύμφωνα με την κατευθυντήρια γραμμή 7·

b. να εντοπίζει και να αξιολογεί όλους τους συναφείς κινδύνους της συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους σύμφωνα με την κατευθυντήρια γραμμή 8·

c. να προβαίνει σε κατάλληλο έλεγχο δέουσας επιμέλειας ως προς τον πιθανό πάροχο υπηρεσιών υπολογιστικού νέφους σύμφωνα με την κατευθυντήρια γραμμή 9·

d. να προσδιορίζει και να αξιολογεί τις συγκρούσεις συμφερόντων που ενδέχεται να προκαλέσει η εξωτερική ανάθεση δραστηριοτήτων σύμφωνα με τις απαιτήσεις που ορίζονται στο άρθρο 274 παράγραφος 3 στοιχείο β) του κατ’ εξουσιοδότηση κανονισμού.

Κατευθυντήρια γραμμή 7 – Αξιολόγηση κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών και δραστηριοτήτων

28. Πριν από τη σύναψη κάθε συμφωνίας με παρόχους υπηρεσιών υπολογιστικού νέφους, η επιχείρηση θα πρέπει να αξιολογεί αν η συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους αφορά επιχειρησιακή λειτουργία ή δραστηριότητα που είναι κρίσιμη ή σημαντική. Κατά τη διενέργεια αυτής της αξιολόγησης, η επιχείρηση θα πρέπει, κατά περίπτωση, να εξετάζει κατά πόσο η συμφωνία ενδέχεται να καταστεί κρίσιμη ή σημαντική στο μέλλον. Σε περίπτωση ουσιώδους μεταβολής της φύσης, του μεγέθους και της πολυπλοκότητας των εγγενών κινδύνων της συμφωνίας, η επιχείρηση θα πρέπει επίσης να επαναξιολογήσει τον κρίσιμο ή σημαντικό χαρακτήρα της επιχειρησιακής λειτουργίας ή δραστηριότητας που ανατέθηκε προηγουμένως σε παρόχους υπηρεσιών υπολογιστικού νέφους.

29. Στο πλαίσιο της αξιολόγησης, η επιχείρηση θα πρέπει να λαμβάνει υπόψη, σε συνδυασμό με το αποτέλεσμα της αξιολόγησης των κινδύνων, τουλάχιστον τους ακόλουθους παράγοντες:

a. τις πιθανές επιπτώσεις που θα είχε οποιαδήποτε ουσιώδης διαταραχή της επιχειρησιακής λειτουργίας ή δραστηριότητας που αποτελεί αντικείμενο εξωτερικής ανάθεσης ή η συνεχής αδυναμία του παρόχου υπηρεσιών υπολογιστικού νέφους να παράσχει τις υπηρεσίες στην επιχείρηση στα συμφωνηθέντα επίπεδα υπηρεσιών:

   i. στη διαρκή συμμόρφωση προς τις κανονιστικές της υποχρεώσεις·

   ii. στη βραχυπρόθεσμη και μακροπρόθεσμη ανθεκτικότητα και βιωσιμότητα σε χρηματοοικονομικό επίπεδο και σε επίπεδο φερεγγυότητας·

   iii. στην επιχειρησιακή συνέχεια και στη λειτουργική της ανθεκτικότητα·

   iv. στον λειτουργικό κίνδυνο, συμπεριλαμβανομένου του κινδύνου συμπεριφοράς, του κινδύνου ΤΠΕ και του νομικού κινδύνου·

   v. στους κινδύνους φήμης.

b. τις πιθανές επιπτώσεις της συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους στην ικανότητα της επιχείρησης:

   i. να εντοπίζει, να παρακολουθεί και να διαχειρίζεται όλους τους συναφείς κινδύνους·

   ii. να συμμορφώνεται με όλες τις νομικές και κανονιστικές απαιτήσεις·

   iii. να διεξάγει κατάλληλους ελέγχους όσον αφορά την επιχειρησιακή λειτουργία ή δραστηριότητα που αποτελεί αντικείμενο εξωτερικής ανάθεσης·

c. στο συνολικό άνοιγμα της επιχείρησης (και/ή του ομίλου, κατά περίπτωση), στον ίδιο πάροχο υπηρεσιών υπολογιστικού νέφους και στις πιθανές σωρευτικές επιπτώσεις των συμφωνιών εξωτερικής ανάθεσης στον ίδιο επιχειρηματικό τομέα·

d. στο μέγεθος και την πολυπλοκότητα κάθε επιχειρηματικού τομέα της επιχείρησης που επηρεάζεται από τη συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους·

e. στη δυνατότητα, εάν αυτό είναι αναγκαίο ή επιθυμητό, μεταφοράς της προτεινόμενης συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους σε άλλον πάροχο υπηρεσιών υπολογιστικού νέφους ή επανενσωμάτωσης των υπηρεσιών («δυνατότητα υποκατάστασης»)·

f. στην προστασία προσωπικών και μη προσωπικών δεδομένων και στις πιθανές επιπτώσεις που θα είχε η παραβίαση της εμπιστευτικότητας ή η αδυναμία διασφάλισης της διαθεσιμότητας και της ακεραιότητας των δεδομένων στην επιχείρηση, τους αντισυμβαλλόμενους ή άλλους σχετικούς υπεύθυνους με βάση, μεταξύ άλλων, τον κανονισμό (ΕΕ) 2016/679[7]. Η επιχείρηση θα πρέπει ιδίως να λαμβάνει μέριμνα για δεδομένα που συνιστούν επιχειρηματικό απόρρητο και/ή είναι ευαίσθητα (για παράδειγμα, δεδομένα που αφορούν την υγεία των αντισυμβαλλόμενων).

Κατευθυντήρια γραμμή 8 – Αξιολόγηση των κινδύνων εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους

30. Κατά κανόνα, η επιχείρηση θα πρέπει να υιοθετεί μια προσέγγιση αναλογική προς τη φύση, το μέγεθος και την πολυπλοκότητα των κινδύνων που είναι εγγενείς στις υπηρεσίες οι οποίες αποτελούν αντικείμενο εξωτερικής ανάθεσης σε παρόχους υπηρεσιών υπολογιστικού νέφους. Αυτό περιλαμβάνει την αξιολόγηση των πιθανών επιπτώσεων οποιασδήποτε εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους, ιδίως όσον αφορά τον λειτουργικό κίνδυνο και τον κίνδυνο φήμης της.

31. Στην περίπτωση εξωτερικής ανάθεσης κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους, η επιχείρηση θα πρέπει:

a. να λαμβάνει υπόψη τα αναμενόμενα οφέλη και το κόστος της προτεινόμενης συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους, μεταξύ άλλων σταθμίζοντας τυχόν σημαντικούς κινδύνους που ενδέχεται να μειωθούν ή να τεθούν υπό καλύτερη διαχείριση σε σύγκριση με τυχόν σημαντικούς κινδύνους που είναι πιθανό να ανακύψουν λόγω της προτεινόμενης συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους·

b. να αξιολογεί, κατά περίπτωση και ενδεχομένως, τους κινδύνους, συμπεριλαμβανομένου του νομικού κινδύνου, του κινδύνου ΤΠΕ, του κινδύνου συμμόρφωσης και φήμης, καθώς και τους εποπτικούς περιορισμούς που προκύπτουν λόγω:

    i. της επιλεχθείσας υπηρεσίας υπολογιστικού νέφους και των προτεινόμενων μοντέλων εφαρμογής (δηλαδή δημόσιο/ιδιωτικό/υβριδικό/κοινοτικό)·

    ii. της μετανάστευσης και/ή της εφαρμογής·

    iii. των δραστηριοτήτων και των σχετικών δεδομένων και συστημάτων για τα οποία εξετάζεται το ενδεχόμενο εξωτερικής ανάθεσης (ή τα οποία αποτελούν ήδη αντικείμενο εξωτερικής ανάθεσης), όπως επίσης τον βαθμό ευαισθησίας τους και τα απαιτούμενα μέτρα ασφάλειας·

    iv. της κατάστασης, από άποψη πολιτικής σταθερότητας και ασφάλειας, που επικρατεί στις χώρες (εντός ή εκτός ΕΕ) στις οποίες παρέχονται ή ενδέχεται να παρέχονται οι υπηρεσίες που αποτελούν αντικείμενο εξωτερικής ανάθεσης και στις οποίες αποθηκεύονται ή είναι πιθανό να αποθηκεύονται τα δεδομένα. Στην αξιολόγηση θα πρέπει να λαμβάνονται υπόψη:

[7] 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).

1. οι ισχύοντες νόμοι, συμπεριλαμβανομένων των νόμων για την προστασία δεδομένων·
2. οι ισχύουσες διατάξεις επιβολής του νόμου·
3. οι διατάξεις της νομοθεσίας περί αφερεγγυότητας που θα εφαρμόζονταν σε περίπτωση πτώχευσης ενός παρόχου υπηρεσιών και τυχόν περιορισμοί που θα ανέκυπταν όσον αφορά την επείγουσα ανάκτηση των δεδομένων της επιχείρησης·

v. της υπεργολαβικής ανάθεσης, συμπεριλαμβανομένων των πρόσθετων κινδύνων που ενδέχεται να ανακύψουν αν ο υπεργολάβος είναι εγκατεστημένος σε τρίτη χώρα ή σε διαφορετική χώρα από τον πάροχο υπηρεσιών υπολογιστικού νέφους, καθώς και του κινδύνου οι μεγάλες και πολύπλοκες αλυσίδες υπεργολαβικής ανάθεσης να περιορίσουν τη δυνατότητα της επιχείρησης να επιβλέπει τις κρίσιμες ή σημαντικές επιχειρησιακές λειτουργίες ή δραστηριότητές της και τη δυνατότητα των εποπτικών αρχών να διασφαλίζουν την αποτελεσματική εποπτεία τους·

vi. του κινδύνου πλήρους συγκέντρωσης της επιχείρησης στον ίδιο πάροχο υπηρεσιών υπολογιστικού νέφους, συμπεριλαμβανομένης της εξωτερικής ανάθεσης δραστηριοτήτων σε πάροχο υπηρεσιών υπολογιστικού νέφους που δεν είναι εύκολο να υποκατασταθεί ή της σύναψης πολλαπλών συμφωνιών εξωτερικής ανάθεσης με τον ίδιο πάροχο υπηρεσιών υπολογιστικού νέφους. Κατά την αξιολόγηση των κινδύνων συγκέντρωσης, η επιχείρηση (και/ή ο όμιλος, κατά περίπτωση) θα πρέπει να λαμβάνει υπόψη όλες τις συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους που σύνηψε με τον εν λόγω πάροχο υπηρεσιών υπολογιστικού νέφους.

32. Η αξιολόγηση των κινδύνων θα πρέπει να διενεργείται πριν από τη σύναψη συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους. Εάν περιέλθει σε γνώση της επιχείρησης η ύπαρξη σοβαρών ελλείψεων και/ή σημαντικών μεταβολών στις παρεχόμενες υπηρεσίες ή στην κατάσταση του παρόχου υπηρεσιών υπολογιστικού νέφους, η αξιολόγηση των κινδύνων θα πρέπει άμεσα να επανεξετάζεται ή να διεξάγεται εκ νέου. Στην περίπτωση ανανέωσης μιας συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους όσον αφορά το περιεχόμενο και το πεδίο εφαρμογής της (για παράδειγμα, διεύρυνση του πεδίου εφαρμογής ή ένταξη στο πεδίο εφαρμογής κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών που προηγουμένως δεν περιλαμβάνονταν), η αξιολόγηση των κινδύνων θα πρέπει επίσης να διενεργείται εκ νέου.

Κατευθυντήρια γραμμή 9 – Έλεγχος δέουσας επιμέλειας του παρόχου υπηρεσιών υπολογιστικού νέφους

33. Η επιχείρηση θα πρέπει να διασφαλίζει την καταλληλότητα του παρόχου υπηρεσιών υπολογιστικού νέφους, στο πλαίσιο της σχετικής διαδικασίας επιλογής και αξιολόγησης, σύμφωνα με τα κριτήρια που προσδιορίζονται στην οικεία γραπτή πολιτική εξωτερικής ανάθεσης.

34. Ο έλεγχος δέουσας επιμέλειας του παρόχου υπηρεσιών υπολογιστικού νέφους θα πρέπει να διενεργείται πριν από την εξωτερική ανάθεση οποιασδήποτε επιχειρησιακής λειτουργίας ή δραστηριότητας. Στην περίπτωση που η επιχείρηση συνάπτει δεύτερη σύμβαση με έναν πάροχο υπηρεσιών υπολογιστικού νέφους ο οποίος έχει ήδη υποβληθεί σε αξιολόγηση, η επιχείρηση θα πρέπει να αποφασίζει, εφαρμόζοντας μια προσέγγιση βάσει κινδύνου, εάν απαιτείται η διενέργεια δεύτερου ελέγχου δέουσας

επιμέλειας. Εάν περιέλθει σε γνώση της επιχείρησης η ύπαρξη σοβαρών ελλείψεων και/ή σημαντικών μεταβολών στις παρεχόμενες υπηρεσίες ή στην κατάσταση του παρόχου υπηρεσιών υπολογιστικού νέφους, ο έλεγχος δέουσας επιμέλειας θα πρέπει άμεσα να επανεξετάζεται ή να διεξάγεται εκ νέου.

35. Στην περίπτωση εξωτερικής ανάθεσης κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών σε παρόχους υπηρεσιών υπολογιστικού νέφους, ο έλεγχος δέουσας επιμέλειας θα πρέπει να περιλαμβάνει αξιολόγηση της καταλληλότητας του παρόχου (για παράδειγμα, όσον αφορά δεξιότητες, υποδομή, οικονομική κατάσταση, εταιρικό και κανονιστικό καθεστώς). Εφόσον κρίνεται σκόπιμο, προκειμένου η επιχείρηση να στηρίξει τη διενέργεια του ελέγχου δέουσας επιμέλειας, μπορεί να χρησιμοποιεί αποδεικτικά στοιχεία, πιστοποιήσεις βάσει διεθνών προτύπων, εκθέσεις ελέγχου που εκπονήθηκαν από αναγνωρισμένα τρίτα μέρη ή εκθέσεις εσωτερικού ελέγχου.

Κατευθυντήρια γραμμή 10 – Συμβατικές απαιτήσεις

36. Τα αντίστοιχα δικαιώματα και οι αντίστοιχες υποχρεώσεις της επιχείρησης και του παρόχου υπηρεσιών υπολογιστικού νέφους θα πρέπει να επιμερίζονται σαφώς και να ορίζονται σε γραπτή σύμβαση.

37. Με την επιφύλαξη των απαιτήσεων που ορίζονται στο άρθρο 274 του κατ' εξουσιοδότηση κανονισμού, σε περίπτωση εξωτερικής ανάθεση κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων σε πάροχο υπηρεσιών υπολογιστικού νέφους, στη γραπτή σύμβαση μεταξύ της επιχείρησης και του παρόχου υπηρεσιών υπολογιστικού νέφους θα πρέπει να καθορίζονται τα ακόλουθα:

a. σαφής περιγραφή της προς εκτέλεση λειτουργίας που αποτελεί αντικείμενο εξωτερικής ανάθεσης (υπηρεσίες υπολογιστικού νέφους, συμπεριλαμβανομένων των υπηρεσιών υποστήριξης)·

b. η ημερομηνία έναρξης και η ημερομηνία λήξης, κατά περίπτωση, της σύμβασης και οι περίοδοι προειδοποίησης για τον πάροχο υπηρεσιών υπολογιστικού νέφους και για την επιχείρηση·

c. η δικαιοδοσία του δικαστηρίου και το εφαρμοστέο δίκαιο που διέπει τη σύμβαση·

d. οι οικονομικές υποχρεώσεις των συμβαλλόμενων μερών·

e. αν επιτρέπεται ή όχι η υπεργολαβική ανάθεση κρίσιμων ή σημαντικών λειτουργιών ή δραστηριοτήτων (ή ουσιωδών μερών τους) και, εάν ναι, οι προϋποθέσεις στις οποίες υπόκειται η σημαντική υπεργολαβική ανάθεση (βλ. κατευθυντήρια γραμμή 13)·

f. η τοποθεσία ή οι τοποθεσίες (δηλαδή οι περιφέρειες ή χώρες) όπου θα αποθηκεύονται και θα υποβάλλονται σε επεξεργασία τα σχετικά δεδομένα (τοποθεσία των κέντρων δεδομένων), και οι προϋποθέσεις που πρέπει να πληρούνται, μεταξύ των οποίων και η απαίτηση ειδοποίησης της επιχείρησης εάν ο πάροχος υπηρεσιών προτίθεται να αλλάξει τοποθεσία ή τοποθεσίες·

g. διατάξεις σχετικά με την προσβασιμότητα, τη διαθεσιμότητα, την ακεραιότητα, την εμπιστευτικότητα, την ιδιωτικότητα και την ασφάλεια των σχετικών δεδομένων, λαμβανομένων υπόψη των ορισθέντων στην κατευθυντήρια γραμμή 12·

h. το δικαίωμα της επιχείρησης να παρακολουθεί τις επιδόσεις του παρόχου υπηρεσιών υπολογιστικού νέφους σε τακτική βάση·

i. τα συμφωνηθέντα επίπεδα υπηρεσιών, τα οποία θα πρέπει να περιλαμβάνουν ακριβείς ποσοτικούς και ποιοτικούς δείκτες επιδόσεων προκειμένου να καθίσταται δυνατή η έγκαιρη παρακολούθηση, ούτως ώστε να μπορούν να

ληφθούν κατάλληλα διορθωτικά μέτρα χωρίς περιττή καθυστέρηση σε περίπτωση μη τήρησης των συμφωνηθέντων επιπέδων υπηρεσιών·

j. οι υποχρεώσεις υποβολής στοιχείων από τον πάροχο υπηρεσιών υπολογιστικού νέφους προς την επιχείρηση, συμπεριλαμβανομένων, κατά περίπτωση, των υποχρεώσεων υποβολής εκθέσεων που είναι σημαντικές για τη λειτουργία ασφάλειας και για βασικές λειτουργίες της επιχείρησης, όπως εκθέσεις σχετικά με τη λειτουργία εσωτερικού ελέγχου του παρόχου υπηρεσιών υπολογιστικού νέφους·

k. αν ο πάροχος υπηρεσιών υπολογιστικού νέφους θα πρέπει να διαθέτει υποχρεωτική ασφάλιση για ορισμένους κινδύνους και, κατά περίπτωση, το απαιτούμενο επίπεδο ασφαλιστικής κάλυψης·

l. οι απαιτήσεις για την εφαρμογή και τον δοκιμαστικό έλεγχο επιχειρησιακών σχεδίων έκτακτης ανάγκης·

m. η υποχρέωση του παρόχου υπηρεσιών να παραχωρεί στην επιχείρηση, τις εποπτικές της αρχές και σε κάθε άλλο πρόσωπο που διορίζεται από την επιχείρηση ή τις εποπτικές αρχές τα ακόλουθα:

   i. πλήρη πρόσβαση σε όλες τις σχετικές επιχειρησιακές εγκαταστάσεις (έδρα και κέντρα επιχειρήσεων), καθώς και σε ολόκληρο το φάσμα των σχετικών συσκευών, συστημάτων, δικτύων, πληροφοριών και δεδομένων που χρησιμοποιούνται για την εκτέλεση της λειτουργίας που αποτελεί αντικείμενο εξωτερικής ανάθεσης, συμπεριλαμβανομένων των σχετικών οικονομικών πληροφοριών, των μελών του προσωπικού και των εξωτερικών ελεγκτών του παρόχου υπηρεσιών υπολογιστικού νέφους («δικαιώματα πρόσβασης»)·

   ii. απεριόριστα δικαιώματα επιθεώρησης και ελέγχου σε σχέση με τη συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους («δικαιώματα ελέγχου»), προκειμένου να τους παρέχει τη δυνατότητα να παρακολουθούν τη συμφωνία εξωτερικής ανάθεσης και να διασφαλίζουν τη συμμόρφωση με όλες τις εφαρμοστέες κανονιστικές και συμβατικές απαιτήσεις·

n. διατάξεις ώστε να διασφαλίζεται η δυνατότητα άμεσης ανάκτησης από την επιχείρηση των δεδομένων που της ανήκουν σε περίπτωση αφερεγγυότητας, εξυγίανσης ή διακοπής των επιχειρηματικών δραστηριοτήτων του παρόχου υπηρεσιών υπολογιστικού νέφους.

Κατευθυντήρια γραμμή 11 – Δικαιώματα πρόσβασης και ελέγχου

38. Η σύμβαση εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους δεν θα πρέπει να περιορίζει την αποτελεσματική άσκηση των δικαιωμάτων πρόσβασης και ελέγχου εκ μέρους της επιχείρησης, καθώς και τις επιλογές ελέγχου των υπηρεσιών υπολογιστικού νέφους με στόχο την τήρηση των κανονιστικών της υποχρεώσεων.

39. Η επιχείρηση θα πρέπει να ασκεί τα οικεία δικαιώματα πρόσβασης και ελέγχου, να καθορίζει τη συχνότητα των ελέγχων και τους τομείς και τις υπηρεσίες προς έλεγχο, εφαρμόζοντας μια προσέγγιση βάσει κινδύνου, σύμφωνα με την ενότητα 8 των κατευθυντήριων γραμμών της EIOPA σχετικά με το σύστημα διακυβέρνησης.

40. Κατά τον καθορισμό της συχνότητας και του πεδίου εφαρμογής της άσκησης των δικαιωμάτων πρόσβασης και ελέγχου, η επιχείρηση θα πρέπει να λαμβάνει υπόψη αν η εξωτερική ανάθεση δραστηριοτήτων υπολογιστικού νέφους αφορά κρίσιμη ή σημαντική επιχειρησιακή λειτουργία ή δραστηριότητα, τη φύση και την έκταση των κινδύνων και τις επιπτώσεις στην επιχείρηση που προκύπτουν από τις συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους.

41. Σε περίπτωση που τα δικαιώματα πρόσβασης ή ελέγχου ή η χρήση ορισμένων τεχνικών ελέγχου συνεπάγονται κινδύνους για το περιβάλλον του παρόχου υπηρεσιών υπολογιστικού νέφους και/ή για άλλον πελάτη του παρόχου υπηρεσιών υπολογιστικού νέφους (για παράδειγμα, επιπτώσεις στα επίπεδα υπηρεσιών, διαθεσιμότητα των δεδομένων, παράμετροι εμπιστευτικότητας), η επιχείρηση και ο πάροχος υπηρεσιών υπολογιστικού νέφους θα πρέπει να συμφωνήσουν στη χρήση εναλλακτικών τρόπων παροχής ανάλογου επιπέδου διασφάλισης και υπηρεσιών στην επιχείρηση (για παράδειγμα, την ένταξη ειδικών ελέγχων που πρέπει να δοκιμάζονται στο πλαίσιο ειδικής έκθεσης/πιστοποίησης του παρόχου υπηρεσιών υπολογιστικού νέφους).

42. Με την επιφύλαξη της τελικής ευθύνης που υπέχουν όσον αφορά τις δραστηριότητες που εκτελούνται από τους παρόχους υπηρεσιών υπολογιστικού νέφους και με σκοπό την αποδοτικότερη χρήση των ελεγκτικών πόρων και τη μείωση του οργανωτικού φόρτου, τόσο για τον πάροχο υπηρεσιών υπολογιστικού νέφους όσο και για τους πελάτες του, οι επιχειρήσεις μπορούν να χρησιμοποιούν:

a. πιστοποιήσεις τρίτων και εκθέσεις ελέγχου τρίτων ή εκθέσεις εσωτερικού ελέγχου που καθίστανται διαθέσιμες από τον πάροχο υπηρεσιών υπολογιστικού νέφους·

b. ομαδοποιημένους ελέγχους που διενεργούνται από κοινού με άλλους πελάτες του ίδιου παρόχου υπηρεσιών υπολογιστικού νέφους ή από τρίτο τον οποίο ορίζουν οι ίδιες·

43. Στην περίπτωση εξωτερικής ανάθεσης κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους, οι επιχειρήσεις θα πρέπει να κάνουν χρήση της μεθόδου που αναφέρεται στην παράγραφο 42 στοιχείο α) μόνον εφόσον:

a. διασφαλίζουν ότι το πεδίο εφαρμογής της πιστοποίησης ή της έκθεσης ελέγχου καλύπτει τα συστήματα (για παράδειγμα, τις διαδικασίες, τις εφαρμογές, την υποδομή, τα κέντρα δεδομένων κ.λπ.) και τους ελέγχους που προσδιορίζονται από την επιχείρηση και αξιολογούν τη συμμόρφωση με τις αντίστοιχες κανονιστικές απαιτήσεις·

b. διενεργούν εμπεριστατωμένη αξιολόγηση του περιεχομένου των νέων πιστοποιήσεων ή εκθέσεων ελέγχου σε τακτική βάση και επαληθεύουν ότι οι πιστοποιήσεις ή οι εκθέσεις δεν είναι παρωχημένες·

c. διασφαλίζουν ότι τα βασικά συστήματα και οι βασικοί έλεγχοι θα εξακολουθούν να καλύπτονται στις μελλοντικές εκδόσεις της πιστοποίησης ή της έκθεσης ελέγχου·

d. είναι πεπεισμένες για τις ικανότητες του μέρους που πραγματοποιεί την πιστοποίηση ή τον έλεγχο (για παράδειγμα, όσον αφορά την εναλλαγή των εταιρειών πιστοποίησης ή ελέγχου, τα προσόντα, την εμπειρογνωσία, την επανεκτέλεση/επαλήθευση των αποδεικτικών στοιχείων στον υποκείμενο φάκελο ελέγχου)·

e. είναι πεπεισμένες ότι οι πιστοποιήσεις εκδίδονται και ότι οι έλεγχοι εκτελούνται σύμφωνα με τα κατάλληλα πρότυπα και περιλαμβάνουν δοκιμαστικό έλεγχο της επιχειρησιακής αποτελεσματικότητας των βασικών ελέγχων που εφαρμόζονται·

f. έχουν το συμβατικό δικαίωμα να ζητούν την επέκταση του πεδίου εφαρμογής των πιστοποιήσεων ή των εκθέσεων ελέγχου σε άλλα σχετικά συστήματα και ελέγχους· τα εν λόγω αιτήματα για την τροποποίηση του πεδίου εφαρμογής θα πρέπει να είναι εύλογα ως προς τον αριθμό και τη συχνότητα υποβολής τους, αλλά και θεμιτά από πλευράς διαχείρισης κινδύνων·

g. διατηρούν το συμβατικό δικαίωμα να διενεργούν επιμέρους επιτόπιους ελέγχους κατά τη διακριτική τους ευχέρεια όσον αφορά την εξωτερική ανάθεση κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους· το δικαίωμα αυτό θα πρέπει να ασκείται σε περίπτωση ειδικών αναγκών, όταν δεν είναι εφικτές άλλες μορφές αλληλεπίδρασης με τον πάροχο υπηρεσιών υπολογιστικού νέφους.

44. Για την εξωτερική ανάθεση κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών σε παρόχους υπηρεσιών υπολογιστικού νέφους, η επιχείρηση θα πρέπει να αξιολογεί αν οι πιστοποιήσεις τρίτων και οι εκθέσεις που αναφέρονται στο σημείο 42 στοιχείο α) είναι κατάλληλες και επαρκείς για τη διασφάλιση της συμμόρφωσής της με τις κανονιστικές υποχρεώσεις της, εφαρμόζοντας μιας προσέγγιση βάσει κινδύνου, και δεν θα πρέπει να βασίζεται αποκλειστικά και μόνο στις εν λόγω εκθέσεις και πιστοποιητικά σε βάθος χρόνου.

45. Πριν από κάθε προγραμματισμένη επιτόπια επίσκεψη, ο συμβαλλόμενος που ασκεί το σχετικό δικαίωμα πρόσβασης (επιχείρηση, ελεγκτής ή τρίτοι που ενεργούν εξ ονόματος της επιχείρησης ή των επιχειρήσεων) θα πρέπει να παρέχει προηγούμενη προειδοποίηση εντός εύλογου χρονικού διαστήματος, εκτός εάν αυτό δεν είναι εφικτό λόγω κατάστασης έκτακτης ανάγκης ή κρίσης. Η προειδοποίηση αυτή θα πρέπει να περιλαμβάνει την τοποθεσία και τον σκοπό της επίσκεψης, καθώς και το προσωπικό που θα συμμετάσχει στην επίσκεψη.

46. Λαμβανομένου υπόψη ότι οι λύσεις υπολογιστικού νέφους χαρακτηρίζονται από υψηλό επίπεδο τεχνικής πολυπλοκότητας, η επιχείρηση θα πρέπει να επαληθεύει ότι το προσωπικό που διενεργεί τον έλεγχο –είτε πρόκειται για τους εσωτερικούς ελεγκτές της είτε για την ομάδα ελεγκτών που ενεργούν εξ ονόματός της είτε για τους διορισμένους ελεγκτές του παρόχου υπηρεσιών υπολογιστικού νέφους– ή, κατά περίπτωση, το προσωπικό που επανεξετάζει την πιστοποίηση τρίτου ή τις εκθέσεις ελέγχου του παρόχου υπηρεσιών έχει αποκτήσει τις κατάλληλες δεξιότητες και γνώσεις για την εκτέλεση των σχετικών ελέγχων και/ή αξιολογήσεων.

Κατευθυντήρια γραμμή 12 – Ασφάλεια των δεδομένων και των συστημάτων

47. Η επιχείρηση θα πρέπει να διασφαλίζει ότι οι πάροχοι υπηρεσιών υπολογιστικού νέφους συμμορφώνονται με τους ευρωπαϊκούς και εθνικούς κανονισμούς, καθώς και με τα κατάλληλα πρότυπα ασφάλειας ΤΠΕ.

48. Σε περίπτωση εξωτερικής ανάθεσης κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους, η επιχείρηση θα πρέπει επιπλέον να καθορίζει ειδικές απαιτήσεις ασφάλειας των πληροφοριών στο πλαίσιο της σύμβασης εξωτερικής ανάθεσης και να παρακολουθεί τη συμμόρφωση με τις εν λόγω απαιτήσεις σε τακτική βάση.

49. Για τους σκοπούς της παραγράφου 48, σε περίπτωση εξωτερικής ανάθεσης κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους, η επιχείρηση, εφαρμόζοντας μια προσέγγιση βάσει κινδύνου και λαμβάνοντας υπόψη τις αρμοδιότητές της και τις αρμοδιότητες του παρόχου υπηρεσιών υπολογιστικού νέφους, θα πρέπει:

a. να συμφωνεί στην ύπαρξη σαφών ρόλων και αρμοδιοτήτων, ρητώς διακριτών, ανάμεσα στον πάροχο υπηρεσιών υπολογιστικού νέφους και την επιχείρηση όσον αφορά τις επιχειρησιακές λειτουργίες ή δραστηριότητες που επηρεάζονται από την εξωτερική ανάθεση δραστηριοτήτων υπολογιστικού νέφους·

b. να καθορίζει και να αποφασίζει κατάλληλο επίπεδο προστασίας των εμπιστευτικών δεδομένων, της συνέχειας των δραστηριοτήτων που αποτελούν

αντικείμενο εξωτερικής ανάθεσης, καθώς και της ακεραιότητας και της ιχνηλασιμότητας των δεδομένων και των συστημάτων στο πλαίσιο της σκοπούμενης εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους·

c. να εξετάζει το ενδεχόμενο λήψης ειδικών μέτρων, όπου αυτό κρίνεται αναγκαίο, για τα δεδομένα σε μεταφορά, τα δεδομένα σε μνήμη και τα δεδομένα σε αδράνεια, όπως, για παράδειγμα, η χρήση τεχνολογιών κρυπτογράφησης, σε συνδυασμό με κατάλληλη διαχείριση κλειδιών·

d. να εξετάζει τους μηχανισμούς ενσωμάτωσης των υπηρεσιών υπολογιστικού νέφους στα συστήματα της επιχείρησης, για παράδειγμα, τις διεπαφές προγραμματισμού εφαρμογών και τη χρηστή διαδικασία διαχείρισης χρηστών και πρόσβασης·

e. να κατοχυρώνει συμβατικά ότι η διαθεσιμότητα της κίνησης δικτύου και η αναμενόμενη δυναμικότητα πληρούν υψηλές απαιτήσεις συνέχειας, εφόσον είναι δυνατόν και εφικτό·

f. να καθορίζει και να αποφασίζει, κατά περίπτωση, δέουσες απαιτήσεις συνέχειας που διασφαλίζουν επαρκή επίπεδα σε κάθε βαθμίδα της τεχνολογικής αλυσίδας·

g. να εφαρμόζει χρηστή και πλήρως τεκμηριωμένη διαδικασία διαχείρισης συμβάντων που περιλαμβάνει τις αντίστοιχες αρμοδιότητες, για παράδειγμα, μέσω του καθορισμού ενός προτύπου συνεργασίας σε περίπτωση εκδήλωσης πραγματικών ή πιθανολογούμενων συμβάντων·

h. να υιοθετεί μια προσέγγιση βάσει κινδύνου για την τοποθεσία ή τις τοποθεσίες (δηλαδή τη χώρα ή την περιφέρεια) αποθήκευσης και επεξεργασίας των δεδομένων, καθώς και για παραμέτρους ασφάλειας των πληροφοριών·

i. να παρακολουθεί την εκπλήρωση των απαιτήσεων αποτελεσματικότητας και αποδοτικότητας των εφαρμοζόμενων ελεγκτικών μηχανισμών από τον πάροχο υπηρεσιών υπολογιστικού νέφους οι οποίοι θα μπορούσαν να αμβλύνουν τους κινδύνους που συνδέονται με τις παρεχόμενες υπηρεσίες.

Κατευθυντήρια γραμμή 13 – Υπεργολαβική ανάθεση κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων

50. Εάν επιτρέπεται η υπεργολαβική ανάθεση κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών (ή μέρους τους), στη σύμβαση εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους μεταξύ της επιχείρησης και του παρόχου υπηρεσιών υπολογιστικού νέφους θα πρέπει:

a. να προσδιορίζονται όλα τα είδη δραστηριοτήτων που εξαιρούνται από την πιθανή υπεργολαβική ανάθεση·

b. να καθορίζονται οι προϋποθέσεις που πρέπει να πληρούνται σε περίπτωση υπεργολαβικής ανάθεσης (για παράδειγμα, ότι ο υπεργολάβος θα συμμορφωθεί πλήρως προς τις σχετικές υποχρεώσεις του παρόχου υπηρεσιών υπολογιστικού νέφους). Οι εν λόγω υποχρεώσεις περιλαμβάνουν τα δικαιώματα ελέγχου και πρόσβασης και την ασφάλεια των δεδομένων και των συστημάτων·

c. να επισημαίνεται ότι ο πάροχος υπηρεσιών υπολογιστικού νέφους διατηρεί πλήρη ευθύνη και εποπτεία των υπηρεσιών που αποτελούν αντικείμενο υπεργολαβικής ανάθεσης·

d. να περιλαμβάνεται για τον πάροχο υπηρεσιών υπολογιστικού νέφους η υποχρέωση ενημέρωσης της επιχείρησης σχετικά με κάθε προγραμματιζόμενη σημαντική αλλαγή, όσον αφορά τους υπεργολάβους ή τις υπεργολαβικές υπηρεσίες, η οποία ενδέχεται να επηρεάσει την ικανότητα του παρόχου υπηρεσιών να τηρήσει τις υποχρεώσεις του δυνάμει της σύμβασης εξωτερικής

ανάθεσης δραστηριοτήτων υπολογιστικού νέφους. Η προθεσμία κοινοποίησης για τις εν λόγω αλλαγές θα πρέπει να παρέχει στην επιχείρηση τη δυνατότητα να διενεργεί, τουλάχιστον, αξιολόγηση των κινδύνων όσον αφορά τις επιπτώσεις των προτεινόμενων αλλαγών πριν τεθεί πράγματι σε ισχύ η αλλαγή όσον αφορά τους υπεργολάβους ή τις υπεργολαβικές υπηρεσίες·

e. να διασφαλίζεται ότι, σε περιπτώσεις που ο πάροχος υπηρεσιών υπολογιστικού νέφους προτίθεται να προβεί σε αλλαγές όσον αφορά τον υπεργολάβο ή τις υπεργολαβικές υπηρεσίες οι οποίες ενδέχεται να επιφέρουν δυσμενείς συνέπειες σε επίπεδο αξιολόγησης των κινδύνων των συμφωνημένων υπηρεσιών, η επιχείρηση έχει το δικαίωμα να προβάλει αντιρρήσεις έναντι αντίστοιχων αλλαγών και/ή το δικαίωμα να καταγγείλει και να λύσει τη σύμβαση.

Κατευθυντήρια γραμμή 14 – Παρακολούθηση και εποπτεία των συμφωνιών εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους

51. Η επιχείρηση θα πρέπει να παρακολουθεί, σε τακτική βάση, την εκτέλεση των δραστηριοτήτων, τα μέτρα ασφάλειας και την τήρηση του συμφωνηθέντος επιπέδου υπηρεσιών από τους παρόχους υπηρεσιών υπολογιστικού νέφους, εφαρμόζοντας μια προσέγγιση βάσει κινδύνου. Στο επίκεντρο θα πρέπει να βρίσκεται η εξωτερική ανάθεση κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών σε παρόχους υπηρεσιών υπολογιστικού νέφους.

52. Γι’ αυτόν τον λόγο, η επιχείρηση θα πρέπει να συστήνει μηχανισμούς παρακολούθησης και εποπτείας, οι οποίοι συνεκτιμούν, όπου κρίνεται εφικτό και σκόπιμο, την ύπαρξη υπεργολαβικής εξωτερικής ανάθεσης κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή μέρους τους.

53. Το διοικητικό, διαχειριστικό ή εποπτικό όργανο θα πρέπει να ενημερώνεται σε τακτά χρονικά διαστήματα σχετικά με τους κινδύνους που διαπιστώνονται όσον αφορά την εξωτερική ανάθεση κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους.

54. Προκειμένου να διασφαλίζεται η κατάλληλη παρακολούθηση και εποπτεία των συμφωνιών εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους που έχουν συνάψει, οι επιχειρήσεις θα πρέπει να απασχολούν επαρκές ανθρώπινο δυναμικό, με κατάλληλες δεξιότητες και γνώσεις για την παρακολούθηση των υπηρεσιών που αποτελούν αντικείμενο εξωτερικής ανάθεσης σε παρόχους υπηρεσιών υπολογιστικού νέφους. Το επιφορτισμένο με τις εν λόγω δραστηριότητες προσωπικό της επιχείρησης θα πρέπει να διαθέτει εξίσου τις γνώσεις ΤΠΕ και τις επιχειρηματικές γνώσεις που κρίνονται απαραίτητες.

Κατευθυντήρια γραμμή 15 – Δικαιώματα καταγγελίας και στρατηγικές εξόδου

55. Στην περίπτωση εξωτερικής ανάθεσης κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων σε πάροχο υπηρεσιών υπολογιστικού νέφους, η επιχείρηση θα πρέπει να ενσωματώνει μια σαφώς καθορισμένη ρήτρα στρατηγικής εξόδου στη σύμβαση εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους, η οποία διασφαλίζει τη δυνατότητά της να καταγγέλλει τη σύμβαση, εφόσον κρίνεται σκόπιμο. Η καταγγελία θα πρέπει να μπορεί να πραγματοποιείται χωρίς να αποβαίνει εις βάρος της συνέχειας και της ποιότητας των παρεχόμενων υπηρεσιών στους αντισυμβαλλόμενους. Για τον σκοπό αυτό, η επιχείρηση θα πρέπει:

a. να καταρτίζει σχέδια εξόδου τα οποία είναι ολοκληρωμένα, βασιζόμενα σε υπηρεσίες, τεκμηριωμένα και επαρκώς δοκιμασμένα (για παράδειγμα, μέσω της διενέργειας ανάλυσης του πιθανού κόστους, των επιπτώσεων, των πόρων και των χρονικών παραμέτρων των διαφόρων πιθανών επιλογών εξόδου)·

b. να προσδιορίζει εναλλακτικές λύσεις και να καταρτίζει κατάλληλα και εφικτά μεταβατικά σχέδια, που παρέχουν στην επιχείρηση τη δυνατότητα να αποσύρει και να μεταφέρει τις υφιστάμενες δραστηριότητες και τα δεδομένα από τον πάροχο υπηρεσιών υπολογιστικού νέφους σε εναλλακτικούς παρόχους υπηρεσιών ή να τα επαναφέρει στην επιχείρηση. Οι λύσεις αυτές θα πρέπει να προσδιορίζονται λαμβανομένων υπόψη των προκλήσεων που ενδέχεται να προκύψουν λόγω της τοποθεσίας στην οποία βρίσκονται τα δεδομένα και με τη λήψη των αναγκαίων μέτρων για τη διασφάλιση της επιχειρησιακής συνέχειας κατά τη διάρκεια της μεταβατικής φάσης·

c. να διασφαλίζει ότι ο πάροχος υπηρεσιών υπολογιστικού νέφους παρέχει επαρκή στήριξη στην επιχείρηση κατά τη μεταφορά των δεδομένων, των συστημάτων ή των εφαρμογών που αποτελούν αντικείμενο εξωτερικής ανάθεσης σε άλλον πάροχο υπηρεσιών ή απευθείας στην ίδια την επιχείρηση·

d. να συνάπτει συμφωνία με τον πάροχο υπηρεσιών υπολογιστικού νέφους, βάσει της οποίας, αφότου επαναμεταβιβαστούν στην επιχείρηση τα δεδομένα της, θα διαγραφούν πλήρως και με ασφάλεια σε όλες τις περιφέρειες από τον πάροχο υπηρεσιών υπολογιστικού νέφους.

56. Κατά την ανάπτυξη στρατηγικών εξόδου, η επιχείρηση θα πρέπει να λαμβάνει υπόψη τα εξής:

a. να καθορίζει στόχους της στρατηγικής εξόδου·

b. να προσδιορίζει τα γεγονότα ενεργοποίησης (για παράδειγμα, τους βασικούς δείκτες κινδύνου που δηλώνουν μη αποδεκτό επίπεδο υπηρεσίας), τα οποία θα μπορούσαν να θέσουν σε κίνηση τη στρατηγική εξόδου·

c. να διενεργεί ανάλυση επιχειρηματικών επιπτώσεων κατ' αναλογία προς τις δραστηριότητες που αποτελούν αντικείμενο εξωτερικής ανάθεσης για τον προσδιορισμό των ανθρώπινων και άλλων πόρων που θα απαιτούνταν για την εφαρμογή του σχεδίου εξόδου, καθώς και του εκτιμώμενου χρόνου εφαρμογής του·

d. να αναθέτει ρόλους και αρμοδιότητες στο πλαίσιο της διαχείρισης των σχεδίων εξόδου και των δραστηριοτήτων μετάβασης·

e. να καθορίζει τα κριτήρια επιτυχούς μετάβασης.

Κατευθυντήρια γραμμή 16 – Εποπτεία των συμφωνιών εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους από τις εποπτικές αρχές

57. Στο πλαίσιο της διαδικασίας εποπτικής εξέτασης, οι εποπτικές αρχές θα πρέπει να διενεργούν ανάλυση των επιπτώσεων που προκύπτουν από τις συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους της επιχείρησης. Η ανάλυση των επιπτώσεων θα πρέπει να εστιάζεται ιδίως στις συμφωνίες που αφορούν την εξωτερική ανάθεση κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων.

58. Κατά την εποπτεία των συμφωνιών εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους που συνάπτουν οι επιχειρήσεις, οι εποπτικές αρχές θα πρέπει να εξετάζουν τους ακόλουθους κινδύνους:

a. κίνδυνοι ΤΠΕ·

b. άλλοι λειτουργικοί κίνδυνοι (συμπεριλαμβανομένου του νομικού κινδύνου και του κινδύνου συμμόρφωσης, του κινδύνου εξωτερικής ανάθεσης και του κινδύνου διαχείρισης από τρίτους)·

c. κίνδυνος φήμης·

d. κίνδυνος συγκέντρωσης, μεταξύ άλλων σε επίπεδο χώρας / τομεακό επίπεδο.

59. Στο πλαίσιο της αξιολόγησής τους, οι εποπτικές αρχές θα πρέπει να συμπεριλαμβάνουν τις ακόλουθες παραμέτρους, εφαρμόζοντας μια προσέγγιση βάσει κινδύνου:

a. την καταλληλότητα και την αποτελεσματικότητα των διαδικασιών διακυβέρνησης και των επιχειρησιακών διαδικασιών της επιχείρησης όσον αφορά την έγκριση, την εφαρμογή, την παρακολούθηση, τη διαχείριση και την ανανέωση των συμφωνιών εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους·

b. κατά πόσο η επιχείρηση διαθέτει επαρκείς ανθρώπινους πόρους, με κατάλληλες δεξιότητες και γνώσεις για την παρακολούθηση των υπηρεσιών που αποτελούν αντικείμενο εξωτερικής ανάθεσης σε παρόχους υπηρεσιών υπολογιστικού νέφους·

c. κατά πόσο η επιχείρηση διαπιστώνει και διαχειρίζεται όλους τους κινδύνους που επισημαίνονται στις παρούσες κατευθυντήριες γραμμές.

60. Στην περίπτωση ομίλων, ο επόπτης ομίλου θα πρέπει να πρέπει να διασφαλίζει ότι οι επιπτώσεις της εξωτερικής ανάθεσης κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους αποτυπώνονται στην αξιολόγηση των εποπτικών κινδύνων του ομίλου, λαμβάνοντας υπόψη τις απαιτήσεις που απαριθμούνται στις παραγράφους 58-59, καθώς και τα επιμέρους χαρακτηριστικά διακυβέρνησης και τα επιχειρησιακά χαρακτηριστικά του ομίλου.

61. Εάν η εξωτερική ανάθεση κρίσιμων ή σημαντικών επιχειρησιακών λειτουργιών ή δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους αφορά περισσότερες από μία επιχειρήσεις σε διαφορετικά κράτη μέλη και η διαχείρισή της πραγματοποιείται σε κεντρικό επίπεδο από μια μητρική εταιρεία ή από θυγατρική ενός ομίλου (για παράδειγμα, μια επιχείρηση ή μια εταιρεία παροχής υπηρεσιών του ομίλου, όπως ο πάροχος υπηρεσιών ΤΠΕ του ομίλου), ο επόπτης ομίλου και/ή οι αρμόδιες εποπτικές αρχές των επιχειρήσεων που μετέχουν στην εξωτερική ανάθεση δραστηριοτήτων υπολογιστικού νέφους θα πρέπει να εξετάζουν, ενδεχομένως, στο πλαίσιο του σώματος εποπτών, τις επιπτώσεις της εξωτερικής ανάθεσης δραστηριοτήτων υπολογιστικού νέφους στο προφίλ κινδύνου του ομίλου.

62. Σε περίπτωση που ανακύπτουν ανησυχίες οι οποίες οδηγούν στο συμπέρασμα ότι μια επιχείρηση δεν διαθέτει πλέον άρτιες ρυθμίσεις διακυβέρνησης ή δεν συμμορφώνεται με τις κανονιστικές απαιτήσεις, οι εποπτικές αρχές θα πρέπει να λαμβάνουν κατάλληλα μέτρα όπως, για παράδειγμα, μεταξύ άλλων, την απαίτηση από την επιχείρηση να βελτιώσει τις ρυθμίσεις διακυβέρνησης, την επιβολή ορίων ή περιορισμών στο πεδίο εφαρμογής των λειτουργιών που αποτελούν αντικείμενο εξωτερικής ανάθεσης ή την απαίτηση εξόδου από μία ή περισσότερες συμφωνίες εξωτερικής ανάθεσης. Ειδικότερα, λαμβανομένης υπόψη της ανάγκης να διασφαλιστεί η συνέχεια της λειτουργίας της επιχείρησης, θα μπορούσε να απαιτείται επίσης η ακύρωση συμβάσεων, εάν δεν είναι δυνατή η διασφάλιση της εποπτείας και της επιβολής των κανονιστικών απαιτήσεων με τη λήψη άλλων μέτρων.

Συμμόρφωση και κανόνες αναφοράς

63. Το παρόν έγγραφο περιέχει κατευθυντήριες γραμμές οι οποίες εκδίδονται δυνάμει του άρθρου 16 του κανονισμού (ΕΕ) αριθ. 1094/2010. Σύμφωνα με το άρθρο 16 παράγραφος 3 του εν λόγω κανονισμού, οι αρμόδιες αρχές και τα χρηματοοικονομικά ιδρύματα καταβάλλουν κάθε δυνατή προσπάθεια για να συμμορφωθούν με τις εκάστοτε κατευθυντήριες γραμμές και συστάσεις.

64. Οι αρμόδιες αρχές που συμμορφώνονται ή προτίθενται να συμμορφωθούν προς τις παρούσες κατευθυντήριες γραμμές θα πρέπει να τις ενσωματώσουν δεόντως στο ρυθμιστικό ή εποπτικό τους πλαίσιο.

65. Οι αρμόδιες αρχές πρέπει να επιβεβαιώνουν στην EIOPA αν συμμορφώνονται ή προτίθενται να συμμορφωθούν προς τις παρούσες κατευθυντήριες γραμμές, αναφέροντας τους λόγους της ενδεχόμενης μη συμμόρφωσης, εντός δύο μηνών από την ημερομηνία έκδοσης της μετάφρασης των κατευθυντήριων γραμμών.

66. Ελλείψει απάντησης εντός της προθεσμίας αυτής, θα θεωρείται ότι οι αρμόδιες αρχές δεν συμμορφώνονται προς τους κανόνες αναφοράς και θα αποτελούν αντικείμενο σχετικής αναφοράς.

Τελική διάταξη περί επανεξέτασης

67. Οι παρούσες κατευθυντήριες γραμμές υπόκεινται σε επανεξέταση από την EIOPA.