

Κατευθυντήριες γραμμές

Σχετικά με την εξωτερική ανάθεση δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους

Πίνακας περιεχομένων

1	Πεδίο εφαρμογής.....	3
2	Νομοθετικές παραπομπές, συντομογραφίες και ορισμοί	4
2.1	Νομοθετικές παραπομπές.....	4
2.2	Συντμήσεις.....	5
2.3	Ορισμοί.....	5
3	Σκοπός.....	8
4	Συμμόρφωση και υποχρεώσεις κοινοποίησης στοιχείων	8
4.1	Καθεστώς των κατευθυντήριων γραμμών	8
4.2	Υποχρεώσεις κοινοποίησης στοιχείων	8
5	Κατευθυντήριες γραμμές σχετικά με την εξωτερική ανάθεση δραστηριοτήτων σε παρόχους υπηρεσιών νέφους	9
	Κατευθυντήρια γραμμή αριθ. 1. Διακυβέρνηση, εποπτεία και τεκμηρίωση	9
	Κατευθυντήρια γραμμή αριθ. 2. Ανάλυση και έλεγχοι δέουσας επιμέλειας πριν από την εξωτερική ανάθεση	11
	Κατευθυντήρια γραμμή αριθ. 3. Βασικά συμβατικά στοιχεία.....	14
	Κατευθυντήρια γραμμή αριθ. 4. Ασφάλεια πληροφοριών	15
	Κατευθυντήρια γραμμή αριθ. 5. Στρατηγικές αποχώρησης	17
	Κατευθυντήρια γραμμή αριθ. 6. Δικαιώματα πρόσβασης και ελέγχου	18
	Κατευθυντήρια γραμμή αριθ. 7. Υπεργολαβική ανάθεση.....	20
	Κατευθυντήρια γραμμή αριθ. 8. Έγγραφο κοινοποίηση στις αρμόδιες αρχές	21
	Κατευθυντήρια γραμμή αριθ. 9. Εποπτεία συμφωνιών εξωτερικής ανάθεσης δραστηριοτήτων νέφους.....	22

1 Πεδίο εφαρμογής

Ποιος;

1. Οι παρούσες κατευθυντήριες γραμμές εφαρμόζονται στις αρμόδιες αρχές και i) στους θεματοφύλακες οργανισμών εναλλακτικών επενδύσεων (ΟΕΕ) που αναφέρονται στο άρθρο 21 παράγραφος 3 στοιχείο γ) και στο άρθρο 21 παράγραφος 3 τρίτο εδάφιο της ΟΔΟΕΕ, όταν δεν είναι χρηματοπιστωτικές οντότητες στις οποίες εφαρμόζεται η DORA, και ii) στους θεματοφύλακες ΟΣΕΚΑ που αναφέρονται στο άρθρο 23 παράγραφος 2 στοιχείο γ) της οδηγίας ΟΣΕΚΑ, όταν δεν είναι χρηματοπιστωτικές οντότητες στις οποίες εφαρμόζεται η DORA.¹

Τι;

2. Οι παρούσες κατευθυντήριες γραμμές εφαρμόζονται σε σχέση με τις ακόλουθες διατάξεις:
 - α) Όσον αφορά τους θεματοφύλακες των ΟΕΕ: το άρθρο 21 της ΟΔΟΕΕ· το άρθρο 98 του κατ' εξουσιοδότηση κανονισμού (ΕΕ) 2013/231 της Επιτροπής·
 - β) Όσον αφορά τους θεματοφύλακες ΟΣΕΚΑ: το άρθρο 22, το άρθρο 22α και το άρθρο 23 παράγραφος 2 της οδηγίας ΟΣΕΚΑ· το άρθρο 32 της οδηγίας 2010/43/ΕΕ της Επιτροπής· Άρθρο 2 παράγραφος 2 στοιχείο i), άρθρο 3 παράγραφος 1, άρθρο 13 παράγραφος 2, άρθρα 15, 16 και 22 του κατ' εξουσιοδότηση κανονισμού (ΕΕ) 2016/438 της Επιτροπής.

Πότε;

3. Οι παρούσες κατευθυντήριες γραμμές εφαρμόζονται από την ημερομηνία δημοσίευσής τους στον ιστότοπο της ESMA σε όλες τις επίσημες γλώσσες της ΕΕ και σε όλες τις ρυθμίσεις εξωτερικής ανάθεσης υπηρεσιών υπολογιστικού νέφους που συνάπτονται, ανανεώνονται ή τροποποιούνται κατά ή μετά την εν λόγω ημερομηνία.
4. Υπό το πρίσμα της εφαρμογής του DORA, οι προηγούμενες κατευθυντήριες γραμμές της ESMA σχετικά με την εξωτερική ανάθεση σε παρόχους υπηρεσιών υπολογιστικού νέφους παύουν να ισχύουν για τις χρηματοπιστωτικές οντότητες που υπόκεινται στον DORA και αναφέρονται στο άρθρο 2 του ίδιου κανονισμού. Για τους θεματοφύλακες των ΟΕΕ και για τους θεματοφύλακες των ΟΣΕΚΑ που αναφέρονται στην παράγραφο 1 ανωτέρω, οι προηγούμενες κατευθυντήριες γραμμές της ESMA σχετικά με την εξωτερική ανάθεση σε παρόχους υπηρεσιών υπολογιστικού νέφους θα εξακολουθήσουν να ισχύουν έως την ημερομηνία δημοσίευσης των εν λόγω κατευθυντήριων γραμμών στον ιστότοπο της ESMA σε όλες τις επίσημες γλώσσες της ΕΕ.

¹ Σε σχέση με τις συμφωνίες ανάθεσης υπηρεσιών υπολογιστικού νέφους, τα χρηματοπιστωτικά ιδρύματα όπως ορίζονται στο άρθρο 2, παράγραφοι 1 και 2 του κανονισμού (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα για τον χρηματοπιστωτικό 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 (κανονισμός DORA), υπόκεινται στους ειδικούς κανόνες που καθορίζονται στον κανονισμό DORA και στους σχετικούς κανονισμούς της Επιτροπής.

2 Νομοθετικές παραπομπές, συντομογραφίες και ορισμοί

2.1 Νομοθετικές παραπομπές

Κανονισμός ESMA	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 ²
Οδηγία AIFMD	Οδηγία 2011/61/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 8ης Ιουνίου 2011, σχετικά με τους διαχειριστές οργανισμών εναλλακτικών επενδύσεων και για την τροποποίηση των οδηγιών 2003/41/ΕΚ και 2009/65/ΕΚ και των κανονισμών (ΕΚ) αριθ. 1060/2009 και (ΕΕ) αριθ. 1095/2010 ³
Κατ' εξουσιοδότηση κανονισμός (ΕΕ) αριθ. 2013/231 της Επιτροπής	Κατ' εξουσιοδότηση κανονισμός (ΕΕ) αριθ. 231/2013 της Επιτροπής, της 19ης Δεκεμβρίου 2012, προς συμπλήρωση της οδηγίας 2011/61/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τις εξαιρέσεις, τους γενικούς όρους λειτουργίας, τους θεματοφύλακες, τη μόχλευση, τη διαφάνεια και την εποπτεία ⁴
Οδηγία ΟΣΕΚΑ	Οδηγία 2009/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουλίου 2009, για τον συντονισμό των νομοθετικών, κανονιστικών και διοικητικών διατάξεων σχετικά με ορισμένους οργανισμούς συλλογικών επενδύσεων σε κινητές αξίες (ΟΣΕΚΑ) ⁵
Οδηγία 2010/43/ΕΕ της Επιτροπής	Οδηγία 2010/43/ΕΕ της Επιτροπής, της 1ης Ιουλίου 2010, για την εφαρμογή της οδηγίας 2009/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τις οργανωτικές απαιτήσεις, τις συγκρούσεις συμφερόντων, την άσκηση επιχειρηματικής δραστηριότητας, τη διαχείριση κινδύνου και το περιεχόμενο της συμφωνίας μεταξύ ενός θεματοφύλακα και μιας εταιρείας διαχείρισης ⁶

² ΕΕ L 331 της 15.12.2010, σ. 84

³ ΕΕ L 174 της 1.7.2011, σ. 1.

⁴ ΕΕ L 83 της 23.3.2013, σ. 1

⁵ ΕΕ L 302 της 17.11.2009, σ. 32

⁶ ΕΕ L 176 της 10.7.2010, σ. 42

DORA	Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 ⁷
ΓΚΠΔ	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 ⁸

2.2 Συντμήσεις

ΠΥΝ	Πάροχος υπηρεσιών νέφους
ESMA	Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών
ΕΕ	Ευρωπαϊκή Ένωση

2.3 Ορισμοί

Λειτουργία	οποιαδήποτε διαδικασία, υπηρεσία ή δραστηριότητα
κρίσιμη ή σημαντική λειτουργία	οποιαδήποτε λειτουργία της οποίας η πλημμελής εκτέλεση ή η παράλειψη εκτέλεσης θα εμπόδιζε ουσιαδώς: α) τη συμμόρφωση μίας επιχείρησης με τις υποχρεώσεις της βάσει της ισχύουσας νομοθεσίας β) τις οικονομικές επιδόσεις μίας επιχείρησης ή γ) την πληρότητα ή τη συνέχεια των βασικών υπηρεσιών και δραστηριοτήτων μίας επιχείρησης

⁷ ΕΕ L 333 της 27.12.2022, σ. 1
⁸ ΕΕ L 119 της 4.5.2016, σ. 1-88

<i>υπηρεσίες νέφους</i>	οι υπηρεσίες που παρέχονται μέσω του υπολογιστικού νέφους ⁹
<i>υπολογιστικό νέφος ή νέφος⁹</i>	πρότυπη τεχνολογική μέθοδος που επιτρέπει την πρόσβαση του δικτύου σε μεταβλητό και ευέλικτο σύνολο κοινόχρηστων υλικών ή εικονικών πόρων (όπως π.χ. διακομιστές, λειτουργικά συστήματα, δίκτυα, λογισμικό, εφαρμογές και αποθηκευτικά μέσα), προσφέροντας στον χρήστη δυνατότητες αυτοεξυπηρέτησης και διαχείρισης όποτε το ζητήσει
<i>πάροχος υπηρεσιών νέφους</i>	τρίτος που παρέχει υπηρεσίες νέφους βάσει συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων νέφους
<i>συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων νέφους</i>	κάθε είδους συμφωνία, περιλαμβανομένων των συμφωνιών ανάθεσης, που συνάπτεται μεταξύ: (i) μίας επιχείρησης και ενός παρόχου υπηρεσιών νέφους βάσει της οποίας ο εν λόγω πάροχος υπηρεσιών νέφους εκτελεί μία λειτουργία η οποία σε οποιαδήποτε άλλη περίπτωση θα εκτελείτο από την ίδια την επιχείρηση· ή (ii) μίας επιχείρησης και ενός τρίτου προσώπου που δεν είναι πάροχος υπηρεσιών νέφους αλλά που βασίζεται σε μεγάλο βαθμό σε πάροχο υπηρεσιών νέφους για να εκτελέσει λειτουργία η οποία σε οποιαδήποτε άλλη περίπτωση θα εκτελείτο από την ίδια την επιχείρηση. Σε αυτή την περίπτωση, η αναφορά σε πάροχο υπηρεσιών νέφους στις παρούσες κατευθυντήριες γραμμές ισοδυναμεί με αναφορά σε ένα τέτοιο τρίτο πρόσωπο.
<i>υπεργολαβική ανάθεση</i>	κατάσταση κατά την οποία ο πάροχος υπηρεσιών νέφους μεταβιβάζει τη λειτουργία που του έχει ανατεθεί (ή μέρος της λειτουργίας) σε άλλον πάροχο υπηρεσιών βάσει συμφωνίας εξωτερικής ανάθεσης
<i>πρότυπο ανάπτυξης υπηρεσιών νέφους</i>	η μέθοδος οργάνωσης του νέφους που βασίζεται στον έλεγχο και στην κοινή χρήση των υλικών ή εικονικών πόρων. Τα πρότυπα ανάπτυξης υπηρεσιών νέφους

⁹ Χάριν συντομίας, το υπολογιστικό νέφος αναφέρεται συχνά ως «νέφος». Για λόγους ευκολίας, στο κείμενο θα χρησιμοποιείται ο όρος «νέφος».

περιλαμβάνουν το κοινοτικό¹⁰, το υβριδικό¹¹, το ιδιωτικό¹² και το δημόσιο¹³ νέφος·

επιχειρήσεις

- a) θεματοφύλακες που αναφέρονται στο άρθρο 21 παράγραφος 3 στοιχείο γ) και στο άρθρο 21 παράγραφος 3 τρίτο εδάφιο της ΟΔΟΕΕ («θεματοφύλακες οργανισμών εναλλακτικών επενδύσεων (ΟΕΕ)»).
- b) θεματοφύλακες που αναφέρονται στο άρθρο 23 παράγραφος 2 στοιχείο γ) της οδηγίας ΟΣΕΚΑ («θεματοφύλακες ΟΣΕΚΑ»).

¹⁰ Σε αυτό το πρότυπο ανάπτυξης οι υπηρεσίες νέφους υποστηρίζουν και χρησιμοποιούνται αποκλειστικά και μόνο από συγκεκριμένη κοινότητα πελατών, οι οποίοι δεσμεύονται από κοινές απαιτήσεις και αναπτύσσουν σχέσεις μεταξύ τους, και οι πόροι ελέγχονται από ένα τουλάχιστον μέλος αυτής της κοινότητας·

¹¹ Σε αυτό το πρότυπο ανάπτυξης χρησιμοποιούνται δύο τουλάχιστον διαφορετικά πρότυπα ανάπτυξης υπηρεσιών νέφους

¹² Σε αυτό το πρότυπο ανάπτυξης οι υπηρεσίες νέφους χρησιμοποιούνται αποκλειστικά και μόνο από έναν πελάτη υπηρεσιών νέφους και οι πόροι ελέγχονται από αυτόν τον πελάτη υπηρεσιών νέφους

¹³ Σε αυτό το πρότυπο ανάπτυξης οι υπηρεσίες νέφους είναι δυνητικά διαθέσιμες σε οποιονδήποτε πελάτη υπηρεσιών νέφους και οι πόροι ελέγχονται από τον πάροχο των υπηρεσιών νέφους

3 Σκοπός

5. Οι παρούσες κατευθυντήριες γραμμές βασίζονται στο άρθρο 16 παράγραφος 1 του κανονισμού ESMA. Οι παρούσες κατευθυντήριες γραμμές αποσκοπούν στη θέσπιση συνεκτικών, αποδοτικών και αποτελεσματικών εποπτικών πρακτικών, στο πλαίσιο του Ευρωπαϊκού Συστήματος Χρηματοπιστωτικής Εποπτείας, και στη διασφάλιση της κοινής, ενιαίας και συνεπούς εφαρμογής των απαιτήσεων που αναφέρονται στο τμήμα 1.1 της ενότητας με τον τίτλο «Τι;» όταν οι επιχειρήσεις αναθέτουν υπηρεσίες σε παρόχους υπηρεσιών νέφους. Συγκεκριμένα, οι παρούσες κατευθυντήριες γραμμές εκδίδονται για να βοηθούν τις επιχειρήσεις και τις αρμόδιες αρχές να εντοπίζουν, να αντιμετωπίζουν και να παρακολουθούν τους κινδύνους και τις δυσκολίες που προκύπτουν από τις συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων νέφους – από τη λήψη της απόφασης για την εξωτερική ανάθεση, την επιλογή του παρόχου υπηρεσιών νέφους και την παρακολούθηση των δραστηριοτήτων που ανατίθενται σε παρόχους έως τις διατάξεις που προβλέπονται για τις στρατηγικές αποχώρησης.

4 Συμμόρφωση και υποχρεώσεις κοινοποίησης στοιχείων

4.1 Καθεστώς των κατευθυντήριων γραμμών

6. Σύμφωνα με το άρθρο 16 παράγραφος 3 του κανονισμού ESMA, οι αρμόδιες αρχές και οι επιχειρήσεις καταβάλλουν κάθε δυνατή προσπάθεια για να συμμορφωθούν με τις παρούσες κατευθυντήριες γραμμές.
7. Οι αρμόδιες αρχές προς τις οποίες απευθύνονται οι παρούσες κατευθυντήριες γραμμές οφείλουν να συμμορφωθούν, ενσωματώνοντάς τις κατευθυντήριες γραμμές κατά περίπτωση στα οικεία εθνικά νομικά και/ή εποπτικά πλαίσια, ακόμη και όταν επιμέρους κατευθυντήριες γραμμές απευθύνονται πρωτίστως σε επιχειρήσεις. Σε αυτήν την περίπτωση, οι αρμόδιες αρχές πρέπει να διασφαλίζουν, μέσω των εποπτικών τους αρμοδιοτήτων, ότι οι επιχειρήσεις συμμορφώνονται προς τις κατευθυντήριες γραμμές.

4.2 Υποχρεώσεις κοινοποίησης στοιχείων

8. Εντός δύο μηνών από την ημερομηνία δημοσίευσης των κατευθυντήριων γραμμών στον δικτυακό τόπο της ESMA και σε όλες τις επίσημες γλώσσες της ΕΕ, οι αρμόδιες αρχές προς τις οποίες απευθύνονται οι παρούσες κατευθυντήριες γραμμές οφείλουν να κοινοποιήσουν στην ESMA αν i) συμμορφώνονται, ii) δεν συμμορφώνονται, αλλά προτίθενται να συμμορφωθούν ή iii) δεν συμμορφώνονται και δεν προτίθενται να συμμορφωθούν με τις κατευθυντήριες γραμμές.
9. Σε περίπτωση μη συμμόρφωσής τους, οι αρμόδιες αρχές οφείλουν επίσης να κοινοποιήσουν στην ESMA εντός δύο μηνών από την ημερομηνία δημοσίευσης των κατευθυντήριων γραμμών στον δικτυακό τόπο της ESMA και σε όλες τις επίσημες γλώσσες της ΕΕ τους λόγους μη συμμόρφωσης με τις κατευθυντήριες γραμμές. Υπόδειγμα για τις κοινοποιήσεις διατίθεται στον δικτυακό τόπο της ESMA. Μόλις το υπόδειγμα συμπληρωθεί, διαβιβάζεται στην ESMA.

10. Οι επιχειρήσεις δεν είναι υποχρεωμένες να αναφέρουν αν συμμορφώνονται ή όχι προς τις παρούσες κατευθυντήριες γραμμές.

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

Κατευθυντήρια γραμμή αριθ. 1. Διακυβέρνηση, εποπτεία και τεκμηρίωση

11. Οι επιχειρήσεις πρέπει να διαθέτουν συγκεκριμένες και επικαιροποιημένες στρατηγικές για την εξωτερική ανάθεση δραστηριοτήτων νέφους, που να συμβαδίζουν με τις σχετικές στρατηγικές και τις εσωτερικές πολιτικές και διαδικασίες των επιχειρήσεων όσον αφορά, μεταξύ άλλων, τις τεχνολογίες των πληροφοριών και των επικοινωνιών, την ασφάλεια των πληροφοριών και τη διαχείριση λειτουργικού κινδύνου.
12. Οι επιχειρήσεις πρέπει:
- α) να αναθέτουν με σαφήνεια αρμοδιότητες για την τεκμηρίωση, τη διαχείριση και τον έλεγχο των συμφωνιών εξωτερικής ανάθεσης δραστηριοτήτων νέφους εντός των οργανισμών τους·
 - β) να εκχωρούν επαρκείς πόρους για να διασφαλίζουν τη συμμόρφωση με τις παρούσες κατευθυντήριες γραμμές και όλες τις νόμιμες απαιτήσεις που ισχύουν για τις συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων νέφους·
 - γ) να καθιερώνουν λειτουργίες εποπτείας της εξωτερικής ανάθεσης δραστηριοτήτων νέφους ή να ορίσουν ανώτατα στελέχη τα οποία θα λογοδοτούν απευθείας στο διοικητικό όργανο και θα είναι υπεύθυνα για να διαχειρίζονται και να εποπτεύουν τους κινδύνους των συμφωνιών εξωτερικής ανάθεσης δραστηριοτήτων νέφους. Κατά τη συμμόρφωσή τους με τις παρούσες κατευθυντήριες γραμμές, οι επιχειρήσεις πρέπει να λαμβάνουν υπόψη τη φύση, το μέγεθος και την πολυπλοκότητα των επιχειρηματικών τους δραστηριοτήτων, εστιάζοντας μεταξύ άλλων στον κίνδυνο που εγκυμονούν οι δραστηριότητές τους για το χρηματοπιστωτικό σύστημα, καθώς και τους κινδύνους που παρουσιάζουν οι ανατεθείσες λειτουργίες, και να μεριμνούν ώστε το διοικητικό τους όργανο να διαθέτει τις κατάλληλες τεχνικές δεξιότητες για να κατανοεί τους κινδύνους που εγκυμονούν οι συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων νέφους. Οι μικρές και λιγότερο περίπλοκες επιχειρήσεις πρέπει τουλάχιστον να διασφαλίζουν τον σαφή επιμερισμό καθηκόντων και αρμοδιοτήτων για τη διαχείριση και την εποπτεία των συμφωνιών εξωτερικής ανάθεσης δραστηριοτήτων νέφους.
13. Οι επιχειρήσεις πρέπει να παρακολουθούν τις επιδόσεις των δραστηριοτήτων, τα μέτρα ασφάλειας και την τήρηση των συμφωνηθέντων επιπέδων εξυπηρέτησης από τους οικείους παρόχους υπηρεσιών νέφους. Η εν λόγω παρακολούθηση πρέπει να

βασίζεται στους κινδύνους και να εστιάζει πρωτίστως στις κρίσιμες ή σημαντικές λειτουργίες που έχουν ανατεθεί.

14. Οι επιχειρήσεις πρέπει να αποτιμούν σε τακτική βάση αν οι συμφωνίες τους για την εξωτερική ανάθεση δραστηριοτήτων αφορούν κρίσιμες ή σημαντικές λειτουργίες και αν ο κίνδυνος, τη φύση ή το μέγεθος της ανατεθείσας λειτουργίας έχει μεταβληθεί ουσιωδώς.
15. Οι επιχειρήσεις πρέπει να τηρούν επικαιροποιημένο μητρώο πληροφοριών για όλες τις συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων νέφους που συνάπτουν, διαχωρίζοντας τις συμφωνίες εξωτερικής ανάθεσης κρίσιμων ή σημαντικών λειτουργιών από τις λοιπές συμφωνίες εξωτερικής ανάθεσης. Όταν διαχωρίζουν τις συμφωνίες εξωτερικής ανάθεσης κρίσιμων ή σημαντικών λειτουργιών από τις λοιπές συμφωνίες εξωτερικής ανάθεσης, οι επιχειρήσεις πρέπει να αναφέρουν συνοπτικά τους λόγους για τους οποίους η ανατεθείσα λειτουργία θεωρείται ή δεν θεωρείται κρίσιμη ή σημαντική. Λαμβάνοντας υπόψη την εθνική νομοθεσία, οι επιχειρήσεις πρέπει επίσης να τηρούν μητρώο με τις καταγγελλθείσες συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων νέφους για κατάλληλο χρονικό διάστημα.
16. Για τις συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων νέφους που αφορούν κρίσιμες ή σημαντικές λειτουργίες, το μητρώο πρέπει να περιλαμβάνει τουλάχιστον τις ακόλουθες πληροφορίες για κάθε συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων νέφους:
 - α) τον αριθμό αναφοράς της συμφωνίας·
 - β) την ημερομηνία έναρξης και, κατά περίπτωση, την επόμενη ημερομηνία ανανέωσης της σύμβασης, την ημερομηνία λήξης και/ή τα χρονικά περιθώρια προειδοποίησης για τον πάροχο υπηρεσιών νέφους και για την επιχείρηση·
 - γ) συνοπτική περιγραφή της ανατεθείσας λειτουργίας, μεταξύ άλλων τα δεδομένα που ανατίθενται και αν τα δεδομένα αυτά περιλαμβάνουν δεδομένα προσωπικού χαρακτήρα (π.χ. σημειώνεται «ναι» ή «όχι» σε χωριστό πεδίο δεδομένων)·
 - δ) την κατηγορία στην οποία κατατάσσει η επιχείρηση την ανατεθείσα λειτουργία με βάση τη φύση της (π.χ. λειτουργία τεχνολογίας πληροφοριών, λειτουργία ελέγχου), η οποία είναι πολύ πιθανό να διευκολύνει την κωδικοποίηση των διαφορετικών ειδών συμφωνιών εξωτερικής ανάθεσης δραστηριοτήτων νέφους·
 - ε) αν η ανατεθείσα λειτουργία υποστηρίζει επιχειρηματικές δραστηριότητες οι οποίες είναι κρίσιμες από πλευράς χρόνου·
 - στ) το όνομα και την εταιρική επωνυμία (αν υπάρχει) του παρόχου υπηρεσιών νέφους, τη χώρα καταχώρισής του, τον εταιρικό αριθμό μητρώου του, τον αναγνωριστικό κωδικό της νομικής του οντότητας (αν υπάρχει), την καταστατική του έδρα, άλλα συναφή στοιχεία επικοινωνίας, καθώς και την επωνυμία της μητρικής του εταιρείας (αν υπάρχει)·
 - ζ) τη νομοθεσία που διέπει τη συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων νέφους και, κατά περίπτωση, τη δικαιοδοσία που έχει επιλεγεί·
 - η) το είδος των υπηρεσιών νέφους και τα πρότυπα ανάπτυξής τους, τα ειδικά χαρακτηριστικά των δεδομένων που πρέπει να φυλάσσονται, καθώς και τις τοποθεσίες (για την ακρίβεια τις περιφέρειες ή τις χώρες) στις οποίες επιτρέπεται να φυλάσσονται αυτά τα δεδομένα·

- θ) την ημερομηνία της τελευταίας αξιολόγησης του κρίσιμου ή σημαντικού χαρακτήρα της ανατεθείσας λειτουργίας και την ημερομηνία της επόμενης προγραμματισμένης αξιολόγησης·
 - ι) την ημερομηνία της τελευταίας εκτίμησης κινδύνου/του τελευταίου ελέγχου του παρόχου υπηρεσιών νέφους, σε συνδυασμό με τη συνοπτική παρουσίαση των βασικών αποτελεσμάτων της εκτίμησης/του ελέγχου, καθώς και την ημερομηνία της επόμενης προγραμματισμένης εκτίμησης κινδύνου/του επόμενου προγραμματισμένου ελέγχου·
 - ια) το πρόσωπο ή το όργανο λήψης αποφάσεων εντός της επιχείρησης που ενέκρινε τη συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων νέφους·
 - ιβ) ανάλογα με την περίπτωση, τα ονόματα των υπεργολάβων στους οποίους ανατίθενται κρίσιμες ή σημαντικές λειτουργίες (ή ουσιώδη μέρη τους), συμπεριλαμβανομένων των χωρών στις οποίες είναι καταχωρισμένοι οι υπεργολάβοι και στις οποίες θα παρέχεται η υπηρεσία που ανατίθεται υπεργολαβικά, καθώς και των τοποθεσιών (δηλαδή των περιφερειών ή των χωρών) στις οποίες θα αποθηκεύονται τα δεδομένα·
 - ιγ) το εκτιμώμενο ετήσιο κόστος του προϋπολογισμού της συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων νέφους·
17. Όσον αφορά τις συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων νέφους που αφορούν μη κρίσιμες ή μη σημαντικές λειτουργίες, οι επιχειρήσεις πρέπει να προσδιορίζουν τις πληροφορίες που θα συμπεριλαμβάνονται στο μητρώο ανάλογα με τη φύση, το μέγεθος και την πολυπλοκότητα των κινδύνων που εγκυμονεί η ανατεθείσα λειτουργία.

Κατευθυντήρια γραμμή αριθ. 2. Ανάλυση και έλεγχοι δέουσας επιμέλειας πριν από την εξωτερική ανάθεση

18. Πριν από τη σύναψη της συμφωνίας για την εξωτερική ανάθεση δραστηριοτήτων νέφους, οι επιχειρήσεις πρέπει:
- α) να αξιολογούν αν η συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων νέφους αφορά κρίσιμη ή σημαντική λειτουργία·
 - β) να εντοπίζουν και να αξιολογούν όλους τους συναφείς κινδύνους της συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων νέφους·
 - γ) να διενεργούν κατάλληλους ελέγχους δέουσας επιμέλειας στους μελλοντικούς παρόχους υπηρεσιών νέφους·
 - δ) να εντοπίζουν και να αξιολογούν συγκρούσεις συμφερόντων που μπορεί να προκαλέσει η εξωτερική ανάθεση.
19. Οι αναλύσεις και οι διαδικασίες δέουσας επιμέλειας για τους μελλοντικούς παρόχους υπηρεσιών νέφους που διενεργούνται πριν από την εξωτερική ανάθεση πρέπει να είναι ανάλογες της φύσης, του μεγέθους και της πολυπλοκότητας της λειτουργίας που προτίθεται να αναθέσει η επιχείρηση, καθώς και των κινδύνων που εγκυμονεί η λειτουργία αυτή. Στο πλαίσιο των διαδικασιών, πρέπει να αξιολογούνται οι επιπτώσεις που είναι πιθανό να προκαλέσει η συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων

νέφους στους επιχειρησιακούς κινδύνους, στους νομικούς κινδύνους στους κινδύνους κανονιστικής συμμόρφωσης και στους κινδύνους για τη φήμη της επιχείρησης.

20. Σε περίπτωση που η συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων νέφους αφορά κρίσιμη ή σημαντική λειτουργία, οι επιχειρήσεις πρέπει επίσης:

α) να αξιολογούν όλους τους σχετικούς κινδύνους που είναι πιθανό να προκύψουν ως αποτέλεσμα της συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων νέφους, μεταξύ άλλων τους κινδύνους που συνδέονται με την τεχνολογία των πληροφοριών και των επικοινωνιών, την ασφάλεια των πληροφοριών, τη συνέχεια των δραστηριοτήτων, τους νομικούς κινδύνους, τους κινδύνους κανονιστικής συμμόρφωσης, τους κινδύνους για τη φήμη των επιχειρήσεων, τους επιχειρησιακούς κινδύνους, καθώς και τα εμπόδια που είναι πιθανό να δυσχεράνουν τα εποπτικά καθήκοντα της επιχείρησης, τα οποία θα μπορούσαν να προκληθούν από:

- i. την υπηρεσία νέφους που επιλέγεται και από το πρότυπο ανάπτυξης που προτείνεται για την υπηρεσία αυτή·
- ii. τις διαδικασίες μετεγκατάστασης και/ή εφαρμογής·
- iii. την ευαισθησία της λειτουργίας και των σχετικών δεδομένων που εξετάζεται να ανατεθούν σε τρίτους και από τα μέτρα ασφάλειας που πρέπει να ληφθούν·
- iv. τη διαλειτουργικότητα των συστημάτων και των εφαρμογών της επιχείρησης και του παρόχου υπηρεσιών νέφους, πιο συγκεκριμένα τη δυνατότητα των επιχειρήσεων και των παρόχων υπηρεσιών νέφους να ανταλλάσσουν πληροφορίες και να χρησιμοποιούν από κοινού τις πληροφορίες που έχουν ανταλλαγή·
- v. τη φορητότητα των δεδομένων της επιχείρησης, πιο συγκεκριμένα τη δυνατότητα εύκολης μεταφοράς των δεδομένων της επιχείρησης από έναν πάροχο υπηρεσιών νέφους σε άλλο πάροχο ή τη δυνατότητα επιστροφής των δεδομένων στην επιχείρηση·
- vi. την πολιτική σταθερότητα, τις συνθήκες ασφάλειας και το νομικό σύστημα (περιλαμβάνονται εν προκειμένω οι διατάξεις επιβολής του νόμου που είναι σε ισχύ, οι διατάξεις της νομοθεσίας περί αφερεγγυότητας που εφαρμόζονται σε περίπτωση πτώχευσης του παρόχου υπηρεσιών νέφους, οι ισχύοντες νόμοι για την προστασία δεδομένων και αν εκπληρώνονται βάσει του ΓΚΠΔ οι προϋποθέσεις για τη μεταφορά των δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα) των χωρών (εντός ή εκτός ΕΕ) στις οποίες θα παρασχεθούν οι ανατεθείσες λειτουργίες και στις οποίες θα αποθηκεύονται τα ανατεθέντα δεδομένα· σε περίπτωση υπεργολαβικής ανάθεσης, τους επιπλέον κινδύνους που είναι πιθανό να προκύψουν αν ο υπεργολάβος βρίσκεται σε τρίτη χώρα ή σε διαφορετική χώρα από τη χώρα του παρόχου υπηρεσιών νέφους και, αν υφίσταται αλυσίδα υπεργολαβίας, τους επιπλέον κινδύνους που ενδέχεται να προκύψουν, μεταξύ άλλων, επειδή δεν έχει συναφθεί απευθείας σύμβαση μεταξύ της επιχείρησης και του υπεργολάβου που επιτελεί την ανατεθείσα λειτουργία·
- vii. τα φαινόμενα συγκέντρωσης που είναι πιθανό να παρουσιαστούν εντός της επιχείρησης (και, αν συντρέχει περίπτωση, εντός του ομίλου), ως αποτέλεσμα της σύναψης πολλαπλών συμφωνιών εξωτερικής ανάθεσης

δραστηριοτήτων νέφους με τον ίδιο πάροχο υπηρεσιών νέφους, καθώς και τα φαινόμενα συγκέντρωσης που είναι πιθανό να παρουσιαστούν εντός του χρηματοπιστωτικού τομέα της ΕΕ, ως αποτέλεσμα της συνεργασίας πολλών επιχειρήσεων με τον ίδιο πάροχο υπηρεσιών νέφους ή με μικρή ομάδα παρόχων υπηρεσιών νέφους. Όταν αξιολογεί τον κίνδυνο συγκέντρωσης, η επιχείρηση πρέπει να λαμβάνει υπόψη όλες τις συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων νέφους που έχει συνάψει (και, αν συντρέχει περίπτωση, τις συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων νέφους στο επίπεδο του ομίλου της) με τον ίδιο πάροχο υπηρεσιών νέφους·

- β) να λαμβάνουν υπόψη τα αναμενόμενα οφέλη και το κόστος της συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων νέφους, σταθμίζοντας μεταξύ άλλων τους σημαντικούς κινδύνους που θα μπορούν να περιοριστούν ή να ελεγχθούν καλύτερα μέσω της συμφωνίας, έναντι των σημαντικών κινδύνων που είναι πιθανό να προκαλέσει η συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων νέφους·

21. Αν η εξωτερική ανάθεση αφορά κρίσιμες ή σημαντικές λειτουργίες, ο έλεγχος δέουσας επιμέλειας πρέπει να περιλαμβάνει την αξιολόγηση της καταλληλότητας του παρόχου υπηρεσιών νέφους. Όταν αξιολογούν την καταλληλότητα του παρόχου υπηρεσιών νέφους, οι επιχειρήσεις πρέπει να διασφαλίζουν ότι ο πάροχος υπηρεσιών νέφους έχει την επιχειρηματική φήμη, τις ικανότητες, τους πόρους (μεταξύ άλλων το ανθρώπινο δυναμικό, τα συστήματα ΤΠ, και τους οικονομικούς πόρους), την οργανωτική δομή και, κατά περίπτωση, τη/τις σχετική/-ές άδεια/-ες ή το/τα σχετικό/-ά πιστοποιητικό/-ά που απαιτούνται για να εκτελέσει την κρίσιμη ή σημαντική λειτουργία με αξιοπιστία και επαγγελματισμό και να εκπληρώσει τις υποχρεώσεις του κατά τη διάρκεια ισχύος της σύμβασης εξωτερικής ανάθεσης δραστηριοτήτων νέφους. Κατά τον έλεγχο δέουσας επιμέλειας που διενεργείται για πάροχο υπηρεσιών νέφους, πρέπει επίσης να λαμβάνονται υπόψη οι ακόλουθοι –ενδεικτικοί– παράγοντες:

- α) η διαχείριση της ασφάλειας των πληροφοριών, κυρίως η προστασία των δεδομένων προσωπικού χαρακτήρα, των απόρρητων ή –σε άλλες περιπτώσεις– ευαίσθητων δεδομένων·
- β) οι υποστηρικτικές υπηρεσίες, μεταξύ άλλων τα σχέδια και οι επαφές υποστήριξης, καθώς και οι διαδικασίες αντιμετώπισης συμβάντων·
- γ) τα σχέδια για την αδιάλειπτη συνέχεια των δραστηριοτήτων της επιχείρησης και τα σχέδια αποκατάστασης της λειτουργίας της επιχείρησης σε περίπτωση καταστροφικού συμβάντος·

22. Κατά περίπτωση, και προκειμένου να υποστηρίξουν τους ελέγχους δέουσας επιμέλειας που διενεργούν, οι επιχειρήσεις έχουν επίσης τη δυνατότητα να χρησιμοποιήσουν πιστοποιήσεις που βασίζονται σε διεθνή πρότυπα και εκθέσεις εξωτερικού ή εσωτερικού ελέγχου.

23. Αν υποπτεύουν στην αντίληψη της επιχείρησης σοβαρές ελλείψεις και/ή σημαντικές αλλαγές στις παρεχόμενες υπηρεσίες ή στην κατάσταση του παρόχου υπηρεσιών υπολογιστικού νέφους, οι αναλύσεις και οι έλεγχοι δέουσας επιμέλειας που

διενεργούνται πριν από την εξωτερική ανάθεση για τον πάροχο υπηρεσιών νέφους πρέπει να επανεξεταστούν αμέσως ή, αν κρίνεται αναγκαίο, να επαναληφθούν.

24. Αν η επιχείρηση συνάψει νέα συμφωνία ή ανανεώσει υφιστάμενη συμφωνία με πάροχο υπηρεσιών νέφους που έχει ήδη αξιολογηθεί, πρέπει να κρίνει, με βάση τους κινδύνους που εντοπίζει, αν πρέπει να διενεργήσει νέο έλεγχο δέουσας επιμέλειας.

Κατευθυντήρια γραμμή αριθ. 3. Βασικά συμβατικά στοιχεία

25. Τα αντίστοιχα δικαιώματα και οι αντίστοιχες υποχρεώσεις της επιχείρησης και του παρόχου υπηρεσιών νέφους πρέπει να επιμερίζονται σαφώς και να ορίζονται σε έγγραφη συμφωνία.
26. Η έγγραφη συμφωνία πρέπει να παρέχει ρητά τη δυνατότητα στην επιχείρηση να καταγγείλει τη συμφωνία αν κριθεί αναγκαίο.
27. Όταν η εξωτερική ανάθεση περιλαμβάνει κρίσιμες ή σημαντικές λειτουργίες, η έγγραφη συμφωνία πρέπει να περιλαμβάνει τουλάχιστον τα εξής:
- α) τη σαφή περιγραφή της ανατεθείσας λειτουργίας·
 - β) την ημερομηνία έναρξης και την ημερομηνία λήξης, κατά περίπτωση, της συμφωνίας και τα χρονικά περιθώρια προειδοποίησης για τον πάροχο υπηρεσιών νέφους και για την επιχείρηση·
 - γ) τη νομοθεσία που διέπει τη συμφωνία και, κατά περίπτωση, τη δικαιοδοσία που έχει επιλεγεί·
 - δ) τις οικονομικές υποχρεώσεις της επιχείρησης και του παρόχου υπηρεσιών νέφους·
 - ε) αν επιτρέπεται η υπεργολαβική ανάθεση και, αν όντως επιτρέπεται, υπό ποιους όρους, με βάση την κατευθυντήρια γραμμή αριθ. 7·
 - στ) την τοποθεσία ή τις τοποθεσίες (για την ακρίβεια τις περιφέρειες ή χώρες) στις οποίες θα παρέχεται η ανατεθείσα λειτουργία και στις οποίες θα αποθηκεύονται και θα υποβάλλονται σε επεξεργασία τα δεδομένα, καθώς και τις προϋποθέσεις που πρέπει να πληρούνται, μεταξύ αυτών και την υποχρέωση ειδοποίησης της επιχείρησης αν ο πάροχος υπηρεσιών νέφους προτίθεται να αλλάξει τοποθεσία ή τοποθεσίες·
 - ζ) τις διατάξεις σχετικά με την ασφάλεια των πληροφοριών και την προστασία δεδομένων προσωπικού χαρακτήρα, με βάση την κατευθυντήρια γραμμή αριθ. 4·
 - η) το δικαίωμα της επιχείρησης να παρακολουθεί τακτικά τις επιδόσεις του παρόχου υπηρεσιών νέφους στο πλαίσιο της συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων νέφους, με βάση την κατευθυντήρια γραμμή αριθ. 6·
 - θ) τα συμφωνηθέντα επίπεδα υπηρεσιών, τα οποία θα πρέπει να περιλαμβάνουν ποσοτικούς και ποιοτικούς δείκτες επιδόσεων, προκειμένου να καθίσταται δυνατή η έγκαιρη παρακολούθηση και να λαμβάνονται κατάλληλα διορθωτικά μέτρα χωρίς αδικαιολόγητες καθυστερήσεις όταν δεν τηρούνται τα επίπεδα εξυπηρέτησης που έχουν συμφωνηθεί·

- ι) τις υποχρεώσεις υποβολής στοιχείων από τον πάροχο υπηρεσιών νέφους προς την επιχείρηση και, ανάλογα με την περίπτωση, τις υποχρεώσεις υποβολής εκθέσεων που είναι σχετικά με τη λειτουργία ασφάλειας και για βασικές λειτουργίες της επιχείρησης, όπως οι εκθέσεις σχετικά με τη λειτουργία εσωτερικού ελέγχου του παρόχου υπηρεσιών νέφους·
- ια) διατάξεις σχετικά με τη διαχείριση των συμβάντων από τον πάροχο υπηρεσιών νέφους, μεταξύ άλλων για την υποχρέωση του παρόχου υπηρεσιών νέφους να αναφέρει στην επιχείρηση χωρίς αδικαιολόγητη καθυστέρηση συμβάντα που έχουν επηρεάσει την παροχή της προβλεπόμενης από τη συμφωνία υπηρεσίας·
- ιβ) αν ο πάροχος υπηρεσιών νέφους πρέπει να διαθέτει υποχρεωτική ασφάλιση για ορισμένους κινδύνους και, κατά περίπτωση, το απαιτούμενο επίπεδο ασφαλιστικής κάλυψης·
- ιγ) την υποχρέωση που υπέχει ο πάροχος υπηρεσιών νέφους να εφαρμόζει και να δοκιμάζει σχέδια για τη συνέχεια των δραστηριοτήτων της επιχείρησής του και για την αποκατάσταση της λειτουργίας της επιχείρησής του μετά από καταστροφικά συμβάντα·
- ιδ) την υποχρέωση που υπέχει ο πάροχος υπηρεσιών νέφους να εκχωρεί στην επιχείρηση, στις αρμόδιες αρχές της και σε οποιοδήποτε άλλο πρόσωπο έχει εξουσιοδοτηθεί για τον σκοπό αυτό από την επιχείρηση ή από τις αρμόδιες αρχές, το δικαίωμα πρόσβασης («δικαίωμα πρόσβασης») και επιθεώρησης («δικαιώματα ελέγχου») των σχετικών πληροφοριών, εγκαταστάσεων, συστημάτων και συσκευών του παρόχου υπηρεσιών νέφους στον βαθμό που απαιτείται για να παρακολουθείται η απόδοση του παρόχου υπηρεσιών νέφους στο πλαίσιο της συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων νέφους και η συμμόρφωσή του με τις ισχύουσες κανονιστικές και συμβατικές απαιτήσεις, με βάση την κατευθυντήρια γραμμή αριθ. 6·
- ιε) διατάξεις που διασφαλίζουν τη δυνατότητα αξιολόγησης, ανάκτησης και επιστροφής στην επιχείρηση, ανάλογα με τις ανάγκες, των δεδομένων που επεξεργάζεται ή φυλάσσει ο πάροχος υπηρεσιών νέφους για λογαριασμό της επιχείρησης, με βάση την κατευθυντήρια γραμμή αριθ. 5.

Κατευθυντήρια γραμμή αριθ. 4. Ασφάλεια πληροφοριών

28. Οι επιχειρήσεις πρέπει να ορίζουν απαιτήσεις για την ασφάλεια των πληροφοριών στις εσωτερικές τους πολιτικές και διαδικασίες και στο πλαίσιο της έγγραφης συμφωνίας για την εξωτερική ανάθεση δραστηριοτήτων νέφους, καθώς και να παρακολουθούν αδιαλείπτως τη συμμόρφωση με αυτές τις απαιτήσεις για να προστατεύουν μεταξύ άλλων απόρρητα, προσωπικά ή –σε άλλες περιπτώσεις– ευαίσθητα δεδομένα. Οι απαιτήσεις αυτές πρέπει να είναι ανάλογες των χαρακτηριστικών, του μεγέθους και της

πολυπλοκότητας της λειτουργίας που αναθέτει η επιχείρηση στον πάροχο υπηρεσιών νέφους και των κινδύνων που εγκυμονεί η λειτουργία αυτή.

29. Για τον σκοπό αυτό, όταν ανατίθενται κρίσιμες ή σημαντικές λειτουργίες, και με την επιφύλαξη των απαιτήσεων που ισχύουν βάσει του ΓΚΠΔ, οι επιχειρήσεις, ακολουθώντας την προσέγγιση βάσει κινδύνων, πρέπει τουλάχιστον:

- α) *οργάνωση της ασφάλειας πληροφοριών*: να διασφαλίζουν τον σαφή επιμερισμό ρόλων και αρμοδιοτήτων μεταξύ της επιχείρησης και του παρόχου υπηρεσιών νέφους όσον αφορά την ασφάλεια των πληροφοριών, εστιάζοντας μεταξύ άλλων στον εντοπισμό των απειλών, στη διαχείριση συμβάντων και στη διαχείριση των ενημερώσεων κώδικα (patch management), καθώς και να διασφαλίζουν ότι ο πάροχος υπηρεσιών νέφους είναι όντως σε θέση να ανταποκριθεί στον ρόλο και στις αρμοδιότητές του·
- β) *διαχείριση ταυτότητας και πρόσβασης*: να διασφαλίζουν ότι υπάρχουν ισχυροί μηχανισμοί επαλήθευσης ταυτότητας (όπως π.χ. για την επαλήθευση ταυτότητας πολλαπλών παραγόντων) και έλεγχοι πρόσβασης προκειμένου να μην επιτρέπεται η μη εξουσιοδοτημένη πρόσβαση στα δεδομένα της επιχείρησης και στους πόρους υπολογιστικού νέφους που χρησιμοποιούνται στο παρασκήνιο (back-end)·
- γ) *κρυπτογράφηση και διαχείριση κλειδιών*: να διασφαλίζουν ότι χρησιμοποιούνται σύγχρονες τεχνολογίες κρυπτογράφησης, όταν χρειάζεται, για τα μεταφερόμενα δεδομένα, τα δεδομένα της μνήμης, τα αδρανή δεδομένα και τα εφεδρικά δεδομένα, σε συνδυασμό με άρτια συστήματα διαχείρισης κλειδιών ώστε να περιορίζεται ο κίνδυνος μη εξουσιοδοτημένης πρόσβασης στα κλειδιά κρυπτογράφησης· συγκεκριμένα, οι επιχειρήσεις θα πρέπει να ενσωματώνουν προηγμένες τεχνολογίες και διαδικασίες στο σύστημα διαχείρισης κλειδιών τους·
- δ) *ασφάλεια της λειτουργίας των υποδομών και του δικτύου*: να μεριμνούν για την επαρκή διαθεσιμότητα του δικτύου τους, για τον διαχωρισμό του δικτύου τους (π.χ. απομόνωση μισθωτή στο κοινόχρηστο περιβάλλον του νέφους, διαχωρισμός λειτουργίας στον ιστό, στο «στρώμα λογικής» των εφαρμογών (application logic), στο λειτουργικό σύστημα, στο δίκτυο, στο σύστημα διαχείρισης βάσης δεδομένων (DBMS) και στο επίπεδο της αποθήκευσης), καθώς και για τα περιβάλλοντα επεξεργασίας (π.χ. δοκιμή, έλεγχος αποδοχής χρήστη, ανάπτυξη, παραγωγή)
- ε) *διεπαφές προγραμματισμού εφαρμογών (ΔΠΕ)*: να εξετάζουν μηχανισμούς για την ενοποίηση των υπηρεσιών νέφους με τα συστήματα της επιχείρησης με σκοπό την ασφάλεια των ΔΠΕ (π.χ. μπορούν να καθιερώσουν και να διατηρούν πολιτικές για την ασφάλεια των πληροφοριών και διαδικασίες για τις ΔΠΕ, καλύπτοντας όλες τις πολλαπλές διεπαφές συστημάτων, τις δικαιοδοσίες καθώς και τις λειτουργίες των συστημάτων ώστε να μην επιτρέπουν τη μη εξουσιοδοτημένη αποκάλυψη, τροποποίηση ή καταστροφή δεδομένων)·
- στ) *συνέχεια των δραστηριοτήτων της επιχείρησης και αποκατάσταση της λειτουργίας της επιχείρησης μετά από καταστροφικό συμβάν*: να διασφαλίζουν ότι εφαρμόζουν αποτελεσματικά μέτρα για τη συνέχεια των δραστηριοτήτων και την αποκατάσταση της λειτουργίας της επιχείρησής τους μετά από καταστροφικά συμβάντα (μπορούν π.χ. να ορίζουν ελάχιστες απαιτήσεις για τη χωρητικότητα των συστημάτων, να επιλέγουν μέσα φιλοξενίας που είναι γεωγραφικά διάσπαρτα και να έχουν τη δυνατότητα να εναλλάσσουν τα μέσα αυτά ή να ζητούν και να επανεξετάζουν την

τεκμηρίωση που απεικονίζει τη διαδρομή μεταφοράς των δεδομένων της επιχείρησης από το ένα σύστημα του παρόχου υπηρεσιών νέφους στο άλλο, καθώς και να μεριμνούν για τη δυνατότητα αναπαραγωγής και μεταφοράς των εικόνων του λειτουργικού συστήματος σε ανεξάρτητη τοποθεσία αποθήκευσης που να είναι αρκετά απομονωμένη από το δίκτυο ή να χρησιμοποιείται εκτός διαδικτύου)·

- ζ) *τοποθεσία δεδομένων*: να ακολουθούν την προσέγγιση βάσει κινδύνων όταν επιλέγουν την τοποθεσία/τις τοποθεσίες αποθήκευσης και επεξεργασίας δεδομένων (δηλαδή τις περιφέρειες ή τις χώρες)·
- η) *συμμόρφωση και παρακολούθηση*: να εξακριβώνουν αν ο πάροχος υπηρεσιών νέφους συμμορφώνεται με τα διεθνώς αναγνωρισμένα πρότυπα της ασφάλειας πληροφοριών και έχει εφαρμόσει επαρκή μέτρα ελέγχου για την ασφάλεια των πληροφοριών (μπορούν π.χ. να ζητούν από το πάροχο υπηρεσιών νέφους να προσκομίσει στοιχεία που αποδεικνύουν ότι διενεργεί ελέγχους σχετικά με την ασφάλεια των πληροφοριών και να διενεργούν τακτικές αξιολογήσεις και δοκιμές στα συστήματα ασφάλειας των πληροφοριών του παρόχου υπηρεσιών νέφους).

Κατευθυντήρια γραμμή αριθ. 5. Στρατηγικές αποχώρησης

30. Όταν η εξωτερική ανάθεση αφορά κρίσιμες ή σημαντικές λειτουργίες, οι επιχειρήσεις πρέπει να διασφαλίζουν ότι έχουν τη δυνατότητα να αποχωρήσουν από τη συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων νέφους χωρίς αδικαιολόγητη διακοπή στις επιχειρηματικές δραστηριότητές τους και στις υπηρεσίες που παρέχουν στους πελάτες τους, και χωρίς να επηρεαστεί δυσμενώς η συμμόρφωση στις υποχρεώσεις που έχουν βάσει της ισχύουσας νομοθεσίας, καθώς και η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων τους. Για τον σκοπό αυτό, οι επιχειρήσεις πρέπει:

- α) να καταρτίζουν σχέδια αποχώρησης που είναι ολοκληρωμένα, τεκμηριωμένα και έχουν υποβληθεί σε επαρκή δοκιμαστικό έλεγχο. Τα σχέδια αυτά πρέπει να επικαιροποιούνται όποτε χρειάζεται, συμπεριλαμβανομένων περιπτώσεων όπου επέρχονται αλλαγές στην ανατεθείσα λειτουργία·
- β) να εντοπίζουν εναλλακτικές λύσεις και να επεξεργάζονται σχέδια μετάβασης ώστε να αφαιρούν την ανατεθείσα λειτουργία και τα ανατεθέντα δεδομένα από τον πάροχο υπηρεσιών νέφους και, κατά περίπτωση, από τους υπεργολάβους, και να μεταβιβάζουν την εν λόγω λειτουργία και τα εν λόγω δεδομένα στον εναλλακτικό πάροχο υπηρεσιών νέφους που υποδεικνύεται από τις επιχειρήσεις ή να τα επιστρέφουν κατευθείαν στις επιχειρήσεις. Οι λύσεις αυτές θα πρέπει να προσδιορίζονται με βάση τις δυσκολίες που ενδέχεται να προκύψουν από την τοποθεσία των δεδομένων και με τη λήψη των αναγκαίων μέτρων που διασφαλίζουν τη συνέχεια των επιχειρησιακών δραστηριοτήτων κατά τη διάρκεια της μεταβατικής περιόδου·
- γ) να διασφαλίζουν ότι η έγγραφη συμφωνία για την εξωτερική ανάθεση δραστηριοτήτων νέφους περιλαμβάνει την υποχρέωση του παρόχου υπηρεσιών νέφους έχει να υποστηρίξει τη συντεταγμένη μεταβίβαση της ανατεθείσας λειτουργίας, και της σχετικής επεξεργασίας δεδομένων, από τον πάροχο υπηρεσιών νέφους και τους ενδεχόμενους υπεργολάβους του σε άλλον πάροχο υπηρεσιών νέφους που υποδεικνύει η επιχείρηση ή απευθείας στην επιχείρηση, σε περίπτωση που η επιχείρηση ενεργοποιήσει τη στρατηγική αποχώρησης. Η

υποχρέωση υποστήριξης της συντεταγμένης μεταβίβασης της ανατεθείσας λειτουργίας, και της σχετικής επεξεργασίας δεδομένων, πρέπει να περιλαμβάνει, κατά περίπτωση, την ασφαλή διαγραφή των δεδομένων από τα συστήματα του παρόχου υπηρεσιών νέφους και των ενδεχόμενων υπεργολάβων του.

31. Κατά την επεξεργασία των σχεδίων αποχώρησης και των λύσεων που αναφέρονται στα σημεία α) και β) ανωτέρω («στρατηγική αποχώρησης»), οι επιχειρήσεις πρέπει:

- α) να προσδιορίζουν τους στόχους της στρατηγικής αποχώρησης·
- β) να προσδιορίζουν τα γεγονότα που μπορούν να ενεργοποιήσουν τη στρατηγική αποχώρησης. Στα γεγονότα αυτά πρέπει οπωσδήποτε να περιλαμβάνεται η καταγγελία της συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων νέφους με πρωτοβουλία της επιχείρησης ή του παρόχου υπηρεσιών νέφους και η διακοπή ή άλλη σοβαρή διαταραχή της επιχειρησιακής δραστηριότητας του παρόχου υπηρεσιών νέφους·
- γ) να διενεργούν ανάλυση επιχειρησιακού αντικτύπου που να είναι ανάλογη της ανατεθείσας λειτουργίας προκειμένου να προσδιορίζουν τους ανθρώπινους και άλλους πόρους που απαιτούνται για να εφαρμόσουν τη στρατηγική αποχώρησης·
- δ) να αναθέτουν ρόλους και αρμοδιότητες για τη διαχείριση της στρατηγικής αποχώρησης·
- ε) να ελέγχουν την καταλληλότητα της στρατηγικής αποχώρησης ακολουθώντας προσέγγιση βάσει κινδύνων (για παράδειγμα, αναλύοντας τις ενδεχόμενες συνέπειες ως προς το κόστος, τον αντίκτυπο, τους πόρους και το χρόνο της μεταβίβασης της ανατεθείσας υπηρεσίας σε εναλλακτικό πάροχο)·
- στ) να καθορίζουν τα κριτήρια για την επιτυχή μετάβαση.

32. Οι επιχειρήσεις πρέπει να χρησιμοποιούν δείκτες για τα γεγονότα που ενεργοποιούν τη στρατηγική αποχώρησης όσο παρακολουθούν και εποπτεύουν σε συνεχή βάση τις υπηρεσίες που παρέχονται από τον πάροχο υπηρεσιών νέφους βάσει της συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων νέφους.

Κατευθυντήρια γραμμή αριθ. 6. Δικαιώματα πρόσβασης και ελέγχου

33. Οι επιχειρήσεις πρέπει να διασφαλίζουν ότι η έγγραφη συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων δεν περιορίζει τις επιχειρήσεις και τις αρμόδιες αρχές να ασκούν αποτελεσματικά τα δικαιώματα πρόσβασης και ελέγχου και τις δυνατότητες εποπτείας του παρόχου υπηρεσιών νέφους.

34. Οι επιχειρήσεις πρέπει να διασφαλίζουν ότι κατά την άσκηση των δικαιωμάτων πρόσβασης και ελέγχου (π.χ. συχνότητα ελέγχων και τομείς και υπηρεσίες που πρέπει να ελέγχονται) λαμβάνεται υπόψη αν η εξωτερική ανάθεση αφορά κρίσιμη ή σημαντική λειτουργία, καθώς και τη φύση και το μέγεθος των κινδύνων που εγκυμονεί η συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων νέφους και ο αντίκτυπός της για τις επιχειρήσεις.

35. Σε περίπτωση που η άσκηση των δικαιωμάτων πρόσβασης ή ελέγχου ή η χρήση συγκεκριμένων τεχνικών ελέγχου δημιουργεί κίνδυνο για το περιβάλλον του παρόχου υπηρεσιών νέφους και/ή άλλου πελάτη του παρόχου υπηρεσιών νέφους (επηρεάζοντας π.χ. το επίπεδο της εξυπηρέτησης, την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων), ο πάροχος υπηρεσιών νέφους

πρέπει να παρέχει σαφή εξήγηση στην επιχείρηση ως προς τους λόγους για τους οποίους οι τεχνικές αυτές δημιουργούν κίνδυνο και ο πάροχος υπηρεσιών νέφους πρέπει να έρχεται σε συμφωνία με την επιχείρηση σχετικά με εναλλακτικούς τρόπους με τους οποίους μπορεί να επιτευχθεί παρόμοιο αποτέλεσμα (π.χ. την προσθήκη ειδικών δοκιμαστικών ελέγχων σε ειδική έκθεση/πιστοποίηση που προσκομίζεται από τον πάροχο υπηρεσιών νέφους).

36. Με την επιφύλαξη της τελικής ευθύνης που αναλαμβάνουν για τις συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων νέφους και με σκοπό την αποδοτικότερη χρήση των ελεγκτικών πόρων και τη μείωση του οργανωτικού φόρτου, τόσο για τον πάροχο υπηρεσιών νέφους όσο και για τους πελάτες του, οι επιχειρήσεις μπορούν να χρησιμοποιούν:

- α) πιστοποιήσεις τρίτων και εκθέσεις εξωτερικού ή εσωτερικού ελέγχου που καθίστανται διαθέσιμες από τον πάροχο υπηρεσιών νέφους·
- β) ομαδικούς ελέγχους, οι οποίοι διενεργούνται από κοινού με άλλους πελάτες του ίδιου παρόχου υπηρεσιών νέφους ή ομαδικούς ελέγχους, οι οποίοι διενεργούνται από τρίτους που έχουν εξουσιοδοτηθεί για τον σκοπό αυτό από πολλούς πελάτες του ίδιου παρόχου υπηρεσιών νέφους.

37. Σε περίπτωση εξωτερικής ανάθεσης κρίσιμων ή σημαντικών λειτουργιών, οι επιχειρήσεις πρέπει να αξιολογούν αν οι πιστοποιήσεις τρίτων και οι εκθέσεις εξωτερικού ή εσωτερικού ελέγχου που αναφέρονται στην παράγραφο 37 στοιχείο α) είναι κατάλληλες και επαρκείς να εξασφαλίσουν τη συμμόρφωσή τους με τις υποχρεώσεις που προκύπτουν βάσει της ισχύουσας νομοθεσίας και πρέπει να επιδιώκουν να μην βασίζονται μόνο σε αυτές τις πιστοποιήσεις και εκθέσεις σε βάθος χρόνου.

38. Σε περίπτωση εξωτερικής ανάθεσης κρίσιμων ή σημαντικών λειτουργιών, οι επιχειρήσεις πρέπει να χρησιμοποιούν τις πιστοποιήσεις τρίτων και τις εκθέσεις εσωτερικού και εξωτερικού ελέγχου που αναφέρονται στην παράγραφο 37 στοιχείο α) μόνο αν:

- α) είναι πεπεισμένες ότι το αντικείμενο των πιστοποιήσεων ή των εκθέσεων ελέγχου καλύπτει τα βασικά συστήματα του παρόχου υπηρεσιών νέφους (π.χ. τις διαδικασίες, τις εφαρμογές, την υποδομή, τα κέντρα δεδομένων), τους βασικούς ελέγχους που προσδιορίζονται από την επιχείρηση και τη συμμόρφωση με τις αντίστοιχες κανονιστικές απαιτήσεις·
- β) ελέγχουν ενδελεχώς και σε τακτική βάση το περιεχόμενο των πιστοποιήσεων ή εκθέσεων ελέγχου και εξακριβώνουν ότι οι πιστοποιήσεις ή οι εκθέσεις δεν είναι παρωχημένες·
- γ) διασφαλίζουν ότι τα βασικά συστήματα και οι βασικοί έλεγχοι του παρόχου υπηρεσιών νέφους θα εξακολουθούν να καλύπτονται στις μελλοντικές εκδόσεις των πιστοποιήσεων ή των εκθέσεων ελέγχου·
- δ) είναι ικανοποιημένες με το τρίτο μέρος που διενεργεί την πιστοποίηση ή τον έλεγχο (όσον αφορά π.χ. τα προσόντα του, τις γνώσεις του, τον επαναληπτικό έλεγχο/την επαλήθευση των αποδεικτικών στοιχείων του φακέλου του αρχικού ελέγχου, καθώς και την εναλλαγή των εταιρειών ελέγχου ή πιστοποίησης)·

- ε) είναι πεπεισμένες ότι οι πιστοποιήσεις εκδίδονται και ότι οι έλεγχοι εκτελούνται σύμφωνα με τα αντίστοιχα πρότυπα και περιλαμβάνουν δοκιμή της αποτελεσματικότητας των βασικών ελέγχων που εφαρμόζονται·
- στ) έχουν το συμβατικό δικαίωμα να ζητούν την επέκταση του αντικειμένου των εκθέσεων πιστοποίησης ή ελέγχου και σε άλλα σχετικά συστήματα και ελέγχους του παρόχου υπηρεσιών νέφους· ο αριθμός και η συχνότητα τέτοιων αιτημάτων για την τροποποίηση του αντικειμένου θα πρέπει να είναι εύλογα και θεμιτά από πλευράς διαχείρισης κινδύνων·
- ζ) διατηρούν το συμβατικό δικαίωμα να διενεργούν επιμέρους επιτόπιους ελέγχους κατά τη διακριτική τους ευχέρεια σχετικά με την ανατεθείσα λειτουργία.

39. Οι επιχειρήσεις πρέπει να διασφαλίζουν ότι, πριν από τις επιτόπιες επισκέψεις, μεταξύ άλλων τις επισκέψεις τρίτων που έχουν εξουσιοδοτηθεί για τον σκοπό αυτό από τις επιχειρήσεις (π.χ. ελεγκτές), ειδοποιείται ο πάροχος υπηρεσιών νέφους εντός εύλογου χρονικού διαστήματος, εκτός αν η ειδοποίηση αυτή είναι αδύνατο να κοινοποιηθεί εγκαίρως λόγω επείγουσας ή έκτακτης ανάγκης ή γιατί θα οδηγούσε σε κατάσταση στην οποία ο έλεγχος θα έπαυε να είναι αποτελεσματικός. Η ειδοποίηση αυτή πρέπει να περιλαμβάνει την τοποθεσία, τον σκοπό της επίσκεψης, καθώς και το προσωπικό που θα συμμετάσχει στην επίσκεψη.

40. Λαμβάνοντας υπόψη ότι οι υπηρεσίες νέφους είναι πολύ περίπλοκες από τεχνική άποψη και εγείρουν συγκεκριμένες δυσκολίες σε επίπεδο δικαιοδοσίας, το προσωπικό που εκτελεί τον έλεγχο –είτε πρόκειται για εσωτερικούς ελεγκτές της επιχείρησης είτε για ελεγκτές που ενεργούν για λογαριασμό της– πρέπει να έχουν τις κατάλληλες δεξιότητες και γνώσεις για να αξιολογούν επαρκώς τις σχετικές υπηρεσίες νέφους και να εκτελούν αποτελεσματικούς και σχετικούς ελέγχους. Η απαίτηση αυτή ισχύει και για το προσωπικό των επιχειρήσεων που επανεξετάζουν τις πιστοποιήσεις ή τις εκθέσεις ελέγχων που παρέχονται από τον πάροχο υπηρεσιών νέφους.

Κατευθυντήρια γραμμή αριθ. 7. Υπεργολαβική ανάθεση

41. Αν επιτρέπεται η υπεργολαβική ανάθεση κρίσιμων ή σημαντικών λειτουργιών (ή ουσιαδών μερών τους), στην έγγραφη συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων νέφους μεταξύ της επιχείρησης και του παρόχου υπηρεσιών νέφους πρέπει:

- α) να προσδιορίζεται κάθε μέρος ή πτυχή της ανατεθείσας δραστηριότητας που εξαιρείται από τη δυνατότητα υπεργολαβικής ανάθεσης·
- β) να καθορίζονται οι προϋποθέσεις που πρέπει να πληρούνται σε περίπτωση υπεργολαβικής ανάθεσης·
- γ) να ορίζεται ότι ο πάροχος υπηρεσιών νέφους παραμένει υπόλογος και υποχρεούται να εποπτεύει τις υπηρεσίες που έχει αναθέσει με υπεργολαβία ώστε να διασφαλίζεται, σε συνεχή βάση, η εκπλήρωση όλων των συμβατικών υποχρεώσεων που προβλέπονται μεταξύ του παρόχου υπηρεσιών νέφους και της επιχείρησης·
- δ) να περιλαμβάνεται η υποχρέωση του παρόχου υπηρεσιών νέφους να ενημερώνει την επιχείρηση για οποιαδήποτε υπεργολαβική ανάθεση, ή ουσιαστικές αλλαγές,

προτίθεται να κάνει, ειδικά εάν οι αλλαγές αυτές ενδέχεται να επηρεάσουν τη δυνατότητα του παρόχου υπηρεσιών νέφους να εκπληρώνει τις υποχρεώσεις που προκύπτουν βάσει της συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων νέφους με την επιχείρηση. Το χρονικό διάστημα προειδοποίησης που ορίζεται στην έγγραφη συμφωνία πρέπει να είναι τέτοιο ώστε η επιχείρηση να έχει τη δυνατότητα να διενεργήσει την εκτίμηση κινδύνου της προτεινόμενης υπεργολαβικής ανάθεσης ή ουσιαστών αλλαγών της, και να εναντιωθεί ή να τις εγκρίνει ρητά, όπως επισημαίνεται στο σημείο ε) κατωτέρω·

- ε) να διασφαλίζεται ότι η επιχείρηση έχει το δικαίωμα εναντίωσης στη μελλοντική υπεργολαβική ανάθεση, ή στις ουσιαστικές αλλαγές της, ή ότι πρέπει να παρέχεται ρητή έγκριση πριν παράγουν αποτελέσματα η προτεινόμενη υπεργολαβική ανάθεση ή οι ουσιαστικές αλλαγές·
- στ) να διασφαλίζεται ότι η επιχείρηση έχει το συμβατικό δικαίωμα να καταγγείλει τη συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων νέφους με τον πάροχο υπηρεσιών νέφους σε περίπτωση που εναντιωθεί στην προτεινόμενη υπεργολαβική ανάθεση ή στις ουσιαστικές αλλαγές της και σε περίπτωση μη αποδεκτής υπεργολαβικής ανάθεσης (π.χ. αν ο πάροχος υπηρεσιών νέφους προβεί στην υπεργολαβική ανάθεση χωρίς να ενημερώσει την επιχείρηση ή αν παραβιάσει σοβαρά τους όρους της υπεργολαβικής ανάθεσης που ορίζονται στη συμφωνία εξωτερικής ανάθεσης).

42. Η επιχείρηση πρέπει να διασφαλίσει ότι ο πάροχος υπηρεσιών νέφους εμποτεύει επαρκώς τον υπεργολάβο.

Κατευθυντήρια γραμμή αριθ. 8. Έγγραφη κοινοποίηση στις αρμόδιες αρχές

43. Η επιχείρηση πρέπει να κοινοποιεί εγγράφως και εγκαίρως στην αρμόδια αρχή της τις προγραμματισμένες συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων νέφους που αφορούν κρίσιμη ή σημαντική λειτουργία. Η επιχείρηση πρέπει επίσης να κοινοποιεί εγκαίρως και εγγράφως στην αρμόδια αρχή της τις συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων νέφους που αφορούν λειτουργία η οποία στο παρελθόν χαρακτηριζόταν μη κρίσιμη ή μη σημαντική, αλλά στη συνέχεια έγινε κρίσιμη ή σημαντική.

44. Η έγγραφη κοινοποίηση της επιχείρησης θα πρέπει να περιλαμβάνει, λαμβάνοντας υπόψη την αρχή της αναλογικότητας, τουλάχιστον τις ακόλουθες πληροφορίες:

- α) την ημερομηνία έναρξης της συμφωνίας εξωτερικής ανάθεσης δραστηριοτήτων νέφους και, κατά περίπτωση, την επόμενη ημερομηνία ανανέωσης της σύμβασης, την ημερομηνία λήξης και/ή τα χρονικά περιθώρια προειδοποίησης για τον πάροχο των υπηρεσιών νέφους και για την επιχείρηση·
- β) συνοπτική περιγραφή της ανατεθείσας λειτουργίας·
- γ) συνοπτική παράθεση των λόγων για τους οποίους η ανατεθείσα λειτουργία θεωρείται κρίσιμη ή σημαντική·
- δ) το όνομα και την εταιρική επωνυμία (αν υπάρχει) του παρόχου υπηρεσιών νέφους, τη χώρα καταχώρισής του, τον εταιρικό αριθμό μητρώου του, τον αναγνωριστικό κωδικό της νομικής του οντότητας (αν υπάρχει), την καταστατική του έδρα, τα

- συναφή στοιχεία επικοινωνίας, καθώς και την επωνυμία της μητρικής του εταιρείας (αν υπάρχει)·
- ε) τη νομοθεσία που διέπει τη συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων νέφους και, κατά περίπτωση, τη δικαιοδοσία που έχει επιλεγεί·
 - στ) το πρότυπο ανάπτυξης υπηρεσιών νέφους και φύση των δεδομένων που θα φυλάσσονται, καθώς και τις τοποθεσίες (για την ακρίβεια τις περιφέρειες ή τις χώρες) στις οποίες θα αποθηκεύονται αυτά τα δεδομένα·
 - ζ) την ημερομηνία της τελευταίας αξιολόγησης του κρίσιμου ή σημαντικού χαρακτήρα της ανατεθείσας λειτουργίας·
 - η) την ημερομηνία της τελευταίας εκτίμησης κινδύνου/του τελευταίου ελέγχου του παρόχου υπηρεσιών νέφους, σε συνδυασμό με τη συνοπτική παρουσίαση των βασικών αποτελεσμάτων της εκτίμησης ή του ελέγχου, καθώς και την ημερομηνία της επόμενης προγραμματισμένης εκτίμησης κινδύνου ή του επόμενου προγραμματισμένου ελέγχου·
 - θ) το πρόσωπο ή το όργανο λήψης αποφάσεων εντός της επιχείρησης που ενέκρινε τη συμφωνία εξωτερικής ανάθεσης δραστηριοτήτων νέφους·
 - ι) ανάλογα με την περίπτωση, τα ονόματα των ενδεχόμενων υπεργολάβων στους οποίους ανατίθενται με υπεργολαβία ουσιώδη μέρη κρίσιμης ή σημαντικής λειτουργίας, συμπεριλαμβανομένης της χώρας ή της περιφέρειας στην οποία είναι καταχωρισμένοι οι υπεργολάβοι, στην οποία θα παρέχεται η ανατεθείσα υπηρεσία και στην οποία θα αποθηκεύονται τα δεδομένα·

Κατευθυντήρια γραμμή αριθ. 9. Εποπτεία συμφωνιών εξωτερικής ανάθεσης δραστηριοτήτων νέφους

45. Στο πλαίσιο των εποπτικών τους διαδικασιών, οι αρμόδιες αρχές πρέπει να αξιολογούν τους κινδύνους που παρουσιάζουν οι συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων νέφους. Συγκεκριμένα, η αξιολόγηση αυτή πρέπει να εστιάζει στις συμφωνίες που αφορούν εξωτερική ανάθεση κρίσιμων ή σημαντικών λειτουργιών.
46. Οι αρμόδιες αρχές θα πρέπει να εξασφαλίζουν ότι είναι σε θέση να ασκούν αποτελεσματική εποπτεία, ειδικά όταν οι επιχειρήσεις προβαίνουν σε εξωτερική ανάθεση κρίσιμων ή σημαντικών λειτουργιών που εκτελούνται εκτός της ΕΕ.
47. Οι αρμόδιες αρχές πρέπει να αξιολογούν, ακολουθώντας την προσέγγιση βάσει κινδύνων, κατά πόσον οι επιχειρήσεις:
- α) διαθέτουν τις σχετικές διαδικασίες διακυβέρνησης, διαχείρισης πόρων και λειτουργικής ικανότητας ώστε να συνάπτουν, να εφαρμόζουν και να επιβλέπουν επαρκώς και αποτελεσματικά συμφωνίες εξωτερικής ανάθεσης δραστηριοτήτων νέφους·
 - β) εντοπίζουν και διαχειρίζονται όλους τους συναφείς κινδύνους της συμφωνίας για την εξωτερική ανάθεση δραστηριοτήτων νέφους·
48. Όταν εντοπίζονται κίνδυνοι συγκέντρωσης, οι αρμόδιες αρχές πρέπει να παρακολουθούν την εξέλιξη αυτών των κινδύνων και να αξιολογούν τόσο τον αντίκτυπο

που μπορούν να έχουν οι κίνδυνοι αυτοί για τις άλλες επιχειρήσεις που εποπτεύουν, όσο και τη σταθερότητα της κεφαλαιαγοράς.