ΕΦΗΜΕΡΙΔΑ
ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ
ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

8 Οκτωβρίου 2019 | ΤΕΥΧΟΣ ΔΕΥΤΕΡΟ | Αρ. Φύλλου **3739**

ΑΠΟΦΑΣΕΙΣ

Αριθμ. 1027

Θέματα εφαρμογής και διαδικασιών του ν. 4577/2018 (Α΄ 199).

Ο ΥΠΟΥΡΓΟΣ ΕΠΙΚΡΑΤΕΙΑΣ

Έχοντας υπόψη:

1. Τις διατάξεις:

α. Του ν. 4577/2018 «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις» (Α΄ 199), όπως ισχύει, ιδίως του δεύτερου εδαφίου της παραγράφου 1 του άρθρου 4, της παραγράφου 4 του άρθρου 10 και της παραγράφου 3 του άρθρου 12,

β. της Οδηγίας (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση,

γ. του Εκτελεστικού Κανονισμού (ΕΕ) 2018/151 της Επιτροπής, της 30ής Ιανουαρίου 2018, που θεσπίζει κανόνες για την εφαρμογή της οδηγίας (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, όσον αφορά τον περαιτέρω προσδιορισμό των στοιχείων που πρέπει να λαμβάνονται υπόψη από τους παρόχους ψηφιακών υπηρεσιών για τη διαχείριση κινδύνων που απειλούν την ασφάλεια των συστημάτων δικτύου και πληροφοριών, καθώς και των παραμέτρων βάσει των οποίων καθορίζεται κατά πόσον ο αντίκτυπος συμβάντος είναι σημαντικός,

δ. του π.δ. 81/2019 «Σύσταση, συγχώνευση, μετονομασία και κατάργηση Υπουργείων και καθορισμός των αρμοδιοτήτων τους - Μεταφορά υπηρεσιών και αρμοδιοτήτων μεταξύ Υπουργείων» (Α΄ 119),

ε. του π.δ. 83/2019 «Διορισμός Αντιπροέδρου της Κυβέρνησης, Υπουργών, Αναπληρωτών Υπουργών και Υφυπουργών» (Α΄ 121 και Διορθώσεις Σφαλμάτων Α΄ 126),

στ. του π.δ. 84/2019 «Σύσταση και κατάργηση Γενικών Γραμματειών και Ειδικών Γραμματειών/Ενιαίων Διοικητικών Τομέων Υπουργείων» (Α΄ 123),

ζ. του π.δ. 82/2017 «Οργανισμός του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης» (Α΄ 117) και ιδίως το άρθρο 15.

2. Την Υ6/2019 απόφαση του Πρωθυπουργού «Ανάθεση αρμοδιοτήτων στον Υπουργό Επικρατείας» (Β΄ 2902).

3. Την από 3.10.2019 Εισήγηση της Διεύθυνσης Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης.

4. Τη διαπίστωση της ανάγκης προς την κατεύθυνση της θέσπισης κανόνων για την επίτευξη υψηλού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών.

5. Το γεγονός ότι από την παρούσα δεν προκαλείται δαπάνη σε βάρος του κρατικού προϋπολογισμού, αποφασίζουμε:

Την έκδοση της παρούσας, οι διατάξεις της οποίας έχουν ως ακολούθως:

Α. ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1
Σκοπός

Σκοπός της παρούσας είναι η έκδοση των βασικών απαιτήσεων ασφαλείας συστημάτων δικτύου και πληροφοριών, της διαδικασίας παροχής πληροφοριών και κοινοποίησης συμβάντων ασφάλειας στις αρμόδιες Αρχές, η μεθοδολογία προσδιορισμού των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών (Φ.Ε.Β.Υ.) καθώς και η μεθοδολογία αξιολόγησης και ελέγχου, σύμφωνα με τις προβλέψεις της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Ιουλίου 2016 (ΕΕ L 194), του Εκτελεστικού Κανονισμού (ΕΕ) 2018/151 της Επιτροπής της 30ης Ιανουαρίου 2018 και του ν. 4577/2018 (Α΄ 199), ο οποίος κατ' εφαρμογή της ως άνω Οδηγίας θεσπίζει μέτρα για την επίτευξη υψηλού επιπέδου ασφάλειας των συστημάτων αυτών.

Άρθρο 2
Γενικοί Όροι και Υποχρεώσεις

1. Κάθε ΦΕΒΥ ή Πάροχος Ψηφιακών Υπηρεσιών (ΠΨΥ), εφεξής «ο Οργανισμός», οφείλει να λαμβάνει όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την ικανοποίηση του σκοπού της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Ιουλίου 2016 (ΕΕ L 194), του Εκτελεστικού Κανονισμού (ΕΕ) 2018/151 της Επιτροπής της 30ης Ιανουαρίου 2018 και του ν. 4577/2018 (Α΄ 199).

2. Κάθε Οργανισμός ευθύνεται για το σύνολο των πράξεων οποιουδήποτε συνεργάτη, φυσικού ή νομικού προσώπου, που χρησιμοποιεί για την κατασκευή, εγκατάσταση, συντήρηση ή λειτουργία των συστη-

μάτων δικτύου και πληροφοριών του για την παροχή των βασικών υπηρεσιών του. Ο Οργανισμός οφείλει να ενημερώνει προσηκόντως τους συνεργάτες του σχετικά με τα τηρούμενα μέτρα για την Ασφάλεια Συστημάτων Δικτύου και Πληροφοριών, λαμβάνοντας υπόψη τη φύση της παρεχόμενης εργασίας, και να απαιτεί την αποδοχή, εκ μέρους τους, της υποχρέωσης τήρησης αυτών.

3. Σε περιπτώσεις εκδήλωσης περιστατικού ασφάλειας, κάθε Οργανισμός οφείλει να συνεργάζεται κατά τις διατάξεις του ν. 4577/2018 (Α΄ 199), με τις Αρμόδιες Αρχές, και να εφαρμόζει τις προβλεπόμενες διαδικασίες προς άμεση επίλυση του περιστατικού και περιορισμό του αντίκτυπου αυτού.

Άρθρο 3
Ενιαία Πολιτική Ασφάλειας

1. Στο πλαίσιο τήρησης ενός ενιαίου ελάχιστου βασικού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών, η Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ) ορίζει τις απαιτήσεις για την εφαρμογή μιας Ενιαίας Πολιτικής Ασφάλειας. Κάθε Οργανισμός θεσπίζει, υλοποιεί και διατηρεί επίκαιρη και καταγεγραμμένη Πολιτική Ασφαλείας σχετική με την ασφάλεια των συστημάτων δικτύου και πληροφοριών, τα οποία υποστηρίζουν την παροχή βασικών υπηρεσιών του φορέα. Η Πολιτική Ασφάλειας του Οργανισμού οφείλει να καλύπτει τουλάχιστον όσα ορίζει η Ενιαία Πολιτική Ασφάλειας. Ειδικότερα ορίζεται ότι:

α. Η Πολιτική Ασφάλειας, οφείλει μεταξύ άλλων να ορίζει τους στόχους ασφάλειας, να περιγράφει τη διακυβέρνηση και να παραπέμπει σε άλλες συμπληρωματικές πολιτικές, σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών του Οργανισμού.

β. Βασικοί στόχοι της Πολιτικής Ασφάλειας είναι:

• η διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων, συστημάτων και υπηρεσιών έναντι εκούσιων ή ακούσιων απειλών

• η ικανοποίηση των νομικών και κανονιστικών απαιτήσεων σχετικών με την ασφάλεια και προστασία δεδομένων

• η επιχειρησιακή συνέχεια των βασικών υπηρεσιών του Οργανισμού έναντι περιστατικών κυβερνοεπιθέσεων

• η ενημέρωση και η εκπαίδευση όλων των υπαλλήλων και λοιπών εμπλεκομένων τρίτων σχετικά με την παροχή των βασικών υπηρεσιών του Οργανισμού

• η άμεση κοινοποίηση και διαχείριση περιστατικών ή αδυναμιών ασφαλείας.

γ. Αρμόδιοι για την εφαρμογή της Πολιτικής Ασφάλειας, είναι:

• η Διοίκηση του Οργανισμού, η οποία εγκρίνει, αναθεωρεί και είναι αρμόδια για την αποτελεσματική και αποδοτική εφαρμογή της Πολιτικής Ασφάλειας.

• ο Υπεύθυνος Ασφάλειας Πληροφοριών και Δικτύων, όπως περιγράφεται στο άρθρο 6 της παρούσας, ο οποίος επιβλέπει και συντονίζει την εφαρμογή αυτής της πολιτικής μέσω χρήσης κατάλληλων προτύπων, διαδικασιών και διεθνών πρακτικών και λειτουργεί ως σημείο επαφής με τους αρμόδιους φορείς

• όλο το προσωπικό και οι συμβεβλημένοι προμηθευτές, οι οποίοι ακολουθούν τις διαδικασίες για την τήρηση της πολιτικής ασφάλειας πληροφοριών.

δ. Η Πολιτική Ασφάλειας θα πρέπει να λαμβάνει μέριμνα για την τήρηση των «Βασικών Απαιτήσεων Ασφάλειας», όπως αυτές ισχύουν και ορίζονται από την Εθνική Αρχή Κυβερνοασφάλειας.

Άρθρο 4
Βασικές Απαιτήσεις Ασφάλειας

Α. ΑΝΑΓΝΩΡΙΣΗ

Οι απαιτήσεις της κατηγορίας «Αναγνώριση» είναι απαραίτητες για την κατανόηση του επιχειρηματικού πλαισίου, των πόρων που υποστηρίζουν τις βασικές υπηρεσίες και την σχετική διακινδύνευση για την ασφάλεια των συστημάτων δικτύου και πληροφοριών και επιτρέπουν στον Οργανισμό να εστιάσει τις προσπάθειές του και να διαχειριστεί τους πόρους του, με αποτελεσματικό και αποδοτικό τρόπο. Ειδικότερα θα πρέπει να πληρούνται οι κάτωθι απαιτήσεις.

1. Επιχειρησιακό περιβάλλον

Η αποστολή, οι στόχοι, τα ενδιαφερόμενα μέρη, οι δραστηριότητες και οι λοιπές απαιτήσεις (κανονιστικές, νομικές, περιβαλλοντικές, συμβατικές και λειτουργικές) του Οργανισμού που σχετίζονται με τις βασικές του υπηρεσίες, εντοπίζονται και καταγράφονται.

Αυτές οι πληροφορίες χρησιμοποιούνται ως βάση κατά τη διεργασία διαχείρισης διακινδύνευσης σε όλα τα σχετικά στάδια (καθορισμός απαιτήσεων, αναγνώριση, ανάλυση, αποτίμηση και αντιμετώπιση διακινδύνευσης).

2. Διαχείριση πόρων.

Όλοι οι πόροι που απαιτούνται για την παροχή ή υποστήριξη βασικών υπηρεσιών του Οργανισμού θα πρέπει να αναγνωρίζονται, να αναλύονται και να καταγράφονται σε κατάλληλο και ενημερωμένο κατάλογο. Αυτός περιλαμβάνει ενδεικτικά, μεταξύ άλλων, δεδομένα, προσωπικό, δομικά στοιχεία, συσκευές, συστήματα, εγκαταστάσεις, προμηθευτές, διαδικασίες, οδηγούς χρήσης, διαμορφώσεις κ.α.

3. Αποτίμηση διακινδύνευσης

Η διακινδύνευση για την ασφάλεια των συστημάτων δικτύου και πληροφοριών αναγνωρίζεται, αναλύεται και αποτιμάται μέσω κατάλληλης, τεκμηριωμένης και αποτελεσματικής διεργασίας.

4. Στρατηγική διαχείρισης διακινδύνευσης

Καθορίζονται οι προτεραιότητες, περιορισμοί, ανοχές διακινδύνευσης και λοιπές παραδοχές οι οποίες χρησιμοποιούνται για την αιτιολόγηση των αποφάσεων σχετικά με τα επιλεγόμενα μέτρα διαχείρισης και μετριασμού της διακινδύνευσης για την ασφάλεια των συστημάτων δικτύου και πληροφοριών.

5. Διαχείριση διακινδύνευσης αλυσίδας εφοδιασμού

Η διακινδύνευση που αφορά στην αλυσίδα εφοδιασμού (προμηθευτές υλικού ή υπηρεσιών) εντοπίζεται, αξιολογείται και μετριάζεται. Ειδικότερα διασφαλίζεται, μέσω Συμφωνιών Επιπέδου Υπηρεσιών (Service Level Agreements - SLA) ή/και επιθεωρήσεις, ότι οι προμηθευτές εφαρμόζουν κατάλληλα και αναλογικά μέτρα ασφάλειας.

6. Αυτοαξιολόγηση - Βελτίωση

Για την παρακολούθηση και συνεχή βελτίωση της ασφάλειας των συστημάτων δικτύου και πληροφοριών, συντάσσεται αναφορά αυτοαξιολόγησης συνοδευόμενης και από σχετικό πλάνο διορθωτικών ή βελτιωτικών ενεργειών, τα οποία κοινοποιούνται στην Εθνική Αρχή Κυβερνοασφάλειας.

Η αυτοαξιολόγηση διενεργείται σε ετήσια βάση ή κατόπιν πρόκλησης σοβαρής διατάραξης της παροχής βασικής υπηρεσίας από τυχόν συμβάν, με τη χρήση κατάλληλου Οδηγού που εκδίδει και αναθεωρεί η Εθνική Αρχή Κυβερνοασφάλειας.

Β. ΠΡΟΣΤΑΣΙΑ

Οι απαιτήσεις της κατηγορίας «Προστασία» είναι απαραίτητες προκειμένου να διασφαλιστούν όλοι οι πόροι (άνθρωποι, διαδικασίες και τεχνολογίες) που υποστηρίζουν τις βασικές υπηρεσίες του Οργανισμού. Τα μέτρα που επιλέγονται για την ικανοποίηση των απαιτήσεων αυτής της κατηγορίας, θα πρέπει να λαμβάνουν υπόψη την στρατηγική διαχείρισης διακινδύνευσης. Ειδικότερα θα πρέπει να πληρούνται οι κάτωθι απαιτήσεις.

7. Πολιτικές, διεργασίες και διαδικασίες προστασίας βασικών υπηρεσιών.

Η συνολική οργανωτική προσέγγιση για την διασφάλιση των συστημάτων δικτύου και πληροφοριών που υποστηρίζουν την παροχή βασικών υπηρεσιών του Οργανισμού, καθορίζεται και τεκμηριώνεται μέσω κατάλληλων πολιτικών, διεργασιών και διαδικασιών.

Ειδικότερα, η πολιτική ασφάλειας του Οργανισμού θα πρέπει να είναι συμβατή και να ικανοποιεί κατ’ ελάχιστο την Ενιαία Πολιτική Ασφάλειας και τις απαιτήσεις ασφάλειας που εκδίδει η Εθνική Αρχή Κυβερνοασφάλειας.

8. Διαχείριση ταυτότητας και έλεγχος πρόσβασης.

Η πρόσβαση (φυσική ή με ηλεκτρονικά μέσα) στα συστήματα δικτύου και πληροφοριών και στις συναφείς εγκαταστάσεις, περιορίζεται στους εξουσιοδοτημένους προς τούτο χρήστες, διεργασίες και συσκευές, σύμφωνα με την αρχή των λιγότερων προνομίων και διαχειρίζεται αναλογικά και σύμφωνα με την εκτιμώμενη διακινδύνευση. Για το σκοπό αυτό γίνεται χρήση κατάλληλων μηχανισμών αυθεντικοποίησης και διαδικασιών ελέγχου πρόσβασης.

9. Φυσική και περιβαλλοντική ασφάλεια.

Οι εγκαταστάσεις των κέντρων δεδομένων και των χώρων επεξεργασίας πληροφοριών διασφαλίζονται έναντι δυνητικής φυσικής ή περιβαλλοντικής διακινδύνευσης μέσω κατάλληλων και αναλογικών πολιτικών και μέτρων και σύμφωνα με τη στρατηγική διαχείρισης διακινδύνευσης.

10. Ασφάλεια συστημάτων και εφαρμογών.

Τα συστήματα και οι εφαρμογές εγκαθίστανται, αναπτύσσονται και διαχειρίζονται με τρόπο που λαμβάνει υπόψη τις αρχές της ασφάλειας «από τον σχεδιασμό» και «εξ ορισμού», και τηρούνται κατάλληλες και αναλογικές απαιτήσεις ασφάλειας σε όλο τον κύκλο της ζωής τους.

11. Ασφάλεια δεδομένων.

Τα δεδομένα διαχειρίζονται σύμφωνα με τη στρατηγική διαχείρισης διακινδύνευσης με σκοπό την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητάς τους. Για το σκοπό αυτό εφαρμόζονται κατάλληλες πολιτικές και διαδικασίες.

12. Αντίγραφα ασφαλείας.

Τα δεδομένα τα οποία είναι απαραίτητα για την παροχή των βασικών υπηρεσιών διασφαλίζονται από πιθανή απώλειά τους μέσω της τήρησης αντιγράφων ασφαλείας σε κατάλληλη μορφή, η οποία δίνει τη δυνατότητα για άμεση ανάκτησή τους. Για το σκοπό αυτό εφαρμόζονται κατάλληλες πολιτικές, διαδικασίες και αυτοματοποιημένα συστήματα λήψης και διατήρησης αντιγράφων ασφαλείας.

13. Τεχνολογίες ασφάλειας.

Για την διασφάλιση της ανθεκτικότητας των συστημάτων έναντι απειλών εγκαθίστανται και χρησιμοποιούνται κατάλληλες και αναλογικές προς το σκοπό αυτό τεχνολογικές λύσεις ασφαλείας. Ειδικότερα, ενθαρρύνεται η χρήση τεχνολογικών λύσεων σχετικά με ανίχνευση, καταγραφή και ανάλυση απειλών.

14. Δοκιμές συστημάτων.

Για την διασφάλιση της ανθεκτικότητας των συστημάτων που υποστηρίζουν βασικές υπηρεσίες έναντι απειλών, εφαρμόζονται κατάλληλες διαδικασίες δοκιμών και τεχνικών ελέγχων.

15. Διαχείριση Αλλαγών.

Οι αλλαγές που γίνονται στα συστήματα και τα δομικά στοιχεία που υποστηρίζουν βασικές υπηρεσίες ακολουθούν συγκεκριμένη και καταγεγραμμένη διαδικασία, ώστε να διατηρείται το επίπεδο διακινδύνευσης εντός των ορίων που καθορίζονται στη στρατηγική διαχείρισης διακινδύνευσης και να λαμβάνονται πρόσθετα μέτρα ασφάλειας όταν αυτό απαιτείται.

16. Ευαισθητοποίηση και κατάρτιση.

Το προσωπικό και οι συνεργάτες οι οποίοι χειρίζονται ή υποστηρίζουν τα συστήματα πληροφοριών και δικτύων ενημερώνονται και εκπαιδεύονται κατάλληλα, ώστε να εκπληρώνουν τα καθήκοντά τους με τρόπο που να διατηρεί και να προάγει την ασφάλεια των συστημάτων αυτών. Για το σκοπό αυτό εφαρμόζεται κατάλληλη πολιτική σχετικά με τη διενέργεια ή συμμετοχή σε τακτικά προγράμματα και δράσεις ευαισθητοποίησης ή εκπαίδευσης.

Γ. ΑΝΤΙΜΕΤΩΠΙΣΗ

Οι απαιτήσεις της κατηγορίας «Αντιμετώπιση» είναι απαραίτητες για την ανίχνευση, την απόκριση, και την εν γένει διαχείριση ενός συμβάντος ασφάλειας που ενδέχεται να επηρεάσει την παροχή βασικών υπηρεσιών του Οργανισμού. Παράλληλα αυτή η κατηγορία προωθεί τη μείωση του αντίκτυπου από ένα περιστατικό ασφάλειας, μέσω της διασφάλισης της συνέχειας και της αποκατάστασης της παροχής βασικών υπηρεσιών του Οργανισμού σε αποδεκτό και προκαθορισμένο επίπεδο.

17. Ανίχνευση απειλών.

Οι απειλές και τα συμβάντα που δύναται να επηρεάσουν την ασφάλεια των συστημάτων δικτύου και πληροφοριών ανιχνεύονται έγκαιρα μέσω κατάλληλων τεχνολογικών λύσεων ασφάλειας ή σχετικών διαδικασιών.

18. Διαχείριση Περιστατικών.

Η έγκαιρη ανταπόκριση, ανάλυση και διαχείριση περιστατικών ασφαλείας με πραγματικές ή δυνητικές

δυσμενείς επιπτώσεις θα πρέπει να διενεργείται βάσει κατάλληλης πολιτικής και σύμφωνα με προκαθορισμένη διαδικασία.

Ειδικότερα στην περίπτωση που αυτά αξιολογούνται ως κρίσιμα, θα πρέπει να ενημερώνονται οι αρμόδιες ομάδες αντιμετώπισης (CSIRTs ή CERTs), η Εθνική Αρχή Κυβερνοασφάλειας και οι λοιποί εμπλεκόμενοι φορείς και να διευκολύνεται η συνεργασία και η παροχή πληροφοριών, σύμφωνα και με όσα ορίζονται στο ν. 4577/2018 (Α΄ 199), όπως αυτός ισχύει.

19. Επιχειρησιακή συνέχεια.

Διασφαλίζεται η δυνατότητα παροχής των βασικών υπηρεσιών του Οργανισμού, σε αποδεκτό και προσυμφωνημένο επίπεδο, σε περίπτωση που έχει εκδηλωθεί κάποιο περιστατικό ασφάλειας. Για το σκοπό αυτό διερευνώνται εναλλακτικοί τρόποι παροχής των υπηρεσιών, λαμβάνονται κατάλληλα οργανωτικά και τεχνικά μέτρα και καταρτίζεται σχετικό, καταγεγραμμένο και προκαθορισμένο σχέδιο.

20. Ανάκαμψη από καταστροφές.

Διασφαλίζεται η ανάκαμψη και αποκατάσταση των συστημάτων δικτύου και πληροφοριών των βασικών υπηρεσιών του Οργανισμού, τα οποία επηρεάζονται από περιστατικά ασφάλειας, εντός προκαθορισμένου και αποδεκτού χρονικού διαστήματος. Για το σκοπό αυτό λαμβάνονται κατάλληλα οργανωτικά και τεχνικά μέτρα και καταρτίζεται σχετικό, καταγεγραμμένο και προκαθορισμένο σχέδιο.

Άρθρο 5
Επιλογή μέτρων ασφάλειας

1. Οι Οργανισμοί κατά την επιλογή των μέτρων ασφαλείας θα πρέπει να λαμβάνουν μέριμνα ώστε αυτά να είναι:

• Αποτελεσματικά, ώστε να αυξάνουν το επίπεδο ετοιμότητας του Οργανισμού έναντι τωρινών και μελλοντικών απειλών ασφάλειας.

• Αποδοτικά, ώστε να επιλέγονται αυτά τα οποία θα έχουν το μεγαλύτερο αντίκτυπο στην ενίσχυση της ασφάλειας ενός Οργανισμού, σε σχέση με τις απαιτήσεις κτήσης και διατήρησής τους.

• Κατάλληλα, ώστε να είναι συμβατά και να διευκολύνουν τη παροχή των βασικών υπηρεσιών του Οργανισμού.

• Αναλογικά, ώστε να επιλέγονται συναρτήσει του εκάστοτε επιπέδου επικινδυνότητας.

• Συγκεκριμένα, ώστε να διασφαλίζεται ότι τα μέτρα θα εφαρμόζονται στην πράξη και θα ενισχύουν ενεργά το επίπεδο ασφάλειας.

• Αξιόπιστα, ώστε να παρέχουν δείκτες και αποδείξεις για την αποτελεσματική και αποδοτική εφαρμογή τους.

• Περιεκτικά, ώστε η εφαρμογή τους να καλύπτει όσες περισσότερες βασικές απαιτήσεις ασφάλειας είναι δυνατό.

2. Προκειμένου να επιλεγούν και να εφαρμοστούν μέτρα που ικανοποιούν τις βασικές απαιτήσεις ασφάλειας, ενθαρρύνεται η χρήση διεθνώς αποδεκτών προτύπων, προδιαγραφών και οδηγών που σχετίζονται με την ασφάλεια των συστημάτων δικτύων και πληροφοριών.

Άρθρο 6
Υπεύθυνος Ασφάλειας Πληροφοριών και Δικτύων

Κάθε Οργανισμός οφείλει να ορίσει συγκεκριμένο εργαζόμενο του ως Υπεύθυνο Ασφάλειας Πληροφοριών και Δικτύων του.

Ο Υπεύθυνος Ασφάλειας Πληροφοριών και Δικτύων:

• Αποτελεί το σημείο επαφής με την Εθνική Αρχή Κυβερνοασφάλειας και το αρμόδιο CSIRT.

• Συνεργάζεται με την Εθνική Αρχή Κυβερνοασφάλειας και με το αρμόδιο CSIRT.

• Συντονίζει και επιβλέπει τον Οργανισμό ως προς τις υποχρεώσεις που απορρέουν από τον ν. 4577/2018 (Α΄ 199), από την παρούσα υπουργική απόφαση και από άλλες διατάξεις της Ευρωπαϊκής Ένωσης ή της Εθνικής Αρχής Κυβερνοασφάλειας σχετικά με την Ασφάλεια Συστημάτων Δικτύων και Πληροφοριών.

• Εποπτεύει την υλοποίηση της Ενιαίας Πολιτικής Ασφάλειας και την ικανοποίηση των βασικών απαιτήσεων ασφάλειας, την εκπαίδευση και ευαισθητοποίηση των υπαλλήλων του Οργανισμού σε θέματα ασφάλειας πληροφοριών και δικτύων καθώς, και τη σύνταξη της αναφοράς αυτοαξιολόγησης του Οργανισμού που αποστέλλεται στην Εθνική Αρχή Κυβερνοσφάλειας.

• Παρίσταται στους ελέγχους που πραγματοποιεί η Ομάδα Επιθεώρησης Ελέγχου, όπως αυτή ορίζεται από την Εθνική Αρχή Κυβερνοσφάλειας, και της παρέχει όλα τα κατάλληλα μέσα για να διευκολύνει το έργο της.

Ο ρόλος του στην οργανωτική δομή του Οργανισμού προτείνεται να είναι ανεξάρτητος και να μην έγκειται σε σύγκρουση συμφερόντων με άλλους εργασιακούς ρόλους που τυχόν κατέχει.

Κάθε Οργανισμός οφείλει αμελλητί να κοινοποιεί στην Εθνική Αρχή Κυβερνοασφάλειας τα στοιχεία επικοινωνίας του εκάστοτε Υπευθύνου που έχει οριστεί και το αργότερο εντός 2 μηνών από την έκδοση της παρούσας υπουργικής απόφασης.

Επιθυμητά προσόντα του Υπεύθυνου Ασφάλειας Πληροφοριών και Δικτύων:

• Να διαθέτει προπτυχιακό ή Μεταπτυχιακό τίτλο ετήσιας τουλάχιστον διάρκειας σε συναφές γνωστικό αντικείμενο.

• Να διαθέτει εμπειρογνωσία στον τομέα της ασφάλειας πληροφοριών και δικτύων τουλάχιστον 5 ετών.

• Να διαθέτει πιστοποιημένη γνώση μεθοδολογιών, διαδικασιών, τεχνικών, εργαλείων και προτύπων ασφάλειας πληροφοριών και ψηφιακών συστημάτων.

• Να γνωρίζει τις επιχειρηματικές διαδικασίες του Οργανισμού.

Β. ΔΙΑΔΙΚΑΣΙΑ ΚΟΙΝΟΠΟΙΗΣΗΣ ΣΥΜΒΑΝΤΩΝ ΑΣΦΑΛΕΙΑΣ

Άρθρο 7
Κριτήρια προσδιορισμού ενός συμβάντος ως σοβαρής διατάραξης για τους φορείς εκμετάλλευσης βασικών υπηρεσιών

1. Σοβαρή διατάραξη, θεωρείται οποιοδήποτε συμβάν με επίπτωση στην ασφάλεια συστημάτων δικτύου

και πληροφοριών, σε συνδυασμό με τους παράγοντες της περίπτωσης 2 του άρθρου 5 του ν. 4577/2018 (Α΄ 199) και ειδικότερα όταν πληροί τουλάχιστον μία από τις ακόλουθες συνθήκες:

α) Κάθε συμβάν κατά το οποίο η συνέχεια της υπηρεσίας που παρέχεται από τον φορέα επηρεάζεται για πάνω από 100.000 χρηστοώρες. Ως συνέχεια της υπηρεσίας ορίζεται η δυνατότητα παροχής της υπηρεσίας σε αποδεκτά επίπεδα εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας και αυθεντικότητας.

β) Κάθε συμβάν που επηρεάζει πληθυσμό τουλάχιστον 50.000 χρηστών.

γ) Απειλή σε ανθρώπινη ζωή. Σε περίπτωση απώλειας ανθρώπινης ζωής το συμβάν κρίνεται αυτομάτως κοινοποιήσιμο.

δ) Το συμβάν έχει προκαλέσει υλικές ζημιές στον ίδιο τον φορέα ή σε άλλους φορείς που υπερβαίνουν το 1.000.000 ευρώ.

Άρθρο 8
Κριτήρια προσδιορισμού ενός συμβάντος ως σοβαρής διατάραξης για τους παρόχους ψηφιακών υπηρεσιών

Σοβαρή διατάραξη, θεωρείται οποιοδήποτε συμβάν πληροί μία από τις καταστάσεις, όπως αυτές ορίζονται στο άρθρο 4 του Εκτελεστικού Κανονισμού (ΕΕ) 2018/151.

Άρθρο 9
Διαδικασία Κοινοποίησης Συμβάντος Ασφάλειας

1. Κάθε Οργανισμός κοινοποιεί στο αρμόδιο CSIRT και στην Εθνική Αρχή Κυβερνοασφάλειας χωρίς αδικαιολόγητη καθυστέρηση κάθε συμβάν που έχει αντίκτυπο στη συνεχή παροχή της υπηρεσίας που προσφέρει.

2. Η αρχική αναφορά παρέχεται στην Αρχή:

α) ηλεκτρονικά ή εγγράφως, στον τύπο που θέτει σχετικό πρότυπο της Αρχής.

β) Σε εύλογο χρόνο και, σε κάθε περίπτωση, εντός 24 ωρών αφότου ο Οργανισμός έλαβε γνώση του περιστατικού.

γ) Ειδικά στην περίπτωση που το συμβάν προσδιορίζεται ως σοβαρή διατάραξη, σύμφωνα με το άρθρο 7 και άρθρο 8 της παρούσης, ο Οργανισμός υποχρεούται να υποβάλει την αρχική αναφορά χωρίς αδικαιολόγητη καθυστέρηση.

3. Η κοινοποίηση πρέπει να περιέχει τουλάχιστον τις ακόλουθες πληροφορίες:

α) Το όνομα ή την επωνυμία του φορέα καθώς και το είδος των υπηρεσιών που παρέχει. Το όνομα του νόμιμου εκπροσώπου του Οργανισμού και του Υπεύθυνου Ασφάλειας Πληροφοριών και Δικτύων.

β) Τον χρόνο, κατά τον οποίο διαγνώστηκε το συμβάν.

γ) Την ακριβή διάρκεια του περιστατικού, από τη στιγμή που διαγνώστηκε μέχρι την πλήρη αντιμετώπισή του, εάν αυτό θεωρείται λήξαν.

δ) Πληροφορίες για τη φύση του συμβάντος, καθώς και μία πρώτη εκτίμηση του αντίκτυπου του βάσει των προαναφερθέντων στοιχείων προσδιορισμού αντίκτυπου.

ε) Πληροφορίες για τις ενέργειες που ακολουθήθηκαν και τα μέτρα περιορισμού του αντίκτυπου του συμβάντος που έχουν ήδη ληφθεί.

στ) Πληροφορίες σχετικά με την πιθανότητα επηρεασμού περισσοτέρων κρατών - μελών από το συμβάν.

ζ) Οποιαδήποτε άλλη πληροφορία κρίνεται ότι θα βοηθούσε το έργο των αρμόδιων Αρχών.

4. Σε περίπτωση που μεταβληθούν ουσιωδώς τα στοιχεία του συμβάντος, ο Οργανισμός δύναται να υποβάλει επικαιροποιημένη αναφορά, με την οποία θα παρέχει όσο το δυνατόν περισσότερες πληροφορίες σχετικά με αυτό.

5. Η τελική αναφορά παρέχεται στην Αρχή:

α) εγγράφως, στον τύπο που τάσσει σχετικό πρότυπο της Αρχής

β) εντός ενός (1) μήνα από την ημερομηνία κλεισίματος του συμβάντος ασφαλείας.

γ) Περιλαμβάνει όλα τα υπό παρ. 2 στοιχεία στην τελική τους μορφή, όπως αυτά περιλαμβάνονται στην Φόρμα Αναφοράς Συμβάντος Κυβερνοασφάλειας που εκδίδει η Αρχή και είναι διαθέσιμη στην ιστοσελίδα της.

Άρθρο 10
Ενέργειες των αρμόδιων Αρχών μετά την Κοινοποίηση

1. Μετά τη λήψη της αρχικής αναφοράς:

α) οι αρμόδιες Αρχές αξιολογούν το συμβάν και αποφασίζουν για τις άμεσες ενέργειες στις οποίες θα προβούν.

β) Σε περίπτωση που το συμβάν έχει σοβαρό αντίκτυπο στη συνέχιση ουσιώδους υπηρεσίας και σε άλλο κράτος-μέλος, οι αρμόδιες Αρχές ενημερώνουν χωρίς καθυστέρηση τις αρμόδιες αρχές του κράτους-μέλους.

2. Μετά τη λήψη της τελικής αναφοράς:

α) Οι αρμόδιες Αρχές αξιολογούν τα στοιχεία, ενημερώνουν τον Οργανισμό σχετικά με την αποτελεσματικότητα της διαχείρισης του συμβάντος και παρέχουν οδηγίες για την αποτροπή ή την καλύτερη διαχείριση μελλοντικών αντίστοιχων συμβάντων.

β) Η Εθνική Αρχή Κυβερνοασφάλειας, λαμβάνοντας υπόψη και τα ευρήματα των προηγουμένως διενεργηθέντων ελέγχων των Αρ. 12 και 13 της παρούσης, αξιολογεί την πιθανότητα κλήσης προς ακρόαση καθώς και επιβολής άλλων πιθανών διοικητικών κυρώσεων.

Άρθρο 11
Ενημέρωση του Κοινού

1. Κατόπιν διαβούλευσης με τον Οργανισμό, και όταν αυτό κρίνεται απαραίτητο για την καλύτερη διαχείριση του συμβάντος, η ΕΑΚ μεριμνά για την ενημέρωση του κοινού που απολαμβάνει την υπηρεσία που επηρεάστηκε από το συμβάν σχετικά με την ύπαρξή του, την αντιμετώπισή του και την πιθανή διατάραξη της ομαλής λειτουργίας την οποία υπέστησαν.

2. Η ενημέρωση του κοινού δεν ενδείκνυται όταν:

α) αφορά ευαίσθητες ή διαβαθμισμένες πληροφορίες

β) επηρεάζει δυσανάλογα τα έννομα συμφέροντα του Οργανισμού.

Σε περίπτωση που η ΕΑΚ κρίνει ότι δεν συντρέχουν οι λόγοι (α) και (β) μπορεί να ενημερώσει το κοινό κρίνοντας κατά περίπτωση και αναλογικά.

Γ. ΔΙΑΔΙΚΑΣΙΑ ΕΛΕΓΧΟΥ

Άρθρο 12
Έλεγχοι της Εθνικής Αρχής Κυβερνοασφάλειας

1. Η Εθνική Αρχή Κυβερνοασφάλειας δύναται να ενεργεί ελέγχους, στις εγκαταστάσεις, στον τεχνικό εξοπλισμό και στις τεχνολογικές υποδομές του Οργανισμού. Οι έλεγχοι διενεργούνται είτε σε τακτική βάση ή εκτάκτως.

2. Κάθε έλεγχος, τακτικός ή έκτακτος, διενεργείται από Ομάδα Επιθεώρησης Ελέγχου την οποία ορίζει και εξουσιοδοτεί η Εθνική Αρχή Κυβερνοασφάλειας, με την παρουσία του Υπεύθυνου Ασφάλειας Πληροφοριών και Δικτύων ή άλλου εξουσιοδοτημένου προς τούτο εργαζόμενου του ελεγχόμενου Οργανισμού.

3. Σε περίπτωση τακτικού ελέγχου ενημερώνεται ο Οργανισμός για την ημερομηνία διενέργειάς του. Η Ομάδα Επιθεώρησης Ελέγχου δύναται να ζητήσει να υπάρχουν διαθέσιμα πλήρη αντίγραφα των υφισταμένων Πολιτικών και των διαδικασιών για την ασφάλεια συστημάτων δικτύου και πληροφοριών. Η ενημέρωση θα πρέπει να έχει γίνει δεκαπέντε (15) ημέρες τουλάχιστον πριν τον έλεγχο.

4. Οι έκτακτοι έλεγχοι δύνανται να διενεργούνται αυτεπαγγέλτως ή κατόπιν έγγραφης αναφοράς/κοινοποίησης συμβάντος ασφάλειας, χωρίς προηγούμενη ενημέρωση του ελεγχόμενου υπόχρεου Οργανισμού.

5. Κατά τη διαδικασία του ελέγχου η Ομάδα Επιθεώρησης Ελέγχου μπορεί να ζητήσει πρόσβαση σε πάσης φύσεως εξοπλισμό, αρχεία, βιβλία, δεδομένα και λοιπά στοιχεία, να διενεργεί έρευνες στα γραφεία και λοιπές εγκαταστάσεις του Οργανισμού, να λαμβάνει ένορκες και ανωμοτί κατά την κρίση της καταθέσεις, με την επιφύλαξη του άρθρου 212 του Κώδικα Ποινικής Δικονομίας, για τη συλλογή κάθε πληροφορίας που εξυπηρετεί τους σκοπούς του ελέγχου.

6. Η Ομάδα Επιθεώρησης Ελέγχου, προβαίνει, όποτε απαιτείται, στην προσωρινή δέσμευση εξοπλισμού συστημάτων δικτύων και πληροφοριών, εάν κατά τη διενέργεια του ελέγχου, ειδικά εφόσον έχει προηγηθεί συμβάν ασφάλειας, διαπιστωθεί ότι τα τελευταία χρήζουν περαιτέρω εξέτασης προκειμένου να εξακριβωθεί η λειτουργικότητα και η ακεραιότητά τους.

7. Η Ομάδα Επιθεώρησης Ελέγχου προβαίνει σε έλεγχο στις εγκαταστάσεις του υπόχρεου Οργανισμού κατά τα ως άνω οριζόμενα, προκειμένου να διαπιστωθεί εάν συμμορφώνεται με τις επιταγές του ν. 4577/2018 (Α΄ 199) και των οριζόμενων στην παρούσα απόφαση. Για κάθε επιτόπιο έλεγχο συντάσσεται ειδικό έγγραφο με τίτλο «Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις του υπόχρεου Οργανισμού», το οποίο συνυπογράφεται από τον Υπεύθυνο Ασφάλειας Πληροφοριών και Δικτύων.

8. Μετά την ολοκλήρωση του επιτόπιου ελέγχου, η Ομάδα Επιθεώρησης Ελέγχου εξετάζει το σύνολο των συλλεχθέντων στοιχείων και συντάσσουν έγγραφο με τίτλο «Έκθεση διενέργειας τακτικού ελέγχου Ασφαλείας Πληροφοριών και Δικτύων στον υπόχρεο Οργανισμό», το οποίο περιλαμβάνει απαραιτήτως τα ακόλουθα στοιχεία:

α) Τα στοιχεία της απόφασης της ΕΑΚ με την οποία ορίστηκε η διενέργεια τακτικού ή έκτακτου ελέγχου.

β) Το ονοματεπώνυμο και την ιδιότητα των προσώπων που απαρτίζουν την Ομάδα Επιθεώρησης Ελέγχου και την ημερομηνία σύστασης της τελευταίας.

γ) Την επωνυμία του ελεγχόμενου υπόχρεου Οργανισμού, καθώς και το όνομα του Υπεύθυνο Ασφάλειας Πληροφοριών και Δικτύων.

δ) Το πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις του υπόχρεου Οργανισμού καθώς και κάθε σχετική έγγραφη επικοινωνία μεταξύ της Αρχής και του Οργανισμού στο πλαίσιο της διεξαγωγής του τακτικού ελέγχου.

ε) Αναλυτική περιγραφή των ευρημάτων του ελέγχου και διαπίστωση τυχόν παραλείψεων καθώς και συστάσεις προς επίλυση αυτών.

στ) Την ημερομηνία έναρξης και περάτωσης του ελέγχου.

ζ) Τελικό πόρισμα του ελέγχου.

9. Η έκθεση κοινοποιείται από την ΕΑΚ στον υπόχρεο Οργανισμό το αργότερο εντός εξήντα (60) ημερών από την ημερομηνία περάτωσης του ελέγχου.

10. Οποιαδήποτε επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τη διαδικασία ελέγχου, διενεργείται σύμφωνα με τον Κανονισμό (ΕΚ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 (ΕΕ L 119) και το ν. 2472/1997 (Α΄ 50).

Δ. ΔΙΑΔΙΚΑΣΙΑ ΕΠΙΒΟΛΗΣ ΔΙΟΙΚΗΤΙΚΩΝ ΚΥΡΩΣΕΩΝ

Άρθρο 13
Κυρώσεις

1. Λαμβάνοντας υπόψη τις διατάξεις του άρθρου 15 του ν. 4577/2018 (Α΄ 199), ο Υπουργός Ψηφιακής Διακυβέρνησης, μετά από εισήγηση της Εθνικής Αρχής Κυβερνοασφάλειας, επιβάλλει σε φυσικά ή νομικά πρόσωπα, διαζευκτικά ή σωρευτικά, τη λήψη συγκεκριμένων διορθωτικών μέτρων εντός τακτού χρονικού διαστήματος, καθώς και διοικητικές κυρώσεις για τις διαπιστούμενες παραβάσεις στις οποίες αυτά υποπίπτουν είτε μία ή περισσότερες από τις εξής κυρώσεις:

α) Σύσταση προς τον Οργανισμό ή τον νόμιμο εκπρόσωπό τους, σε περίπτωση που, κατόπιν διενέργειας ελέγχου ή συνδρομή συμβάντος ασφαλείας, αναγνωριστεί ότι δεν τηρούνται τα απαιτούμενα από το νόμο μέτρα ασφαλείας.

β) Επίπληξη προς τον Οργανισμό ή τον νόμιμο εκπρόσωπό τους, σε περίπτωση που κατόπιν διενέργειας ελέγχου ή συνδρομή συμβάντος ασφαλείας, αναγνωριστεί ότι παρά την πρότερη σύσταση της αρχής δεν συμμορφώθηκαν με τις υποδείξεις της ΕΑΚ.

γ) Στην περίπτωση μη συμμόρφωσης του Οργανισμού με την διαδικασία σύστασης η επίπληξης, επιβάλλεται διοικητικό πρόστιμο στον Οργανισμό σύμφωνα με τις διατάξεις του άρθρου 15 του ν. 4577/2018 (Α΄ 199).

2. Κατά την επιμέτρηση της κύρωσης λαμβάνονται υπόψη τα κριτήρια της αποτελεσματικότητας, της αναλογικότητας και του αποτρεπτικού χαρακτήρα της κύρωσης.

Άρθρο 14
Κριτήρια Επιμέτρησης Κυρώσεων

Προκειμένου για τον καθορισμό και την επιμέτρηση των εκάστοτε επιβαλλόμενων κυρώσεων η Αρχή λαμβάνει υπόψη τα ακόλουθα κριτήρια:

1) Για το νομικό πρόσωπο:

α) Τον αριθμό των επιμέρους υποχρεώσεων που έχουν παραβιασθεί, σύμφωνα με τα προβλεπόμενα στα άρθρα 9 έως 12 και 15 του ν. 4577/2018 (Α΄ 199) και ειδικότερα:

β) Την αξιολόγηση του αντίκτυπου του περιστατικού, σε περίπτωση που η παράβαση αφορά παράλειψη κοινοποίησης ή κοινοποίηση με αδικαιολόγητη καθυστέρηση συμβάντος.

γ) Τη γενική αξιολόγηση των τεχνικών και οργανωτικών προληπτικών μέτρων για τη διαχείριση των κινδύνων, αναφορικά με την ασφάλεια των δικτύων και των συστημάτων πληροφοριών, η οποία προκύπτει από την εξέταση:

αα) των πολιτικών και των διαδικασιών για την ασφάλεια δικτύων και πληροφοριακών συστημάτων,

ββ) της λειτουργίας και αποτελεσματικότητας εσωτερικών ελέγχων καθώς και προτάσεων για την πραγματοποίηση διορθωτικών ενεργειών των διαπιστούμενων ελλείψεων στο πεδίο της ασφάλειας δικτύων,

γγ) της εγκατάστασης και ορθής λειτουργίας πληροφοριακών συστημάτων που παρακολουθούν την ασφάλεια των δικτύων,

δδ) του βαθμού συμμόρφωσης του νομικού προσώπου με τις επιβαλλόμενες υποχρεώσεις,

εε) της ανάθεσης της παρακολούθησης της ασφάλειας δικτύου και πληροφοριακών συστημάτων σε εξειδικευμένο προσωπικό.

δ) Εάν έχει προηγηθεί σύσταση προς συμμόρφωση και εάν τηρήθηκε το ενδεδειγμένο πλάνο ενεργειών μέσα σε εύλογο χρονικό διάστημα.

ε) Τη διάθεση για συνεργασία σε περίπτωση περιστατικού ασφαλείας και την ανταπόκριση του νομικού προσώπου σε τυχόν άμεσες υποδείξεις συμμόρφωσης και την αποτελεσματικότητα της τελευταίας.

στ) Το μέγεθος και το μερίδιο αγοράς του νομικού προσώπου.

2) Για το φυσικό πρόσωπο:

α) Το βαθμό υπαιτιότητας του φυσικού προσώπου ως προς τη συνδρομή του περιστατικού ή τη μη συμμόρφωση του Οργανισμού.

β) Ειδικότερα, την πλημμελή εκτέλεση των καθηκόντων του αναφορικά με τον έλεγχο επί της ασφάλειας δικτύου και συστημάτων πληροφορικής του Οργανισμού.

Άρθρο 15
Διαδικασία Επιβολής Κυρώσεων

1. Προ της επιβολής οποιασδήποτε κύρωσης, η ΕΑΚ, καλεί υποχρεωτικά τα ενδιαφερόμενα νομικά και φυσικά πρόσωπα να υποβάλουν τις απόψεις τους σε ημερομηνία που απέχει τουλάχιστον πέντε (5) εργάσιμες ημέρες από την κοινοποίηση της ειδοποίησης.

2. Οι κατά τα ανωτέρω κυρώσεις λαμβάνονται με αιτιολογημένες αποφάσεις, καταχωρούνται σε ειδικό βιβλίο, κοινοποιούνται στο ενδιαφερόμενο νομικό ή φυσικό πρόσωπο εντός δέκα (10) εργάσιμων ημερών από την έκδοσή τους και μπορούν να ανακοινώνονται δημόσια, εφόσον η δημοσιοποίησή τους δεν πρόκειται να προκαλέσει δυσανάλογη ζημιά στο νομικό ή φυσικό πρόσωπο στο οποίο επιβάλλεται η κύρωση, στην εθνική άμυνα και τη δημόσια ασφάλεια, σε κάθε δε περίπτωση αναρτώνται στην επίσημη ιστοσελίδα της Εθνικής Αρχής Κυβερνοασφάλειας.

Άρθρο 16
Μεθοδολογία Προσδιορισμού Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών

Ένας φορέας για να πληροί τις προϋποθέσεις και να χαρακτηριστεί ως ΦΕΒΥ, πρέπει να ανήκει σε τομέα ή υποτομέα του ν. 4577/2018 (Α΄ 199), να προσφέρει βασική υπηρεσία με βάση το παράρτημα 1 της παρούσης, η παροχή υπηρεσίας του να βασίζεται σε ψηφιακά συστήματα και να καλύπτει τουλάχιστον ένα από τα παρακάτω κριτήρια του παρόντος άρθρου, ανά τομέα. Α. Τομέας ηλεκτρικής ενέργειας.

1. Για τον υποτομέα ηλεκτρικής ενέργειας το κατώτατο όριο είναι:

α) Για τη βασική υπηρεσία της προμήθειας ηλεκτρικής ενέργειας, το κατώτατο όριο είναι ο φορέας να προμηθεύει με ηλεκτρική ενέργεια περισσότερους από το 10% του συνόλου των πελατών του δικτύου διανομής ηλεκτρικής ενέργειας ή να διαθέτει περισσότερους από 500.000 πελάτες ή να προμηθεύει το 10% της συνολικής τροφοδοτούμενης ισχύος στο Εθνικό Σύστημα Μεταφοράς Ηλεκτρικής Ενέργειας (ΕΣΜΗΕ) ή να τροφοδοτεί το ΕΣΜΗΕ με ισχύ τουλάχιστον 1,5 GW.

β) Για τη βασική υπηρεσία της διανομής ηλεκτρικής ενέργειας, το κατώτατο όριο είναι ο φορέας να τροφοδοτεί με ηλεκτρική ενέργεια περισσότερους από το 10% του συνόλου των πελατών του δικτύου διανομής ή να διαθέτει περισσότερους από 500.000 πελάτες συνδεδεμένους στο δίκτυο διανομής ηλεκτρικής ενέργειας.

γ) Για τη βασική υπηρεσία της μεταφοράς ηλεκτρικής ενέργειας, το κατώτατο όριο είναι ο φορέας να διαχειρίζεται τουλάχιστον το 10% των TWh που διακινούνται ετησίως στο Εθνικό Σύστημα Μεταφοράς Ηλεκτρικής Ενέργειας (ΕΣΜΗΕ) ή να διαχειρίζεται το 5TWh που διακινούνται ετησίως στο ΕΣΜΗΕ.

2. Για τον υποτομέα του πετρελαίου το κατώτατο όριο είναι:

α) Για τη βασική υπηρεσία της μεταφοράς πετρελαίου μέσω αγωγού, το κατώτατο όριο είναι ο φορέας να διαχειρίζονται αγωγό ή αγωγούς με ικανότητα μεταφοράς άνω του 10% των ετήσιων αναγκών της χώρας σε πετρέλαιο ή τουλάχιστον 1,5 εκατομμύριο κυβικά μέτρα πετρέλαιο ετησίως.

β) Για τη βασική υπηρεσία της παραγωγής, διύλισης, επεξεργασίας, αποθήκευσης και μεταφοράς πετρελαίου, το κατώτατο όριο είναι ο φορέας, ανά περίπτωση, να διαχειρίζεται το 10% των ετήσιων αναγκών της χώρας σε πετρέλαιο ή τουλάχιστον 1,5 εκατομμύριο κυβικά μέτρα πετρέλαιο ετησίως.

3. Για τον υποτομέα αερίου το κατώτατο όριο είναι:

α) Για τη βασική υπηρεσία της προμήθειας φυσικού αερίου στο Εθνικό Σύστημα Μεταφοράς Φυσικού Αερίου,

το κατώτατο όριο είναι ο φορέας να εισάγει στο Εθνικό Σύστημα Μεταφοράς Φυσικού Αερίου περισσότερα από 500.000.000 κυβικά μέτρα φυσικού αερίου.

β) Για τη βασική υπηρεσία της διανομής φυσικού αερίου, το κατώτατο όριο είναι ο φορέας να τροφοδοτεί με φυσικό αέριο περισσότερους από το 10% του συνόλου των πελατών του δικτύου διανομής ή να διαθέτει περισσότερους από 50.000 πελάτες συνδεδεμένους στο δικτύου διανομής φυσικού αερίου ή η δικαιοδοσία του να καλύπτει τα όρια μιας γεωγραφικής περιφέρειας.

γ) Για τη βασική υπηρεσία της μεταφοράς φυσικού αερίου, το κατώτατο όριο είναι ο φορέας να διαχειρίζεται τουλάχιστον τα 10% ή 500.000.000 κυβικά μέτρα φυσικού αερίου που διακινούνται ετήσια στο Εθνικό Σύστημα Μεταφοράς Φυσικού Αερίου.

δ) Για τη βασική υπηρεσία της αποθήκευσης φυσικού αερίου, το κατώτατο όριο είναι ο φορέας να διαθέτει εγκαταστάσεις αποθήκευσης φυσικού αερίου με χωρητικότητα μεγαλύτερη από 100.000 κυβικά μέτρα υγροποιημένου φυσικού αερίου (ΥΦΑ).

ε) Για τη βασική υπηρεσία της διαχείρισης συστημάτων ΥΦΑ, το κατώτατο όριο είναι ο φορέας να διαθέτει την τεχνολογική ικανότητα να εισάγει περισσότερα από 10% της ετήσιας κατανάλωσης ή 500.000.000 κυβικά μέτρα φυσικού αερίου ετησίως στο Εθνικό Σύστημα Μεταφοράς Φυσικού Αερίου.

στ) Για τη βασική υπηρεσία της προμήθειας φυσικού αερίου σε καταναλωτές, το κατώτατο όριο είναι ο φορέας να διαθέτει περισσότερους από το 10% του συνόλου των πελατών του δικτύου διανομής φυσικού αερίου ή να διαθέτει τουλάχιστον 50.000 πελάτες συνδεδεμένους στο δίκτυο διανομής φυσικού αερίου.

ζ) Για τη βασική υπηρεσία της διύλισης και επεξεργασίας φυσικού αερίου, το κατώτατο όριο είναι ο φορέας να έχει την ικανότητα διύλισης και επεξεργασίας τουλάχιστον 500.000.000 κυβικά μέτρα φυσικού αερίου.

Β. Τομέας Μεταφορών

1. Για τον υποτομέα αεροπορικών μεταφορών:

α) Για τη βασική υπηρεσία της αερομεταφοράς, το κατώτατο όριο είναι ο φορέας να έχει ετήσια επιβατική κίνηση τουλάχιστον 4.000.000 επιβάτες ή να διακινεί περισσότερο από το 10% του ετήσιου συνολικού αριθμού επιβατών των ελληνικών αεροδρομίων.

β) Για τη βασική υπηρεσία της Διαχείρισης αερολιμένα και βοηθητικών εγκαταστάσεων εντός αερολιμένα, το κατώτατο όριο είναι ο φορέας να διαχειρίζεται αερολιμένα με ετήσια επιβατική κίνηση τουλάχιστον 4.000.000 επιβατών ή αερολιμένα ο οποίος διακινεί περισσότερους από το 10% του ετήσιου συνολικού αριθμού επιβατών των ελληνικών αεροδρομίων.

γ) Για τη βασική υπηρεσία της διαχείρισης της εναέριας κυκλοφορίας, το κατώτατο όριο είναι ο φορέας να διαχειρίζεται αερολιμένα με ετήσια επιβατική κίνηση τουλάχιστον 4.000.000 επιβατών ή αερολιμένα ο οποίος διακινεί περισσότερους από το 10% του ετήσιου συνολικού αριθμού επιβατών των ελληνικών αεροδρομίων.

2. Για τον υποτομέα των σιδηροδρομικών μεταφορών το κατώτατο όριο είναι:

α) Για τη βασική υπηρεσία της διαχείρισης της σιδηροδρομικής υποδομής, το κατώτατο όριο είναι ο φορέας να διαχειρίζεται υποδομή που εξυπηρετεί μεταφορικό έργο, κατά έτος, πάνω από 125 εκατομμύρια επιβατοχιλιόμετρα ή 25 εκατομμύρια τονοχιλιόμετρα ή πάνω από το 10% των ετήσιων επιβατοχιλιόμετρων ή πάνω από το 10% των τονοχιλιόμετρων του σιδηροδρομικού δικτύου.

β) Για τη βασική υπηρεσία της παροχής σιδηροδρομικών υπηρεσιών, το κατώτατο όριο είναι ο φορέας να έχει μεταφορικό έργο κατά έτος, πάνω από 125 εκατομμύρια επιβατοχιλιόμετρα ή 25 εκατομμύρια τονοχιλιόμετρα ή πάνω από το 10% των ετήσιων επιβατοχιλιόμετρων ή πάνω από το 10% των τονοχιλιόμετρων του σιδηροδρομικού δικτύου.

3. Για τον υποτομέα των πλωτών μεταφορών το κατώτατο όριο είναι:

α) Για τη βασική υπηρεσία των εσωτερικών πλωτών, θαλάσσιων και ακτοπλοϊκών μεταφορών επιβατών και εμπορευμάτων, το κατώτατο όριο είναι ο φορέας να μεταφέρει κατ’ ελάχιστον 3.000.000 επιβάτες κατ’ έτος ή να μεταφέρει κατ’ ελάχιστον 400.000 εμπορευματοκιβώτια (TEUS) κατ’ έτος ή να μεταφέρει κατ’ ελάχιστον 100.000 φορτηγά κατ’ έτος.

β) Για τη βασική υπηρεσία της διαχείρισης και εκμετάλλευσης λιμένων, συμπεριλαμβανομένων των λιμενικών τους εγκαταστάσεων καθώς και την εκμετάλλευση έργων και εξοπλισμού που βρίσκονται εντός των λιμένων, το κατώτατο όριο είναι ο φορέας να διαχειρίζεται λιμένα που μεταφέρει κατ’ ελάχιστον 3.000.000 επιβάτες κατ’ έτος ή να μεταφέρει κατ’ ελάχιστον 400.000 εμπορευματοκιβώτια (TEUS) κατ’ έτος ή να μεταφέρει κατ’ ελάχιστον 100.000 φορτηγά κατ’ έτος.

γ) Για τη βασική υπηρεσία της Διαχείρισης Κυκλοφορίας πλοίων (VTS), το κατώτατο όριο είναι ο φορέας να έχει υπό την εποπτεία του λιμένα ή λιμένες που να μεταφέρει κατ’ ελάχιστον 3.000.000 επιβάτες κατ’ έτος ή να μεταφέρει κατ’ ελάχιστον 400.000 εμπορευματοκιβώτια (TEUS) κατ’ έτος ή να μεταφέρει κατ’ ελάχιστον 100.000 φορτηγά κατ’ έτος.

4. Για τον υποτομέα των οδικών μεταφορών, το κατώτατο όριο είναι:

α) Για τη βασική υπηρεσία ελέγχου διαχείρισης κυκλοφορίας, το κατώτατο όριο είναι ο φορέας (οδική αρχή) να είναι υπεύθυνος για τον έλεγχο διαχείρισης της κυκλοφορίας αυτοκινητοδρόμων με επιβατική κίνηση οχημάτων κατ’ ελάχιστον 10 εκατομμυρίων οχηματοχιλιόμετρων κατ’ έτος ή τουλάχιστον 10.000 μέση ημερήσια κυκλοφορία οχημάτων κατ’ έτος ή 50 χιλιόμετρα συνολικό μήκος εθνικού αυτοκινητοδρόμου.

β) Για τη βασική υπηρεσία των συστημάτων ευφυών μεταφορών (ITS), το κατώτατο όριο είναι ο φορέας να είναι υπεύθυνος για την διαχείριση συστημάτων ευφυών μεταφορών (ITS) οχημάτων με επιβατική κίνηση τουλάχιστον 10 εκατομμυρίων οχηματοχιλιόμετρων κατ’ έτος ή τουλάχιστον 10.000 μέση ημερήσια κυκλοφορία οχημάτων κατ’ έτος ή 50 χιλιόμετρων συνολικού μήκος εθνικού αυτοκινητοδρόμου.

Γ. Τομέας τραπεζών

Για τη βασική υπηρεσία Χρηματοπιστωτικών Συναλλαγών, το κατώτατο όριο είναι το τραπεζικό ίδρυμα να

έχει λάβει άδεια λειτουργίας στην Ελλάδα και να έχει χαρακτηριστεί από την Τράπεζα της Ελλάδος ως συστημικό σημαντικό πιστωτικό ίδρυμα (Other Systemically Important Institutions -O-SII). Η Τράπεζα της Ελλάδος, βάσει του ν. 4261/2014 (άρθρο 124), είναι αρμόδια για τον προσδιορισμό των λοιπών συστημικά σημαντικών πιστωτικών ιδρυμάτων μεταξύ των πιστωτικών ιδρυμάτων που έχουν λάβει άδεια λειτουργίας στην Ελλάδα.

Δ. Τομέας υποδομών χρηματοπιστωτικών αγορών

Για τον τομέα υποδομών χρηματοπιστωτικών αγορών το κατώτατο όριο είναι:

α) Για τη βασική υπηρεσία της εκμετάλλευσης τόπων διαπραγμάτευσης, το κατώτατο όριο είναι ο φορέας να πραγματοποιεί τουλάχιστον το 10% των συνολικών συναλλαγών που πραγματοποιούνται σε ετήσια βάση.

β) Για τη βασική υπηρεσία των Κεντρικών αντισυμβαλλόμενων (CCPs), το κατώτατο όριο είναι ο φορέας να πραγματοποιεί τουλάχιστον το 10% των συνολικών συναλλαγών που πραγματοποιούνται σε ετήσια βάση.

Ε. Τομέας της υγείας

Για τον τομέα της υγείας και ειδικότερα για τη βασική υπηρεσία της παροχής υγειονομικής περίθαλψης το κατώτατο όριο είναι ο φορέας να αποτελεί Γενικό Νοσοκομείο, με τουλάχιστον 40.000 νοσηλευθέντες ασθενείς κατ’ έτος, ή Γενικό Νοσοκομείο που να διαθέτει τουλάχιστον 500 κλίνες.

ΣΤ. Τομέας προμήθειας και διανομής πόσιμου νερού

Για τον τομέα προμήθειας και διανομής πόσιμου νερού και ειδικότερα για την αντίστοιχη βασική υπηρεσία προμήθειας και διανομής πόσιμου νερού, το κατώτατο όριο είναι ο φορέας ύδρευσης να προμηθεύει κατ’ έτος με πόσιμο νερό πληθυσμό μεγαλύτερο των 500.000 καταναλωτών ή από το δίκτυό του να διανέμονται περισσότερα από 50.000.000 κυβικά μέτρα νερό ετησίως.

Ζ. Τομέας ψηφιακής υποδομής

Για τον τομέα ψηφιακής υποδομής το κατώτατο όριο είναι:

α) Για τη βασική υπηρεσία της ανταλλαγής κίνησης αυτόνομων συστημάτων διαδικτύου (IXP), το κατώτατο όριο είναι ο φορέας να έχει μέση ημερήσια κίνηση περισσότερο από 5Gbit/δευτερόλεπτο ή να κατέχει τουλάχιστον το 10% της συνολικής κίνησης όλων των Φορέων IXP που δραστηριοποιούνται στην Ελλάδα.

β) Για τη βασική υπηρεσία της ονοματοδοσίας στο διαδίκτυο (DNS), το κατώτατο όριο είναι ο πάροχος υπηρεσιών DNS να εξυπηρετεί τουλάχιστον 1.000.000.000 αιτήματα την ημέρα (request/day) ή να διαθέτει στα Μητρώα του καταχωρημένα τουλάχιστον 50.000 διαφορετικά ενεργά ονόματα χώρου (domain names) ή να κατέχει τουλάχιστον το 10% του συνόλου των ερωτημάτων μεταξύ όλων των παροχών DNS.

γ) Για τη βασική υπηρεσία της καταχώρισης Μητρώων Ονομάτων Χώρου Ανώτατου Επιπέδου στο διαδίκτυο (registrar TLD), το κατώτατο όριο είναι ο φορέας να εξυπηρετεί τουλάχιστον 50.000.000 ερωτήματα την ημέρα (queries/day) ή να κατέχει τουλάχιστον το 10% του συνόλου των ερωτημάτων μεταξύ όλων των καταχωρητών (registrar) Μητρώου TLD.

Άρθρο 17
Μεταβατικές και λοιπές διατάξεις

Κάθε Οργανισμός οφείλει να πραγματοποιεί αυτοαξιολόγηση των συστημάτων δικτύου και πληροφοριών του με τη χρήση του Οδηγού Αυτοαξιολόγησης που θα εκδόσει η Εθνική Αρχή Κυβερνοασφάλειας εντός 6 μηνών από την έκδοσή του και έχει υποχρέωση να κοινοποιήσει τα αποτελέσματα της αυτοαξιολόγησης στην Εθνική Αρχή Κυβερνοασφαλειας και κάθε χρόνο εφεξής.

Η Εθνική Αρχή Κυβερνοασφάλειας δύναται να εξειδικεύει περαιτέρω όσα ορίζονται με τη παρούσα, με σχετικές Οδηγίες κατ’ εξουσιοδότηση της παρούσης.

Άρθρο 18

Προσαρτώνται στην παρούσα υπουργική απόφαση, και αποτελούν αναπόσπαστο τμήμα αυτού τα Παραρτήματα 1 και 2.

Άρθρο 19
Έναρξη ισχύος

Η ισχύς της παρούσας αρχίζει από τη δημοσίευσή της, εκτός αν άλλως ορίζεται στις επιμέρους διατάξεις.

Παράρτημα 1 – Κατάλογος Βασικών Υπηρεσιών

Τομέας/ Υποτομέας	Είδος υπηρεσίας
Ενέργεια - Ηλεκτρική	Προμήθεια
	Διανομή
	Μεταφορά
Ενέργεια - Πετρέλαιο	Μεταφορά
	Διύλιση/ Επεξεργασία /Αποθήκευση/ Παραγωγή
Ενέργεια - Αέριο	Προμήθεια
	Διανομή
	Μεταφορά
	Αποθήκευση
	Υγροποιημένο Φυσικό Αέριο (ΥΦΑ)
	Διύλιση/Επεξεργασία
Μεταφορές – Αεροπορικές	Αερομεταφορές
	Διαχείριση αερολιμένα και βοηθητικών εγκαταστάσεων εντός αερολιμένα
	Διαχείριση εναέριας κυκλοφορίας
Μεταφορές – Σιδηροδρομικές	Διαχείριση υποδομής
	Μεταφορά επιβατών και εμπορευμάτων
Μεταφορές – Πλωτές	Μεταφορά επιβατών και εμπορευμάτων
	Διαχείριση λιμένων και εκμετάλλευση έργων εξοπλισμού εντός λιμένων
	Διαχείριση Κυκλοφορίας πλοίων (VTS)
Μεταφορές - Οδικές	Έλεγχος και Διαχείριση Κυκλοφορίας
	Συστήματα Ευφυών Μεταφορών (ITS)
Τράπεζες	Χρηματοπιστωτικές συναλλαγές
Υποδομών Χρηματοπιστωτικών αγορών	Εκμετάλλευση τόπων διαπραγμάτευσης
	Κεντρικοί αντισυμβαλλόμενοι (CCPs) –Εκκαθάριση Προϊόντων

Υγεία	Παροχή υγειονομικής περίθαλψης
Νερό	Προμήθεια ή διανομή πόσιμου νερού
Ψηφιακές Υποδομές	Ανταλλαγή κίνησης αυτόνομων συστημάτων διαδικτύου (IXP)
	Καταχώρηση ονομάτων χώρου στο διαδίκτυο (DNS)
	Καταχώριση ονομάτων χώρου ανώτατου επιπέδου στο διαδίκτυο (TLD)

Η απόφαση αυτή να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως, πλην του Παραρτήματος 2 το οποίο έχει χαρακτηριστεί ως απόρρητο.

Αθήνα, 4 Οκτωβρίου 2019

Ο Υπουργός

ΚΥΡΙΑΚΟΣ ΠΙΕΡΡΑΚΑΚΗΣ

ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ

Το Εθνικό Τυπογραφείο αποτελεί δημόσια υπηρεσία υπαγόμενη στο Υπουργείο Διοικητικής Ανασυγκρότησης και έχει την ευθύνη τόσο για τη σύνταξη, διαχείριση, εκτύπωση και κυκλοφορία των Φύλλων της Εφημερίδας της Κυβερνήσεως (ΦΕΚ), όσο και για την κάλυψη των εκτυπωτικών - εκδοτικών αναγκών του δημοσίου και του ευρύτερου δημόσιου τομέα (ν. 3469/2006/Α΄ 131 και π.δ. 29/2018/Α΄58).

1. ΦΥΛΛΟ ΤΗΣ ΕΦΗΜΕΡΙΔΑΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ (ΦΕΚ)

• Τα **ΦΕΚ σε ηλεκτρονική μορφή** διατίθενται δωρεάν στο **www.et.gr**, την επίσημη ιστοσελίδα του Εθνικού Τυπογραφείου. Όσα ΦΕΚ δεν έχουν ψηφιοποιηθεί και καταχωριστεί στην ανωτέρω ιστοσελίδα, ψηφιοποιούνται και αποστέλλονται επίσης δωρεάν με την υποβολή αίτησης, για την οποία αρκεί η συμπλήρωση των αναγκαίων στοιχείων σε ειδική φόρμα στον ιστότοπο www.et.gr.

• Τα **ΦΕΚ σε έντυπη μορφή** διατίθενται σε μεμονωμένα φύλλα είτε απευθείας από το Τμήμα Πωλήσεων και Συνδρομητών, είτε ταχυδρομικά με την αποστολή αιτήματος παραγγελίας μέσω των ΚΕΠ, είτε με ετήσια συνδρομή μέσω του Τμήματος Πωλήσεων και Συνδρομητών. Το κόστος ενός ασπρόμαυρου ΦΕΚ από 1 έως 16 σελίδες είναι 1,00 €, αλλά για κάθε επιπλέον οκτασέλιδο (ή μέρος αυτού) προσαυξάνεται κατά 0,20 €. Το κόστος ενός έγχρωμου ΦΕΚ από 1 έως 16 σελίδες είναι 1,50 €, αλλά για κάθε επιπλέον οκτασέλιδο (ή μέρος αυτού) προσαυξάνεται κατά 0,30 €. Το τεύχος Α.Σ.Ε.Π. διατίθεται δωρεάν.

• **Τρόποι αποστολής κειμένων προς δημοσίευση:**

Α. Τα κείμενα προς δημοσίευση στο ΦΕΚ, από τις υπηρεσίες και τους φορείς του δημοσίου, αποστέλλονται ηλεκτρονικά στη διεύθυνση **webmaster.et@et.gr** με χρήση προηγμένης ψηφιακής υπογραφής και χρονοσήμανσης.

Β. Κατ’ εξαίρεση, όσοι πολίτες δεν διαθέτουν προηγμένη ψηφιακή υπογραφή μπορούν είτε να αποστέλλουν ταχυδρομικά, είτε να καταθέτουν με εκπρόσωπό τους κείμενα προς δημοσίευση εκτυπωμένα σε χαρτί στο Τμήμα Παραλαβής και Καταχώρισης Δημοσιευμάτων.

• Πληροφορίες, σχετικά με την αποστολή/κατάθεση εγγράφων προς δημοσίευση, την ημερήσια κυκλοφορία των Φ.Ε.Κ., με την πώληση των τευχών και με τους ισχύοντες τιμοκαταλόγους για όλες τις υπηρεσίες μας, περιλαμβάνονται στον ιστότοπο (www.et.gr). Επίσης μέσω του ιστότοπου δίδονται πληροφορίες σχετικά με την πορεία δημοσίευσης των εγγράφων, με βάση τον Κωδικό Αριθμό Δημοσιεύματος (ΚΑΔ). Πρόκειται για τον αριθμό που εκδίδει το Εθνικό Τυπογραφείο για όλα τα κείμενα που πληρούν τις προϋποθέσεις δημοσίευσης.

2. ΕΚΤΥΠΩΤΙΚΕΣ - ΕΚΔΟΤΙΚΕΣ ΑΝΑΓΚΕΣ ΤΟΥ ΔΗΜΟΣΙΟΥ

Το Εθνικό Τυπογραφείο ανταποκρινόμενο σε αιτήματα υπηρεσιών και φορέων του δημοσίου αναλαμβάνει να σχεδιάσει και να εκτυπώσει έντυπα, φυλλάδια, βιβλία, αφίσες, μπλοκ, μηχανογραφικά έντυπα, φακέλους για κάθε χρήση, κ.ά.

Επίσης σχεδιάζει ψηφιακές εκδόσεις, λογότυπα και παράγει οπτικοακουστικό υλικό.

Ταχυδρομική Διεύθυνση: Καποδιστρίου 34, τ.κ. 10432, Αθήνα

ΤΗΛΕΦΩΝΙΚΟ ΚΕΝΤΡΟ: 210 5279000 - fax: 210 5279054

ΕΞΥΠΗΡΕΤΗΣΗ ΚΟΙΝΟΥ

Πωλήσεις - Συνδρομές: (Ισόγειο, τηλ. 210 5279178 - 180)
Πληροφορίες: (Ισόγειο, Γρ. 3 και τηλεφ. κέντρο 210 5279000)
Παραλαβή Δημ. Ύλης: (Ισόγειο, τηλ. 210 5279167, 210 5279139)

Ωράριο για το κοινό: Δευτέρα ως Παρασκευή: 8:00 - 13:30

Ιστότοπος: **www.et.gr**

Πληροφορίες σχετικά με την λειτουργία του ιστότοπου: **helpdesk.et@et.gr**

Αποστολή ψηφιακά υπογεγραμμένων εγγράφων προς δημοσίευση στο ΦΕΚ: **webmaster.et@et.gr**

Πληροφορίες για γενικό πρωτόκολλο και αλληλογραφία: **grammateia@et.gr**

Πείτε μας τη γνώμη σας,

για να βελτιώσουμε τις υπηρεσίες μας, συμπληρώνοντας την ειδική φόρμα στον ιστότοπό μας.

02037390810190012