ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΤΑΧΥΔΡΟΜΕΙΩΝ

Μαρούσι, 23-12-2024

ΑΠ 1138/24

ΑΠΟΦΑΣΗ

Έγκριση της «Πολιτικής Διαχείρισης Τρίτων Μερών»

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ),

Έχοντας υπόψη:

1. Τις διατάξεις:

1.1 του Ν. 4070/2012 «*Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις*» (ΦΕΚ 82/Α/2012), όπως ισχύει τροποποιηθείς,

1.2 του Ν. 4053/2012 *«Ρύθμιση λειτουργίας της ταχυδρομικής αγοράς, θεμάτων ηλεκτρονικών επικοινωνιών και άλλες διατάξεις»* (ΦΕΚ 44/Α/2012), όπως ισχύει τροποποιηθείς,

1.3 του Ν. 4727/2020 *«Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) – Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις.»* (ΦΕΚ 184/Α/2020),

1.4 του Κανονισμού (ΕΕ) αριθ. 679/2016 της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων ή ΓΚΠΔ),

1.5 του Ν. 4624/2019 *«Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική*

Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις» (ΦΕΚ 137/Α/2019),

1.6 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»*, (ΦΕΚ 199/ Α' /03-12-2018), όπως ισχύει,

1.7 του Ν. 4961/2022 «*Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις*», (ΦΕΚ 146/Α'/27-7-2022),

1.8 του Ν. 5002/2022 «*Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών*», (ΦΕΚ 228/Α΄/2022),

1.9 του Ν. 5160/2024 «*Ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του Κανονισμού (ΕΕ) 910/2014 και της Οδηγίας (ΕΕ) 2018/1972, και την κατάργηση της Οδηγίας (ΕΕ) 2016/1148 (Οδηγία NIS 2) και άλλες διατάξεις*» (Α΄ 195),

2. Την ΑΠ 996/08/22-06-2021 Απόφαση της ΕΕΤΤ «*Έγκριση Οργανισμού της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων*» (ΦΕΚ 3367/Β΄/2021),

3. Την ΑΠ 1004/40/30-8-2021 Απόφαση της ΕΕΤΤ «*Κανονισμός Λειτουργίας της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)*» (ΦΕΚ 4660/Β΄/8-10-2021), όπως ισχύει τροποποιηθείσα με την ΑΠ 1062/18/24-01-2023 (ΦΕΚ 947/Β΄/2023),

4. Την εγκεκριμένη από τον Πρόεδρο της ΕΕΤΤ «*Πολιτική Ασφαλείας της ΕΕΤΤ, έκδοση 1.0*» με αριθ. πρωτ. 278/1-6-2018,

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

5. Την ΑΠ 989/25/26-04-2021 Απόφαση της ΕΕΤΤ «*Έγκριση της εφαρμογής της αναθεωρημένης "Πολιτικής Αποδεκτής Χρήσης των Πληροφοριακών Αγαθών της ΕΕΤΤ*"»,
6. Την ΑΠ 1048/13/24-10-2022 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διαχείρισης Συμβάντων Ασφαλείας Πληροφοριών"*»,
7. Την ΑΠ 1069/13/27-03-2023 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Ασφάλειας Τελικού Χρήστη"*»,
8. Την ΑΠ 1078/23/17-07-2023 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Προστασίας Προσωπικών Δεδομένων"*»,
9. Την ΑΠ 1115/11/10-06-2024 Απόφαση της ΕΕΤΤ *«Έγκριση της "Πολιτικής Διαχείρισης Πληροφοριακών Πόρων"»*,
10. Την ΑΠ 1125/17/16-09-2024 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα"*»,
11. Την ΑΠ 1128/24/07-10-2024 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Προμήθειας και Ανάπτυξης Συστημάτων"*»,
12. Την ΑΠ 1109/13/15-4-2024 Απόφαση της ΕΕΤΤ «*Επικύρωση του Εγχειριδίου Διαδικασιών της ΕΕΤΤ*»,
13. Την Εισήγηση αριθ. 38098/Φ600/18-12-2024 της αρμόδιας Υπηρεσίας της ΕΕΤΤ,

και ύστερα από προφορική εισήγηση του Προέδρου της ΕΕΤΤ (Καθηγητή Κωνσταντίνου Μασσέλου),

Επειδή :

1. Είναι κοινά αποδεκτό ότι η συνεργασία κάθε οργανισμού με τρίτα μέρη αυξάνει τους πιθανούς κινδύνους που απειλούν τον οργανισμό αναφορικά με την κυβερνοασφάλεια, την επιβολή κυρώσεων λόγω παραβίασης κανονιστικών και νομοθετικών υποχρεώσεων από το τρίτο μέρος ή άλλους κινδύνους στρατηγικούς, λειτουργικούς, οικονομικούς κτλ.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

2. Ιδίως τρίτα μέρη που έχουν πρόσβαση σε ευαίσθητη, εμπιστευτική πληροφορία, προσωπικά δεδομένα ή στο εσωτερικό δίκτυο του οργανισμού ή εκτελούν κρίσιμες επιχειρησιακές λειτουργίες για λογαριασμό του παρουσιάζουν δυνητικά αυξημένους κινδύνους ασφάλειας για τον οργανισμό.
3. Η ΕΕΤΤ διαχειρίζεται, σε συνεχή βάση, τρίτα μέρη, όπως προμηθευτές, συμβούλους, παρόχους εξειδικευμένων υπηρεσιών, προσωρινό προσωπικό, κτλ. Για το λόγο αυτό, κρίνεται σκόπιμη η υιοθέτηση μιας πολιτικής που θα καθορίσει τις πρακτικές και τα μέτρα που χρησιμοποιεί η ΕΕΤΤ για να διασφαλίσει ότι:
    - Προστατεύεται επαρκώς η ασφάλεια των συστημάτων και των πληροφοριών της στα οποία εμπλέκονται τρίτα μέρη.
    - Οι συνδέσεις/προσβάσεις των τρίτων μερών στα συστήματα της πραγματοποιούνται με μια επίσημη και ασφαλή μέθοδο.
    - Οι απαιτήσεις της ΕΕΤΤ αναφορικά με την ασφάλεια των πληροφοριών ενσωματώνονται στις σχετικές συμβατικές ρήτρες που διέπουν τη σχέση και διασύνδεση με τα τρίτα μέρη.

Αποφασίζει :

1. **Εγκρίνει** την «*Πολιτική Διαχείρισης Τρίτων Μερών*», η οποία έχει ως εξής:

« ***Πολιτική Διαχείρισης Τρίτων Μερών***

Έκδοση: 1η

Τελευταία Ημερομηνία Ενημέρωσης: Δεκέμβριος 2024

1. Σκοπός και πεδίο εφαρμογής

Σκοπός της Πολιτικής Διαχείρισης Τρίτων Μερών είναι να καθορίσει τις πρακτικές και τα μέτρα που χρησιμοποιεί η ΕΕΤΤ για να διασφαλίσει ότι:

- *Προστατεύεται επαρκώς η εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και ιδιωτικότητα των πληροφοριακών πόρων[1] της στους οποίους εμπλέκονται τρίτα μέρη.*

[1] *Στον όρο "πληροφοριακοί πόροι" περιλαμβάνονται οι πληροφορίες που έχει στην κατοχή της, παράγει ή διαχειρίζεται η ΕΕΤΤ, τα πληροφοριακά συστήματα, το λογισμικό και ο εξοπλισμός της που*

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

- *Οι συνδέσεις/προσβάσεις των τρίτων μερών στα συστήματα της ΕΕΤΤ πραγματοποιούνται με μια επίσημη και ασφαλή μέθοδο.*
- *Οι απαιτήσεις της ΕΕΤΤ αναφορικά με την ασφάλεια των πληροφοριών ενσωματώνονται στις σχετικές συμβατικές ρήτρες που διέπουν τη σχέση και διασύνδεση με τα τρίτα μέρη.*

Η πολιτική περιλαμβάνει τις απαιτήσεις ασφαλείας που έχει η ΕΕΤΤ από τα τρίτα μέρη με τα οποία συνεργάζεται ή ενδέχεται να συνεργαστεί, καθώς και τα μέτρα ασφαλείας που απαιτεί να λαμβάνουν. Αφορά σε κανονιστική συμμόρφωση, ασφάλεια ανθρώπινου δυναμικού, φυσική και περιβαλλοντική ασφάλεια, ασφάλεια δικτύων και συστημάτων, ασφάλεια δεδομένων, έλεγχο πρόσβασης, ασφάλεια κατά την προμήθεια, ανάπτυξη και συντήρηση συστημάτων, ασφάλεια υπεργολάβων, διαχείριση περιστατικών ασφαλείας, επιχειρησιακή συνέχεια και ανάκαμψη από καταστροφές.

Το πεδίο εφαρμογής της πολιτικής περιλαμβάνει όλα τα τρίτα μέρη (προμηθευτές, αναδόχους, προσωρινό προσωπικό, υπεργολάβους των τρίτων μερών που συνεργάζεται η ΕΕΤΤ, προσωρινό προσωπικό και τρίτα μέρη που προσλαμβάνεται από τους υπεργολάβους κτλ.) τα οποία έχουν πρόσβαση ή προτίθενται να έχουν πρόσβαση στους πληροφοριακούς πόρους της ΕΕΤΤ είτε από τις εγκαταστάσεις της είτε απομακρυσμένα. Χαρακτηριστικά παραδείγματα τρίτων μερών για την παρούσα είναι σύμβουλοι, πάροχοι εξειδικευμένων υπηρεσιών, προμηθευτές πληροφοριακών συστημάτων και εφαρμογών, πάροχοι υπηρεσιών υπολογιστικού νέφους, κέντρα δεδομένων, εταιρείες διαχείρισης μισθοδοσίας, φοιτητές που πραγματοποιούν πρακτική άσκηση, ασκούμενοι δικηγόροι κτλ.

Ειδικότερα, η πολιτική καλύπτει τις παρακάτω πτυχές της σχέσης της ΕΕΤΤ με τα τρίτα μέρη:

- *Αξιολόγηση και επιλογή των τρίτων μερών.*
- *Ανάλυση κινδύνων που απορρέουν από τη συνεργασία με τρίτα μέρη και προσδιορισμός των μέτρων ασφαλείας για τον περιορισμό των κινδύνων.*
- *Περιεχόμενο των συμβάσεων που συνάπτει η ΕΕΤΤ με τα τρίτα μέρη.*
- *Παρακολούθηση και διαχείριση της συνεργασίας με τα τρίτα μέρη.*
- *Διαχείριση εξουσιοδοτήσεων και διαδικασιών σύνδεσης/πρόσβασης των τρίτων μερών στα συστήματα της ΕΕΤΤ.*
- *Ανασκόπηση και παρακολούθηση των συνδέσεων/προσβάσεων στα συστήματα της ΕΕΤΤ.*
- *Αλλαγές της Πολιτικής Διαχείρισης Τρίτων Μερών.*

2. Αξιολόγηση και επιλογή τρίτων μερών

Η επιλογή τρίτων μερών, όπως προμηθευτών, ανάδοχων, συμβούλων κλπ. λαμβάνει χώρα στην ΕΕΤΤ βάσει της νομοθεσίας περί δημοσίων συμβάσεων. Αντίστοιχα, η επιλογή φοιτητών για πρακτική άσκηση ή ασκούμενων δικηγόρων γίνεται βάσει της νομοθεσίας και των σχετικών Αποφάσεων και διαδικασιών της ΕΕΤΤ.

Ιδιαίτερα όταν η επιλογή τρίτων μερών αφορά προμήθεια εξοπλισμού ή λογισμικού, συντήρηση και υποστήριξη εξοπλισμού ή λογισμικού, διαχείριση των πληροφοριακών συστημάτων της ΕΕΤΤ, παροχή υπηρεσιών που προϋποθέτει πρόσβαση σε πληροφορίες, έγγραφα ή δεδομένα της ΕΕΤΤ κτλ., τότε η προκήρυξη διαγωνισμού μπορεί να ενσωματώνει απαιτήσεις ασφάλειας και προστασίας δεδομένων προσωπικού χαρακτήρα (βλ. Ενότητα 5), κατά περίπτωση. Ενδεικτικά, σε περιπτώσεις έργων / υπηρεσιών / προμηθειών που εκτιμώνται ως υψηλού κινδύνου από πλευράς ασφάλειας πληροφοριών, οι προκηρύξεις θα

επεξεργάζεται ή αποθηκεύει δεδομένα.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

μπορούσαν να απαιτούν ή να προκρίνουν την πιστοποίηση των υποψηφίων με ένα διεθνώς αναγνωρισμένο πρότυπο ασφάλειας πληροφοριών, όπως για παράδειγμα το ISO 27001.

Σε κάθε περίπτωση πρέπει να αποφεύγεται η συνεργασία με τρίτα μέρη με τα οποία η ΕΕΤΤ έχει καταγγείλει συμβάσεις λόγω αναξιοπιστίας των αντισυμβαλλόμενων μερών.

3. Γενικά θέματα συνεργασίας / σύνδεσης / πρόσβασης τρίτου μέρους

3.1 Συμμόρφωση με το νομικό και κανονιστικό πλαίσιο

Όλες οι διαδικασίες σχετικά με την ανταλλαγή πληροφοριών με τρίτα μέρη και τα μέτρα ασφαλείας που εφαρμόζονται πρέπει να είναι σύμφωνα με το ισχύον νομοθετικό και κανονιστικό πλαίσιο.

Τα δεδομένα που χαρακτηρίζονται ως δεδομένα προσωπικού χαρακτήρα πρέπει να επεξεργάζονται σε συμμόρφωση με το Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR) και την Πολιτική Προστασίας Προσωπικών Δεδομένων της ΕΕΤΤ.

Παράλληλα, οι πληροφορίες και τα πληροφοριακά συστήματα πρέπει να προστατεύονται σύμφωνα με το νομοθετικό και κανονιστικό πλαίσιο περί κυβερνοασφάλειας και τις σχετικές πολιτικές ασφαλείας της ΕΕΤΤ.

3.2 Διαδικασία σύνδεσης τρίτου μέρους στα συστήματα της ΕΕΤΤ

Η διαδικασία σύνδεσης τρίτου μέρους στα συστήματα της ΕΕΤΤ αφορά την χορήγηση από μέρους της ΕΕΤΤ στα τρίτα μέρη ασφαλούς πρόσβασης στα υπολογιστικά συστήματά της, είτε αυτά είναι εντός των εγκαταστάσεών της είτε στο Κυβερνητικό Νέφος (G-Cloud), για σκοπούς συντήρησης, διαχείρισης, υποστήριξης των συστημάτων. Η πρόσβαση μάλιστα αυτή συχνά απαιτείται να είναι προνομιακή λόγω της φύσης των εργασιών που εκτελούν τα τρίτα μέρη.

Με σκοπό να διασφαλιστεί ότι η σύνδεση/πρόσβαση των τρίτων μερών στα πληροφοριακά συστήματα της ΕΕΤΤ ελέγχεται και διασφαλίζεται επαρκώς, εφαρμόζεται μια τεκμηριωμένη διαδικασία διαχείρισης τρίτων μερών που ρυθμίζει την είσοδο, επιλογή, εγκατάσταση και διαχείριση των συνδέσεων μεταξύ ΕΕΤΤ και τρίτων μερών.

Σε συνέχεια της σύναψης της σύμβασης με το τρίτο μέρος και εφόσον το τρίτο μέρος χρειάζεται πρόσβαση στα συστήματα της ΕΕΤΤ, τα αρμόδια στελέχη της Διεύθυνσης Ψηφιακής Διακυβέρνησης δημιουργούν κατάλληλα τον απαιτούμενο ή τους απαιτούμενους λογαριασμούς με τα απαραίτητα δικαιώματα. Στη συνέχεια προκειμένου να αποκτήσει απομακρυσμένη πρόσβαση ένα στέλεχος του τρίτου μέρους στο δίκτυο της ΕΕΤΤ απαιτείται έλεγχος ταυτότητας δύο παραγόντων. Δηλαδή δεν αρκεί το συνθηματικό του χρήστη για την είσοδο. Για λόγους ασφαλείας, απαιτούνται δύο διακριτές μορφές αναγνώρισης για την επίτευξη πρόσβασης και μάλιστα η δεύτερη ελέγχεται από στέλεχος της ΕΕΤΤ. Ο πρώτος παράγοντας είναι το συνθηματικό του χρήστη του τρίτου μέρους και ο δεύτερος είναι μια ειδοποίηση για επαλήθευση ότι το τρίτο μέρος είναι εκείνο που προσπαθεί να εισέλθει στο Virtual Private Network (VPN), η οποία αποστέλλεται αυτόματα στο έξυπνο τηλέφωνο κάποιου στελέχους της Διεύθυνσης Ψηφιακής Διακυβέρνησης που επιλέγεται να επιφορτιστεί με αυτό το ρόλο. Το επιφορτισμένο στέλεχος απαντά στην ειδοποίηση αποδεχόμενο την αυθεντικοποίηση οπότε το τρίτο μέρος αποκτά πρόσβαση ή εναλλακτικά απαντά αρνητικά οπότε η πρόσβαση αποτυγχάνει.

Επομένως, η διαδικασία έχει ως εξής: Ο χρήστης αποστέλλει μήνυμα ηλεκτρονικού ταχυδρομείου (ή εναλλακτικά ενημερώνει τηλεφωνικά το αρμόδιο στέλεχος) στην ομάδα υποστήριξης της ΕΕΤΤ ότι επιχειρεί να εισέλθει στο VPN. Το αρμόδιο στέλεχος της Διεύθυνσης Ψηφιακής Διακυβέρνησης απαντά θετικά στο μήνυμα. Αφού λάβει την θετική απάντηση ο χρήστης επιχειρεί να συνδεθεί στο VPN πληκτρολογώντας όνομα χρήστη και συνθηματικό στην εφαρμογή στον υπολογιστή του. Το πρόγραμμα σύνδεσης αποστέλλει αυτόματα αίτημα έγκρισης σύνδεσης στο κινητό του αρμόδιου στελέχους της Διεύθυνσης Ψηφιακής Διακυβέρνησης και το στέλεχος το αποδέχεται. Έτσι παραχωρείται πρόσβαση στο

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

τρίτο μέρος (στους πόρους για τους οποίους του έχει δοθεί δικαίωμα πρόσβασης). Εάν αντίθετα το αρμόδιο στέλεχος της Διεύθυνσης Ψηφιακής Διακυβέρνησης δεν έχει λάβει μήνυμα ηλεκτρονικού ταχυδρομείου από το τρίτο μέρος, τότε απορρίπτει ως ύποπτο κάθε αυτόματο αίτημα πρόσβασης που λαμβάνει στο κινητό του.

3.3 Αρχές πρόσβασης τρίτου μέρους

Η πρόσβαση τρίτων πρέπει να:

- *παρέχεται μόνο όταν έχουν ληφθεί τα απαιτούμενα μέτρα ασφαλείας,*
- *περιορίζεται στις ελάχιστες υπηρεσίες, συστήματα, λειτουργίες και πληροφορίες που απαιτούνται για την εκτέλεση της επιχειρησιακής διαδικασίας,*
- *χρησιμοποιείται μόνο από εξουσιοδοτημένους χρήστες της ΕΕΤΤ και / ή τρίτων μερών*
- *συμμορφώνεται με την πολιτική και τις διαδικασίες προσβάσεων της ΕΕΤΤ.*

3.4 Απαιτήσεις επιπέδου έγκρισης

Για να παραχωρηθεί σε τρίτο μέρος δυνατότητα σύνδεσης με τα πληροφοριακά συστήματα της ΕΕΤΤ, απαιτείται έγκριση από δύο επίπεδα της ΕΕΤΤ: από τον Ιδιοκτήτη των πληροφοριών και από τον Υπεύθυνο Ασφάλειας Πληροφοριακών Συστημάτων.

3.5 Αρχειοθέτηση συνδέσεων

Η ΕΕΤΤ πρέπει να τηρεί ένα αρχείο συνδέσεων όπου οι συνδέσεις τρίτων μερών θα καταγράφονται επαρκώς. Δηλαδή θα καταγράφονται τα αιτήματα από τρίτους, οι ημερομηνίες έναρξης συνδέσεων, οι διαχειριστές συνδέσεων τρίτων και η περιγραφή των υπηρεσιών συνδεσιμότητας.

3.6 Μέθοδοι σύνδεσης

Κάθε πρόσβαση από τρίτους στα πληροφοριακά συστήματα της ΕΕΤΤ πρέπει να υλοποιείται βάσει των τυποποιημένων μεθόδων για ασφαλή παροχή σύνδεσης δικτύου σε τρίτα μέρη, όπως πρόσβαση SSL VPN, κρυπτογράφηση από πελάτη προς site ή από site σε site tunneling, υπηρεσίες τερματικού, κλπ.

3.7 Ένταξη του πλαισίου ασφάλειας πληροφοριών στις συμβάσεις

Στις συμβάσεις έργου/υπηρεσιών/προμηθειών μεταξύ της ΕΕΤΤ και του τρίτου μέρους και ανάλογα πάντα με το συγκεκριμένο αντικείμενο της κάθε σύμβασης, θα πρέπει να ενσωματώνεται και η συμμόρφωση με το πλαίσιο ασφάλειας πληροφοριών της ΕΕΤΤ, ώστε προγενέστερα της χορήγησης πρόσβασης στα πληροφοριακά συστήματα της ΕΕΤΤ, το τρίτο μέρος να έχει δεσμευτεί να συμμορφώνεται με τις πολιτικές και διαδικασίες της ΕΕΤΤ.

3.8 Συμφωνία Επιπέδου Υπηρεσίας (SLA)

Η σύμβαση μεταξύ της ΕΕΤΤ και του τρίτου μέρους πρέπει να ενισχύεται από τη σχετική συμφωνία για το επίπεδο των παρεχόμενων υπηρεσιών (Service Level Agreement - SLA), που προσδιορίζει με ακρίβεια και σαφήνεια το επίπεδο διαθεσιμότητας, απόδοσης, λειτουργίας, ή άλλων χαρακτηριστικών των υπηρεσιών που θα παρέχονται στην ΕΕΤΤ από το τρίτο μέρος.

3.9 Σχέδιο επικοινωνίας

Για κάθε σύμβαση η ΕΕΤΤ πρέπει να προετοιμάσει και να συμφωνήσει το σχέδιο επικοινωνίας των δύο μερών, το οποίο θα περιλαμβάνει το είδος, το μέσο και το σκοπό της επικοινωνίας, τη συχνότητα και τη δομή των αναφορών / αρχείων για την πρόοδο των εργασιών κτλ. και γενικότερα όλες τις απαραίτητες λεπτομέρειες προκειμένου η επικοινωνία των δύο μερών να

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

ικανοποιεί τις προσδοκίες τους για ενημέρωση και συνεργασία και να επιτυγχάνει τους εκάστοτε σκοπούς της.

Το τρίτο μέρος πρέπει να ορίσει έναν υπεύθυνο με τον οποίο θα επικοινωνεί η ΕΕΤΤ για θέματα ασφαλείας και προστασίας δεδομένων.

4. Αναγνώριση και προσδιορισμός των βασικών απαιτήσεων ασφάλειας

4.1 Ανάλυση κινδύνων που απορρέουν από τρίτα μέρη

Η συνεργασία κάθε οργανισμού με τρίτα μέρη (προμηθευτές, αναδόχους, συνεργάτες κτλ.) αυξάνει τους πιθανούς κινδύνους που απειλούν τον οργανισμό. Οι κίνδυνοι λόγω συνεργασίας με τρίτα μέρη ενδέχεται να περιλαμβάνουν κινδύνους κυβερνοεπίθεσης μετά από παραβίαση της ασφάλειας του τρίτου μέρους και επέκτασής της στον οργανισμό, κινδύνους επιβολής κυρώσεων λόγω παραβίασης των κανονιστικών και νομοθετικών υποχρεώσεων από το τρίτο μέρος, κινδύνους στρατηγικούς, λειτουργικούς, οικονομικούς ή προσβολής της εικόνας, με επιπτώσεις, αντίστοιχα, στη στρατηγική, τη λειτουργία, την οικονομική κατάσταση ή την εικόνα του οργανισμού.

Η ανάλυση και διαχείριση των κινδύνων που απορρέουν από τη συνεργασία με τρίτα μέρη είναι κρίσιμη για την προστασία των λειτουργιών της ΕΕΤΤ από τις εξωτερικές απειλές. Ιδίως τρίτα μέρη που έχουν πρόσβαση σε ευαίσθητη, εμπιστευτική πληροφορία ή προσωπικά δεδομένα ή έχουν πρόσβαση στο εσωτερικό δίκτυο της ΕΕΤΤ ή εκτελούν κρίσιμες επιχειρησιακές λειτουργίες για λογαριασμό της παρουσιάζουν δυνητικά αυξημένους κινδύνους ασφάλειας για την ΕΕΤΤ.

Για τους λόγους αυτούς, για κάθε συνεργασία/σύνδεση μεταξύ ΕΕΤΤ και τρίτου μέρους θα πρέπει να διενεργείται ανάλυση κινδύνου, προκειμένου να καθοριστούν οι επιπτώσεις στην ασφάλεια πληροφοριών και τα απαιτούμενα μέτρα περιορισμού των κινδύνων.

Η ανάλυση και διαχείριση κινδύνων τρίτου μέρους περιλαμβάνει τα ακόλουθα βήματα:

- *Προσδιορισμό των πιθανών κινδύνων τρίτου μέρους: Προϋποθέτει την απάντηση, από μέρους της ΕΕΤΤ, ερωτήσεων για το τρίτο μέρος, όπως:*
  - *Εάν το τρίτο μέρος έχει πρόσβαση στην ΕΕΤΤ σε ευαίσθητη ή εμπιστευτική πληροφορία ή προσωπικά δεδομένα. Στην περίπτωση αυτή ο κίνδυνος είναι αυξημένος*
  - *Εάν εκτελεί κρίσιμες επιχειρησιακές λειτουργίες για λογαριασμό της ΕΕΤΤ. Στην περίπτωση αυτή ο κίνδυνος είναι αυξημένος*
  - *Εάν έχει πρόσβαση στο εσωτερικό δίκτυο της ΕΕΤΤ, οπότε ο κίνδυνος είναι αυξημένος*
  - *Ποιο είναι το επίπεδο πρόσβασης που του έχει παραχωρηθεί. Το επίπεδο πρόσβασης επηρεάζει το επίπεδο του κινδύνου*
  - *Εάν το τρίτο μέρος υπάγεται σε συγκεκριμένες κανονιστικές και νομοθετικές υποχρεώσεις κατά τη συνεργασία του με την ΕΕΤΤ (π.χ. αποτελεί εκτελούντα την επεξεργασία κατά την έννοια του GDPR, δηλαδή επεξεργάζεται προσωπικά δεδομένα για λογαριασμό της ΕΕΤΤ). Εάν ναι, τότε ο κίνδυνος είναι αυξημένος*
  - *Μήπως το τρίτο μέρος χρησιμοποιεί άλλα τρίτα μέρη (υπεργολάβους, μη μόνιμο προσωπικό κτλ.) που θα μπορούσαν να θέσουν σε κίνδυνο την ασφαλή παροχή της υπηρεσίας του στην ΕΕΤΤ. Σε αυτή την περίπτωση, ο κίνδυνος είναι αυξημένος*
- *Αξιολόγηση των μέτρων ασφάλειας του τρίτου μέρους, αναφορικά με τα εξής:*
  - *Εάν το τρίτο μέρος έχει μια ενημερωμένη πολιτική ασφάλειας και πόσο συχνά την ανασκοπεί και ενημερώνει*

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

- *Τα μέτρα ασφάλειας που λαμβάνει το τρίτο μέρος για να περιορίσει τους κινδύνους*
- *Τα πρότυπα ασφαλείας με τα οποία συμμορφώνεται και εάν είναι πιστοποιημένο στην ασφάλεια πληροφοριών*
- *Εάν εκπαιδεύει το προσωπικό του σε καλές πρακτικές ασφαλείας*
- *Πώς και πού αποθηκεύει τα δεδομένα και πώς τα προστατεύει. Για παράδειγμα, εάν τα κρυπτογραφεί, ψευδωνυμοποιεί, ανωνυμοποιεί κτλ.*
- *Εάν διαθέτει σχέδιο αντιμετώπισης περιστατικών ασφαλείας και αν το σχέδιο του περιλαμβάνει την άμεση ειδοποίηση της ΕΕΤΤ σε περίπτωση συμβάντος*
- *Εάν διαθέτει σχέδιο για τη συνέχιση της λειτουργίας και την ανάκαμψη από καταστροφές*
- *Εάν έχει υποστεί παραβίαση δεδομένων ή κάποιο σημαντικό περιστατικό ασφάλειας και πώς το διαχειρίστηκε*
- *Εάν έχει υποβληθεί σε κυρώσεις ή άλλες παρεμβάσεις από τις αρμόδιες αρχές λόγω παραβίασης του κανονιστικού ή νομοθετικού πλαισίου*
- *Εάν εκτελεί σε τακτική βάση εσωτερικούς ελέγχους ασφαλείας, σαρώσεις ευπάθειας, δοκιμές διείσδυσης (penetration tests) και πότε ολοκλήρωσε τον πιο πρόσφατο έλεγχο της ασφάλειάς του*

- *Ανάλυση των κινδύνων των υπεργολάβων του τρίτου μέρους: Περιλαμβάνει μελέτη των σχεδίων που εφαρμόζει το τρίτο μέρος για την αξιολόγηση, διαχείριση, παρακολούθηση κινδύνου των υπεργολάβων του.*
- *Ταξινόμηση της σοβαρότητας των κινδύνων του τρίτου μέρους σύμφωνα με την πιθανότητα να συμβούν οι κίνδυνοι και τις εκτιμώμενες επιπτώσεις τους στην περίπτωση που συμβούν.*
- *Ανάπτυξη σχεδίου αντιμετώπισης των κινδύνων των τρίτων μερών για την περίπτωση που μετατραπούν σε πραγματική απειλή ή συμβάν ασφάλειας: Περιλαμβάνει οργανωτικά και τεχνικά μέτρα προστασίας, όπως έλεγχο πρόσβασης, κρυπτογράφηση κτλ.*
- *Διαρκή παρακολούθηση των κινδύνων των τρίτων μερών, καθώς νέες απειλές προκύπτουν και τα συστήματα μεταβάλλονται: Περιλαμβάνει συνεχή έλεγχο ότι τα τρίτα μέρη ακολουθούν τις δεσμεύσεις τους ως προς την ασφάλεια και, επίσης, επισήμανση εκείνων των τρίτων μερών που υπερβαίνουν το όριο κινδύνου που έχει χαρακτηριστεί ως αποδεκτό.*
- *Καθορισμό στρατηγικής άμεσης προστασίας από επικίνδυνο τρίτο μέρος, η οποία θα περιλαμβάνει:*
  - *ανάκληση οποιασδήποτε φυσικής πρόσβασης στις εγκαταστάσεις της ΕΕΤΤ έχει παραχωρηθεί στο τρίτο μέρος,*
  - *επιστροφή στην ΕΕΤΤ οποιουδήποτε εξοπλισμού έχει τυχόν παραχωρηθεί στο τρίτο μέρος,*
  - *κατάργηση των λογαριασμών πρόσβασης και των διαπιστευτηρίων σύνδεσης του τρίτου μέρους στα δίκτυα και συστήματα της ΕΕΤΤ,*
  - *κατάλληλη εκκαθάριση των δεδομένων που ελήφθησαν από το τρίτο μέρος,*
  - *διατήρηση αρχείων καταγραφής πρόσβασης για την ανίχνευση μη εξουσιοδοτημένων προσπαθειών πρόσβασης.*

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

5. Απαιτήσεις ασφαλείας στις συμβάσεις της ΕΕΤΤ με τρίτα μέρη

Η ΕΕΤΤ συνάπτει γραπτές συμβάσεις με τα τρίτα μέρη στα οποία αναθέτει προμήθειες, υπηρεσίες ή έργα, σύμφωνα με τη νομοθεσία περί δημοσίων συμβάσεων. Ασχέτως του ποσού της σύμβασης, συνάπτει υποχρεωτικά γραπτή σύμβαση (ή άλλη νομική πράξη υπαγόμενη στο δίκαιο της Ένωσης ή του ελληνικού κράτους) και με όλους τους αναδόχους που αποτελούν εκτελούντες την επεξεργασία κατά την έννοια του GDPR, δηλαδή επεξεργάζονται προσωπικά δεδομένα για λογαριασμό της.

Οι συμβάσεις συμπεριλαμβάνουν ελάχιστα επίπεδα υπηρεσιών και βασικές απαιτήσεις ασφάλειας και συμμόρφωσης. Ο γενικός κανόνας είναι ότι η ΕΕΤΤ τηρεί κοινά πρότυπα συνεργασίας και παρακολούθησης για το σύνολο των τρίτων μερών με τα οποία συνάπτει συμβάσεις.

Η ΕΕΤΤ πρέπει να διασφαλίζει ότι οι κάτωθι απαιτήσεις ασφάλειας πληροφοριών εμπεριέχονται στις συμβάσεις με τρίτα μέρη, σε συνάρτηση βέβαια και με το συγκεκριμένο αντικείμενο της κάθε σύμβασης.

5.1 Συμμόρφωση με το νομοθετικό και κανονιστικό πλαίσιο

Η σύμβαση πρέπει να περιλαμβάνει το νομοθετικό και κανονιστικό πλαίσιο στο οποίο πρέπει να συμμορφώνεται το τρίτο μέρος, π.χ. τον Κανονισμό GDPR, την Οδηγία NIS2 κτλ. Ενδεικτικά, θα περιλαμβάνει τους κατάλληλους όρους για την προστασία δεδομένων προσωπικού χαρακτήρα. Ιδίως στην περίπτωση που το τρίτο μέρος αποτελεί εκτελούντα την επεξεργασία, τότε πρέπει η σύμβαση να ικανοποιεί πλήρως το άρθρο 28 του GDPR.

Το τρίτο μέρος επικουρεί την ΕΕΤΤ με τα κατάλληλα τεχνικά και οργανωτικά μέτρα, στο βαθμό που αυτό είναι δυνατό, για την εκπλήρωση της υποχρέωσης συμμόρφωσης με το νομοθετικό και κανονιστικό πλαίσιο περί προστασίας δεδομένων προσωπικού χαρακτήρα και κυβερνοασφάλειας. Επίσης, θέτει στη διάθεση της ΕΕΤΤ κάθε απαραίτητη πληροφορία προς απόδειξη της συμμόρφωσης αυτής.

5.2 Πολιτική ασφαλείας του τρίτου μέρους

Το τρίτο μέρος πρέπει να διατηρεί μια εγκεκριμένη από τη Διοίκησή του πολιτική ασφάλειας που θα βασίζεται σε αναγνωρισμένα πρότυπα ασφαλείας και βέλτιστες πρακτικές. Η πολιτική αυτή θα αποτελεί την δέσμευση του τρίτου μέρους αναφορικά με την ασφάλεια της πληροφορίας και την προστασία δεδομένων προσωπικού χαρακτήρα. Ενδεικτικά, θα ρυθμίζει θέματα ισχυρού συνθηματικού, ενεργοποίησης/απενεργοποίησης λογαριασμών χρηστών, πολιτικής καθαρού γραφείου, ασφάλειας ανθρώπινου δυναμικού, διαχείρισης πληροφοριακών πόρων, διαχείρισης προσωπικών δεδομένων, διαχείρισης ασφαλούς δικτύου, κρυπτογράφησης, ψευδωνυμοποίησης, ανωνυμοποίησης, διαχείρισης συμβάντων ασφαλείας, επιχειρησιακής συνέχειας, ανάκαμψης από καταστροφές, κτλ.

Το τρίτο μέρος πρέπει να συμφωνήσει στη συναπτόμενη σύμβαση να παρέχει αντίγραφο της πολιτικής του αυτής στην ΕΕΤΤ μετά από αίτημά της. Ομοίως πρέπει να συμφωνήσει να παρέχει, μετά από σχετικό αίτημα της ΕΕΤΤ, τεκμηρίωση συμμόρφωσης με τα πρότυπα ασφαλείας, τις βέλτιστες πρακτικές και απαιτήσεις ασφαλείας που επικαλείται ότι ακολουθεί. Σε περιπτώσεις έργων/υπηρεσιών/προμηθειών υψηλού κινδύνου, η σύμβαση θα μπορούσε να απαιτεί το τρίτο μέρος να διατηρεί ενεργή πιστοποίηση με ένα διεθνώς αναγνωρισμένο πρότυπο ασφάλειας πληροφοριών, όπως το ISO 27001.

Το τρίτο μέρος πρέπει να δεσμευτεί ότι επεξεργάζεται/χρησιμοποιεί τους πληροφοριακούς πόρους της ΕΕΤΤ αποκλειστικά και μόνο για το σκοπό παροχής στην ΕΕΤΤ των υπηρεσιών που έχουν συμφωνηθεί στη μεταξύ τους σύμβαση. Δεν επιτρέπεται να αντιγράφει έγγραφα, πληροφορίες και δεδομένα της ΕΕΤΤ άνευ εξουσιοδότησης. Θα παρέχει τις υπηρεσίες του σύμφωνα με τη σύμβαση και δεν θα διαθέτει σε τρίτους πληροφορίες της ΕΕΤΤ χωρίς την προηγούμενη γραπτή έγκρισή της.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

Το τρίτο μέρος θα διαβιβάζει πληροφορία μέσω ασφαλών καναλιών που είναι κρυπτογραφημένα. Διαβίβαση, αποθήκευση ή επεξεργασία προσωπικών δεδομένων εκτός Ευρωπαϊκής Ένωσης θα επιχειρείται μόνο μετά από γραπτή έγκριση της ΕΕΤΤ και αφού πρώτα το τρίτο μέρος δώσει πλήρεις λεπτομέρειες των δεδομένων, τοποθεσιών, εγγυήσεων και ότι άλλο ζητήσει η ΕΕΤΤ.

Το τρίτο μέρος θα λαμβάνει οργανωτικά και τεχνικά μέτρα προστασίας έναντι κάθε εσκεμμένης ή εκ παραδρομής ή μη εξουσιοδοτημένης αποκάλυψης, πρόσβασης, εκμετάλλευσης, τροποποίησης, καταστροφής, απώλειας πληροφορίας της ΕΕΤΤ που έχει στην κατοχή του το ίδιο ή οι υπεργολάβοι του. Θα τεκμηριώνει ότι εφαρμόζει πολιτικές ασφαλείας κατά τη χρήση φορητών υπολογιστών, τηλεργασίας και μέσων επικοινωνίας στο πλαίσιο εργασίας του για την ΕΕΤΤ. Θα τεκμηριώνει ότι διαθέτει πολιτικές και διαδικασίες ασφαλούς διατήρησης και διαγραφής / καταστροφής των εγγράφων, δεδομένων και πληροφοριών της ΕΕΤΤ.

Το ανθρώπινο δυναμικό του τρίτου μέρους που διαχειρίζεται πληροφοριακούς πόρους της ΕΕΤΤ πρέπει να είναι ενήμερο και εκπαιδευμένο στην πολιτική ασφαλείας του.

Το τρίτο μέρος θα εκτελεί ελέγχους ασφαλείας, θα αξιολογεί τις διεργασίες του για τη διαχείριση της ασφάλειας των πληροφοριακών πόρων της ΕΕΤΤ σε τακτική βάση και θα ενημερώνει την ΕΕΤΤ για τυχόν προσαρμογές που διενεργεί σε αυτές.

Ειδικότερα θέματα αναφορικά με την ασφάλεια των πληροφοριών από τα τρίτα μέρη αναλύονται στις επόμενες ενότητες.

5.3 Συμμόρφωση τρίτου μέρους με πολιτικές ασφάλειας της ΕΕΤΤ

Η σύμβαση πρέπει να διασφαλίζει τη συμμόρφωση του τρίτου μέρους με κατάλληλες πολιτικές της ΕΕΤΤ ανάλογα και με το αντικείμενό της.

Όλα τα τρίτα μέρη δεσμεύονται από τα οριζόμενα στην παρούσα πολιτική. Στην περίπτωση προμηθειών ή ανάπτυξης πληροφοριακών συστημάτων εφαρμόζεται η Πολιτική Προμήθειας και Ανάπτυξης Συστημάτων. Η πρόσβαση και χρήση του εξοπλισμού, των συστημάτων, των υπηρεσιών και των πληροφοριών της ΕΕΤΤ διέπεται από τις πολιτικές τελικού χρήστη και αποδεκτής χρήσης πληροφοριακών αγαθών κ.ο.κ.

Ειδικότερες απαιτήσεις αναφορικά με τη συμμόρφωση των τρίτων μερών με πολιτικές ασφαλείας της ΕΕΤΤ αναφέρονται στις επόμενες ενότητες.

5.4 Σύμβαση εμπιστευτικότητας

Η ΕΕΤΤ πρέπει να διασφαλίζει ότι υπογράφεται σύμβαση εμπιστευτικότητας από το τρίτο μέρος και τους υπεργολάβους του, πριν του επιτραπεί η πρόσβαση στις πληροφορίες και / ή τα πληροφοριακά συστήματα της ΕΕΤΤ.

Οι υπεργολάβοι ή/και υποπρομηθευτές του συμβαλλόμενου τρίτου μέρους υπάγονται στις ίδιες απαιτήσεις ασφάλειας πληροφοριών με το τρίτο μέρος.

5.5 Δικαίωμα του δημιουργού, πνευματικής ιδιοκτησίας και ευρεσιτεχνίες

Πληροφορίες σχετικά με δικαιώματα του δημιουργού, δικαιώματα στην πνευματική ιδιοκτησία και ευρεσιτεχνίες πρέπει να εμπεριέχονται στις συμβάσεις με τα τρίτα μέρη.

5.6 Καταγραφή και ταξινόμηση της πληροφορίας

Το τρίτο μέρος θα επιβεβαιώνει ότι οι πληροφοριακοί πόροι της ΕΕΤΤ που αποτελούν αρμοδιότητά του στο πλαίσιο της σύμβασης με την ΕΕΤΤ είναι καταγεγραμμένοι στο Μητρώο Πληροφοριακών Πόρων και ταξινομημένοι σύμφωνα με την Πολιτική Διαχείρισης Πληροφοριακών Πόρων της ΕΕΤΤ και η διαχείρισή τους είναι ανάλογη προς την ταξινόμηση αυτή. Επομένως, στην περίπτωση προμήθειας ή ανάπτυξης πληροφοριακού συστήματος ή εφαρμογής, το τρίτο μέρος πρέπει να παρέχει την ταξινόμηση του συστήματος ή της εφαρμογής. Περαιτέρω, εφόσον το πληροφοριακό σύστημα ή η εφαρμογή διαχειρίζεται

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

προσωπικά δεδομένα και απαιτείται σύμφωνα με τον GDPR, να συνδράμει στην εκπόνηση μελέτης εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων (ΕΑΠΔ ή αλλιώς DPIA).

Επίσης, θα εξασφαλίζει ότι οποιοδήποτε μέσο που χρησιμοποιείται για καταγραφή, αποθήκευση ή επεξεργασία πληροφορίας της ΕΕΤΤ στο πλαίσιο των υπηρεσιών που παρέχει στην ΕΕΤΤ, συμπεριλαμβανομένων εγγράφων σε φυσική μορφή, φορητών υπολογιστών, φορητών μέσων αποθήκευσης κτλ., διαχειρίζεται, μεταφέρεται και κρυπτογραφείται με ασφάλεια και ότι η χρήση του είναι εξουσιοδοτημένη.

5.7 Διαχείριση αλλαγών

Το τρίτο μέρος θα εκτελεί αλλαγές στα συστήματα της ΕΕΤΤ, στο πλαίσιο των συμβατικών υποχρεώσεών του, σύμφωνα με την Πολιτική Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα. Όπου είναι εφικτό, θα καταγράφονται οι αλλαγές για σκοπούς ελέγχου και προστασίας της ασφάλειας.

Η διαχείριση των αλλαγών στα συστήματα της ΕΕΤΤ που φιλοξενούνται σε εγκαταστάσεις τρίτων μερών (είτε τα διαχειρίζονται τρίτα μέρη είτε η ίδια η ΕΕΤΤ) πρέπει να προβλέπεται και να ρυθμίζεται κατάλληλα στις σχετικές προκηρύξεις διαγωνισμών και στις συμβάσεις που υπογράφονται μεταξύ της ΕΕΤΤ και των τρίτων μερών.

5.8 Διαχείριση ελέγχου πρόσβασης

Έλεγχοι Προσβάσεων στα πληροφοριακά συστήματα που εμπλέκονται στις συνδέσεις μεταξύ ΕΕΤΤ και τρίτου μέρους πρέπει να γίνονται σύμφωνα με την πολιτική της ΕΕΤΤ για τη διαχείριση προσβάσεων χρηστών. Η πρόσβαση θα περιορίζεται στο ανθρώπινο δυναμικό που τη χρειάζεται για να εκτελέσει τα καθήκοντά του σύμφωνα με τις συμβατικές υποχρεώσεις.

Τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται εμπιστευτικές πληροφορίες ή δεδομένα προσωπικού χαρακτήρα θα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας ή τελούν υπό τη δέουσα κανονιστική υποχρέωση τήρησης εμπιστευτικότητας.

Το τρίτο μέρος απαγορεύεται να εκχωρήσει δικαιώματα πρόσβασης χωρίς την άδεια της ΕΕΤΤ.

5.9 Διαχείριση της ασφάλειας δικτύων

Το τρίτο μέρος πρέπει να χρησιμοποιεί ασφαλείς αρχιτεκτονικές και λειτουργίες δικτύων και να διασφαλίζει ότι τα δίκτυα που μεταφέρουν τα δεδομένα της ΕΕΤΤ έχουν σχεδιαστεί, κατασκευαστεί, ελέγχονται και διαχειρίζονται σύμφωνα με τα πρότυπα ασφαλείας και τις βέλτιστες πρακτικές, προκειμένου να εμποδίζουν την χωρίς εξουσιοδότηση πρόσβαση στην πληροφορία της ΕΕΤΤ.

Το τρίτο μέρος χρησιμοποιεί μέτρα προστασίας έναντι της παραβίασης δεδομένων (π.χ. μέτρα ελέγχου της πρόσβασης) και εξασφαλίζει ότι απαγορεύεται και δεν χρησιμοποιείται οιαδήποτε παράκαμψη των μηχανισμών ασφάλειας.

5.10 Πιστοποίηση συνδέσεων από απόσταση

Η από απόσταση πρόσβαση στα πληροφοριακά συστήματα της ΕΕΤΤ από τρίτα μέρη και το αντίστροφο πρέπει να υπόκειται σε αυστηρούς μηχανισμούς πιστοποίησης των στελεχών των τρίτων μερών και μη αποποίησης των ενεργειών τους, όπου αυτό είναι εφικτό.

5.11 Επιστροφή πληροφοριακών πόρων

Η ΕΕΤΤ πρέπει να διασφαλίζει ότι η σύμβαση που υπογράφεται με το τρίτο μέρος, καθορίζει με σαφήνεια τις υποχρεώσεις του τρίτου μέρους περί επιστροφής όλου το υλικού και του λογισμικού, συμπεριλαμβανομένων των αποθηκευμένων πληροφοριών/δεδομένων τα οποία ανήκουν στην ΕΕΤΤ μετά τη λήξη ή καταγγελία της σύμβασης ή τη μεταβίβαση της σύμβασης

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

σε άλλο τρίτο μέρος. Επίσης, πρέπει να εξασφαλίζει την ασφαλή διαγραφή/καταστροφή τυχόν αντιγράφων δεδομένων, πληροφοριών ή εγγράφων.

5.12 Επιβεβαίωση της επάρκειας και της ακεραιότητας του προσωπικού του τρίτου μέρους

Τα τρίτα μέρη φέρουν την ευθύνη εφαρμογής μέτρων που θα επιβεβαιώνουν την επάρκεια και ακεραιότητα του προσωπικού τους που εμπλέκεται στη σύμβαση της ΕΕΤΤ.

Θα διασφαλίζουν ότι οι ρόλοι και οι αρμοδιότητες ασφάλειας πληροφοριών του προσωπικού τους είναι ορισμένοι και τεκμηριωμένοι. Παράλληλα θα εξασφαλίζουν ότι παρέχουν ολοκληρωμένες και σαφείς οδηγίες στο προσωπικό τους για την προστασία της ασφάλειας των πληροφοριακών πόρων της ΕΕΤΤ.

Το τρίτο μέρος θα ενημερώνει, εκπαιδεύει και ευαισθητοποιεί το ανθρώπινο δυναμικό του με δομημένο τρόπο και σε διαρκή βάση αναφορικά με την ασφάλεια. Το προσωπικό δεσμεύεται ότι συμφωνεί να συμμορφωθεί με όλες τις πολιτικές του τρίτου μέρους.

Η ΕΕΤΤ πρέπει να διασφαλίζει ότι σχετικές διατάξεις έχουν συμπεριληφθεί στη σύμβαση που υπογράφηκε με το τρίτο μέρος.

5.13 Διαχείριση υπεργολάβων του τρίτου μέρους

Τα τρίτα μέρη φέρουν την ευθύνη της διαχείρισης των υπεργολάβων τους που εμπλέκονται στη σύμβαση της ΕΕΤΤ. Όσα αναφέρονται παραπάνω για το προσωπικό του τρίτου μέρους ισχύουν και για τους υπεργολάβους του.

Το τρίτο μέρος θα ελέγχει τακτικά την ασφάλεια των υπεργολάβων του εφόσον αυτοί έχουν πρόσβαση στους πληροφοριακούς πόρους της ΕΕΤΤ και θα είναι σε θέση να τεκμηριώσει ότι διαθέτουν και εφαρμόζουν τα απαιτούμενα μέτρα ασφαλείας.

Το τρίτο μέρος δεν προσλαμβάνει υπεργολάβο χωρίς την προηγούμενη έγκριση της ΕΕΤΤ, εκτός εάν προβλέπεται διαφορετικά στη σύμβαση μεταξύ του τρίτου μέρους και της ΕΕΤΤ. Σε κάθε περίπτωση, το τρίτο μέρος υποχρεούται να αποκαλύπτει πληροφορίες σχετικά με βασικούς υπεργολάβους του που εμπλέκονται σε κρίσιμες επιχειρησιακές δραστηριότητες ή χειρίζονται ευαίσθητα δεδομένα.

Προκειμένου η ΕΕΤΤ να μειώσει τον κίνδυνο από τους υπεργολάβους του τρίτου μέρους, πρέπει να εξετάζει την προσθήκη των ακόλουθων χαρακτηριστικών δικλείδων ασφαλείας σε κάθε νέα σύμβαση:

- *Να έχει η ΕΕΤΤ τη δυνατότητα να ελέγχει τη διαχείριση υπεργολάβων που διενεργεί το τρίτο μέρος ή να απαιτεί από αυτόν να της παρέχει εκθέσεις ελέγχου σε τακτική βάση.*
- *Το τρίτο μέρος να διασφαλίζει ότι οι υπεργολάβοι του συμμορφώνονται με ένα συγκεκριμένο πρότυπο ασφάλειας, απορρήτου ή/και συμμόρφωσης, όπως ενδεικτικά το ISO 27001.*
- *Να απαιτείται από το τρίτο μέρος να ειδοποιεί αμέσως την ΕΕΤΤ για τυχόν προβλήματα με υπεργολάβους του που θα μπορούσαν να την επηρεάσουν.*
- *Να καθορίζεται ρητά και με σαφήνεια η ευθύνη των μερών σε περίπτωση παραβίασης ασφάλειας ή απώλειας δεδομένων από τρίτους, κ.ο.κ.*

Η ΕΕΤΤ πρέπει να διασφαλίζει ότι σχετικές διατάξεις έχουν συμπεριληφθεί στη σύμβαση που υπογράφηκε με το τρίτο μέρος.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

5.14 Άμεση ενημέρωση για αλλαγές στο προσωπικό ή στους υπεργολάβους του τρίτου μέρους

Η ΕΕΤΤ πρέπει να διασφαλίζει ότι η σύμβαση που υπογράφηκε με το τρίτο μέρος προσδιορίζει με σαφήνεια τις ευθύνες του τρίτου μέρους σχετικά με αλλαγές στο προσωπικό ή τους υπεργολάβους που εμπλέκονται στη συνεργασία με την ΕΕΤΤ.

Το τρίτο μέρος υποχρεούται να γνωστοποιεί άμεσα στην ΕΕΤΤ κάθε αλλαγή των στελεχών της ομάδας του ή των υπεργολάβων του, κατά τη διάρκεια της σύμβασης, καθώς και τις απαιτούμενες πληροφορίες και τεκμηρίωση σχετικά με κάθε στέλεχος ή νέο υπεργολάβο που το τρίτο μέρος προτίθεται να χρησιμοποιεί εν συνεχεία στην εν λόγω σύμβαση, διασφαλίζοντας την ομαλή εκτέλεση της σύμβασης. Οποιαδήποτε αλλαγή τελεί υπό τη γραπτή έγκριση της ΕΕΤΤ.

Είναι κρίσιμο η ΕΕΤΤ να ενημερώνεται άμεσα για τέτοιες αλλαγές, ώστε να ανακαλεί αμέσως τα δικαιώματα πρόσβασης των αποχωρησάντων.

5.15 Εκμετάλλευση και αναφορά πιθανών αδυναμιών ασφαλείας

Η ΕΕΤΤ και τα τρίτα μέρη οφείλουν να μην εκμεταλλεύονται πιθανές αδυναμίες ασφάλειας τεχνικού, οργανωτικού, διαδικαστικού ή οποιουδήποτε άλλου είδους, με στόχο να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στα πληροφοριακά συστήματα του άλλου μέρους.

Τα κενά ή οι αδυναμίες της ασφάλειας που τυχόν εντοπιστούν, θα πρέπει να αναφέρονται άμεσα στο αντισυμβαλλόμενο μέρος.

5.16 Φυσική ασφάλεια των εγκαταστάσεων των τρίτων

Όταν η διαχείριση ενός πληροφοριακού συστήματος κρίσιμης σημασίας έχει ανατεθεί σε τρίτο μέρος και οι σχετικές ενέργειες εκτελούνται στις εγκαταστάσεις του τρίτου μέρους, ή όταν τα πληροφορικά συστήματα της ΕΕΤΤ φιλοξενούνται στις εγκαταστάσεις τρίτου μέρους, τότε πρέπει να διενεργούνται έλεγχοι φυσικής και περιβαλλοντικής ασφάλειας όμοιοι με αυτούς που γίνονται στις εγκαταστάσεις της ΕΕΤΤ.

5.17 Αναφορά προβλημάτων και συμβάντων ασφαλείας

Τα τρίτα μέρη πρέπει να χρησιμοποιούν μία προκαθορισμένη διαδικασία διαχείρισης και αντιμετώπισης συμβάντων ασφαλείας. Το προσωπικό τους πρέπει να αναφέρει κάθε αδυναμία συστήματος ή διαδικασίας και κάθε συμβάν που υποπέσει στην αντίληψή του στο τρίτο μέρος.

Τόσο τα τρίτα μέρη όσο και η ΕΕΤΤ πρέπει να αναφέρουν άμεσα μεταξύ τους όλα τα προβλήματα και συμβάντα ασφαλείας (π.χ. παραβίαση ή απώλεια δεδομένων), που σχετίζονται με τη συνεργασία τους ή τη σύνδεση/πρόσβαση του τρίτου μέρους στα συστήματα της ΕΕΤΤ.

Η διαδικασία και το χρονικό πλαίσιο ενημέρωσης της ΕΕΤΤ από το τρίτο μέρος σε περίπτωση περιστατικού πρέπει να είναι προκαθορισμένα ανάμεσα στα δύο μέρη και ανάλογα της σοβαρότητας του συμβάντος. Αναφορικά με την αντιμετώπιση και τα επίπεδα κλιμάκωσης του συμβάντος ασφαλείας ακολουθείται από την ΕΕΤΤ η Πολιτική Διαχείρισης Συμβάντων Ασφαλείας Πληροφοριών. Το τρίτο μέρος υποχρεούται να παρέχει κάθε πληροφορία που διαθέτει ώστε να συνδράμει στην επίλυση του συμβάντος και στην ενημέρωση των αρμόδιων αρχών.

Η ΕΕΤΤ πρέπει να διασφαλίζει ότι η υπογεγραμμένη σύμβαση με το τρίτο μέρος καθορίζει με σαφήνεια τα σημεία επαφής και επικοινωνίας.

5.18 Δικαίωμα ελέγχου της ασφάλειας του τρίτου

Στη συναπτόμενη σύμβαση η ΕΕΤΤ διατηρεί το δικαίωμα να ελέγχει, χρησιμοποιώντας είτε δικό της προσωπικό είτε τρίτους, τη συμμόρφωση του τρίτου μέρους με την παρούσα, καθώς

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

και τους μηχανισμούς ασφαλείας που χρησιμοποιεί το αντισυμβαλλόμενο τρίτο μέρος για τη διαχείριση και την προστασία των πληροφοριών και / ή των πληροφοριακών συστημάτων της ΕΕΤΤ (τόσο σε λογικό, όσο και σε φυσικό επίπεδο). Το τρίτο μέρος θέτει στη διάθεση της ΕΕΤΤ κάθε απαραίτητη πληροφορία προς απόδειξη της συμμόρφωσής του προς τις υποχρεώσεις που απορρέουν από το νομοθετικό και κανονιστικό πλαίσιο και από την παρούσα και επιτρέπει και διευκολύνει τους ελέγχους και τις επιθεωρήσεις που διενεργούνται από την ΕΕΤΤ ή από άλλον εντεταλμένο της. Με τον τρόπο αυτό κατά τη διάρκεια της σύμβασης παρακολουθείται η απόδοση του τρίτου μέρους στα θέματα ασφάλειας και προστασίας προσωπικών δεδομένων. Μάλιστα, στην περίπτωση σύναψης σύμβασης που εκτιμάται ως υψηλού κινδύνου από πλευράς ασφάλειας, συνιστάται αυτή να καθορίζει τον έλεγχο του τρίτου μέρους σε τακτική περιοδική βάση, για παράδειγμα ετησίως.

Επίσης, έλεγχοι πρέπει να διενεργούνται για την εκτίμηση κινδύνων αναφορικά με τα τρίτα μέρη και τότε αυτά θα πρέπει να λαμβάνουν άμεσα μέτρα περιορισμού αυτών των κινδύνων. Συνιστάται η σύμβαση να ορίζει τη συχνότητα ανάλυσης κινδύνων του τρίτου μέρους και ποια θα είναι τα επόμενα βήματα εάν η ανάλυση κινδύνου αναδείξει ευρήματα υψηλού ρίσκου.

5.19 Κυρώσεις για μη συμμόρφωση

Η ΕΕΤΤ πρέπει να διασφαλίζει ότι η σύμβαση που υπογράφεται με το τρίτο μέρος καθορίζει με σαφήνεια τις συνέπειες για τη μη συμμόρφωση με το πλαίσιο ασφάλειας πληροφοριών της ΕΕΤΤ και γενικότερα τις κυρώσεις στην περίπτωση παραβίασης των συμφωνηθέντων, όπως ενδεικτικά κατάργηση των δικαιωμάτων πρόσβασης, ποινικές ρήτρες ή/και καταγγελία σύμβασης. Η σύμβαση πρέπει να περιλαμβάνει το σχέδιο δράσης της ΕΕΤΤ στην περίπτωση που το τρίτος μέρος αποτύχει στις υπηρεσίες που παρέχει.

6. Παρακολούθηση και διαχείριση της συνεργασίας με τα τρίτα μέρη

6.1 Παρακολούθηση της συμμόρφωσης προς τα συμφωνηθέντα

Σύμφωνα με το νομοθετικό πλαίσιο, η ΕΕΤΤ ορίζει αρμόδιο συλλογικό όργανο, την Επιτροπή Παρακολούθησης και Παραλαβής, με την αρμοδιότητα της παρακολούθησης και παραλαβής της σύμβασης που συνάπτει με το τρίτο μέρος.

Η ΕΕΤΤ πρέπει να εποπτεύει και να ελέγχει τα τρίτα μέρη και να διασφαλίζει ότι όλα τα τρίτα μέρη στα οποία δίνεται πρόσβαση στα πληροφοριακά συστήματά της, αντιλαμβάνονται την ανάγκη για προστασία των πληροφοριών της ΕΕΤΤ και εκτελούν τα καθήκοντά τους σε συμμόρφωση με τις πολιτικές και τα συμφωνημένα στη σύμβαση. Οι κίνδυνοι που απορρέουν από τη συνεργασία πρέπει να παρακολουθούνται διαρκώς.

6.2 Επικοινωνία και αναφορές για την πρόοδο των εργασιών

Κατά την παρακολούθηση της σύμβασης, εφαρμόζεται το προκαθορισμένο σχέδιο επικοινωνίας μεταξύ των δύο μερών. Το τρίτο μέρος αποστέλλει τις αναφορές και τα αρχεία τεκμηρίωσης για την πρόοδο των εργασιών σύμφωνα με τα συμφωνηθέντα, ενώ η ΕΕΤΤ τα μελετά και καθίσταται ενήμερη για τις εξελίξεις, με σκοπό τον έγκαιρο εντοπισμό, την ενημέρωση της Διοίκησης όταν απαιτείται και την αποτελεσματική αντιμετώπιση των προβλημάτων που ενδεχομένως προκύπτουν.

6.3 Συνεχής αξιολόγηση καταλληλότητας τρίτου

Η καταλληλότητα του τρίτου μέρους πρέπει να αξιολογείται συνεχώς και να μην περιορίζεται στην αρχική εκτίμηση.

Κάθε αρνητική πληροφορία που έρχεται σε άμεση ή έμμεση γνώση της ΕΕΤΤ και αφορά τρίτο μέρος, πρέπει να ελέγχεται και να επιβεβαιώνεται.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

7. Έλεγχος των συνδέσεων / προσβάσεων

7.1 Τακτική ανασκόπηση των δικαιωμάτων πρόσβασης χρήστη

Τα δικαιώματα πρόσβασης χρήστη για κάθε σύνδεση μεταξύ ΕΕΤΤ και τρίτου μέρους πρέπει να ελέγχονται τακτικά.

7.2 Τακτική ανασκόπηση των συνδέσεων στα συστήματα

Η λίστα με τα εξουσιοδοτημένα τρίτα μέρη που έχουν συνδεθεί με τα πληροφοριακά συστήματα της ΕΕΤΤ πρέπει να ελέγχεται σε τακτά χρονικά διαστήματα, ώστε να επιβεβαιώνεται η επιχειρησιακή ανάγκη των εν λόγω συνδέσεων.

Οι λογαριασμοί πρόσβασης πρέπει να απενεργοποιούνται άμεσα μόλις παύουν να είναι απαραίτητοι ή σε περίπτωση σημαντικής παραβίασης των κανόνων ασφαλείας.

7.3 Ενεργοποίηση καταγραφής συμβάντων ασφαλείας

Η παρακολούθηση της δραστηριότητας και καταγραφή συμβάντων ασφαλείας πρέπει να είναι πλήρως ενεργοποιημένη σε όλα τα πληροφοριακά συστήματα στα οποία παρέχεται πρόσβαση σε τρίτα μέρη.

8. Αλλαγές στην Πολιτική Διαχείρισης Τρίτων Μερών

Η ΕΕΤΤ θα επανεξετάζει σε τακτική βάση την παρούσα πολιτική διαχείρισης τρίτων μερών και ενδέχεται να την τροποποιεί / επικαιροποιεί, χωρίς προηγούμενη ειδοποίηση, προκειμένου να ανταποκρίνεται στα πρότυπα ασφαλείας, στις εξελίξεις της νομοθεσίας και των υπηρεσιακών αναγκών της. Τα τρίτη μέρη οφείλουν, μέσα σε εύλογο χρονικό διάστημα, να συμμορφώνονται στις αλλαγές της παρούσας που παρέχονται σε γραπτή μορφή.

»

2. **Εντέλλεται** την κοινοποίηση της παρούσας Απόφασης στο προσωπικό της ΕΕΤΤ μέσω ανάρτησής της στη Γνωσιακή Πύλη (portal) και αποστολής της με μήνυμα ηλεκτρονικού ταχυδρομείου.
3. **Εντέλλεται** την ανάρτηση της παρούσας Απόφασης στο διαδικτυακό τόπο της ΕΕΤΤ προς ενημέρωση των τρίτων μερών.
4. **Εξουσιοδοτεί** τον Πρόεδρο της ΕΕΤΤ όπως:
    - Προβεί σε κάθε διαδικαστική ενέργεια ή έκδοση πράξης, που θα διευκολύνει την έγκαιρη και πλήρη ολοκλήρωση κάθε δράσης που αφορά στην εφαρμογή της *«Πολιτικής Διαχείρισης Τρίτων Μερών»*.
    - Τροποποιεί την *«Πολιτική Διαχείρισης Τρίτων Μερών»*, όποτε αυτό απαιτείται, για να ευθυγραμμίζεται με τις τρέχουσες ανάγκες και εξελίξεις.

Ο ΠΡΟΕΔΡΟΣ

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

ΚΑΘΗΓΗΤΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ ΜΑΣΣΕΛΟΣ

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr