ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ
ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ
«ΔΙΟΙΚΗΣΗ, ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΠΟΙΟΤΗΤΑ»

ΔΙΑΤΡΙΒΗ ΕΠΙΠΕΔΟΥ ΜΑΣΤΕΡ

ΤΙΤΛΟΣ ΔΙΑΤΡΙΒΗΣ

Μελέτη Ασφάλειας Προσωπικών Δεδομένων στην Ηλεκτρονική Διακυβέρνηση

ΠΑΝΑΓΙΩΤΗΣ ΚΑΠΕΤΑΝΑΚΗΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ
ΔΗΜΗΤΡΙΟΣ ΦΩΛΙΝΑΣ

ΠΑΤΡΑ, ΔΕΚΕΜΒΡΙΟΣ 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Οικονομικών Επιστημών και Διοίκησης

Μεταπτυχιακό Πρόγραμμα Σπουδών

Διοίκηση, Τεχνολογία και Ποιότητα

Μεταπτυχιακή Διατριβή

Μελέτη Ασφάλειας Προσωπικών Δεδομένων στην Ηλεκτρονική Διακυβέρνηση

Παναγιώτης Καπετανάκης

Επιβλέπων Καθηγητής

Δημήτριος Φωλίνας

Δεκέμβριος, 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Οικονομικών Επιστημών και Διοίκησης

Μεταπτυχιακό Πρόγραμμα Σπουδών

Διοίκηση, Τεχνολογία και Ποιότητα

Μεταπτυχιακή Διατριβή

Μελέτη Ασφάλειας Προσωπικών Δεδομένων στην Ηλεκτρονική Διακυβέρνηση

Παναγιώτης Καπετανάκης

Επιβλέπων Καθηγητής

Δημήτριος Φωλίνας

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στη Διοίκηση, Τεχνολογία και Ποιότητα.
από τη Σχολή Οικονομικών Επιστημών και Διοίκησης
του Ανοικτού Πανεπιστημίου Κύπρου.

Δεκέμβριος, 2019

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Στην παρούσα διπλωματική εργασία μελετάται η ασφάλεια των προσωπικών δεδομένων στα πλαίσια της Ηλεκτρονικής Διακυβέρνησης. Πιο συγκεκριμένα και στα πλαίσια αυτά, διερευνώνται οι πολιτικές ασφάλειας που χρησιμοποιεί ο Οργανισμός Τηλεπικοινωνιών Ελλάδας – ΟΤΕ ώστε να διασφαλίσει την προστασία των Προσωπικών Δεδομένων των πολιτών.

Οδηγό στην κατεύθυνση αυτή αποτελεί ο νέος Ευρωπαϊκός Γενικός Κανονισμός για τα Προσωπικά Δεδομένα (GDPR), η θέσπιση του οποίου παρέχει ισχυρότερη προστασία στους πολίτες καθώς όλοι οι εμπλεκόμενοι στην Ηλεκτρονική Διακυβέρνηση φορείς υποχρεούνται να τηρούν τα απαραίτητα μέτρα ασφαλείας για τα προσωπικά δεδομένα των πολιτών τα οποία διαχειρίζονται.

Στα πλαίσια λοιπόν των αναγκών του Απορρήτου των Τηλεπικοινωνιών έχουν θεσπιστεί οι αντίστοιχες πολιτικές ασφαλείας καθώς και ο Κώδικας Δεοντολογίας για την Προστασία των Δικαιωμάτων του Ατόμου κατά την Επεξεργασία των Προσωπικών Δεδομένων του εντός του ΟΤΕ.

Για την υλοποίηση της μελέτης χρησιμοποιήθηκε ερωτηματολόγιο ανοικτού τύπου του οποίου σκοπός ήταν να διερευνηθεί ο βαθμός στον οποίο εφαρμόζονται πολιτικές ασφάλειας καθώς και ο Γενικός Κανονισμός για τα Προσωπικά Δεδομένα (GDPR) εντός του Οργανισμού Τηλεπικοινωνιών Ελλάδας.

Αποδεικνύεται μέσα από την έρευνα σε μέγιστο ποσοστό η πλήρης λήψη εσωτερικών οργανωτικών και τεχνικών μέτρων για την ασφάλεια προσωπικών δεδομένων. Ως αποτέλεσμα της καθολικής τήρησης των γενικών υποχρεώσεων του Οργανισμού Τηλεπικοινωνιών Ελλάδας στην επεξεργασία των προσωπικών δεδομένων των πολιτών έχουμε την εμπιστοσύνη και των πολιτών απέναντι του.

Λέξεις Κλειδιά: Ηλεκτρονικής Διακυβέρνηση, Πολιτικές Ασφάλειας, Γενικός Κανονισμός για τα Προσωπικά Δεδομένα –GDPR.

Summary

The present thesis examines the security of personal data in the context of E-Government. Specifically, and in this context, we investigate the security policies used by OTE to ensure the protection of citizens' personal data.

Guided in this direction is the new European General Data Protection Regulation (GDPR), which provides stronger protection for citizens as all eGovernment stakeholders are required to comply with the necessary security measures for the privacy of citizens who manage.

Therefore, in accordance with the requirements of the Telecommunications Privacy, the respective security policies as well as the Code of Conduct for the Protection of Human Rights during the Processing of Personal Data within OTE have been adopted.

An open-ended questionnaire was used to conduct the study to investigate the extent to which security policies are implemented and the General Regulation on Personal Data (GDPR) within the Greek Telecommunications Organization.

The research demonstrates to the fullest extent possible the complete adoption of internal organizational and technical measures for the security of personal data. As a result of the universal compliance of the Greek Telecommunications Organization with the processing of citizens' personal data, we have the confidence of the public as well.

Keywords: E-Government, Security Policies, General Privacy Policy -GDPR.

Ευχαριστίες

Την σύντροφο μου και μέλλουσα σύζυγό μου Σοφία Στασινού, για την αμέριστη συμπαράσταση και κατανόηση που είχε στο να μπορέσω να φέρω εις πέρας την διπλωματική διατριβή και να καταφέρω να ολοκληρώσω τον κύκλο σπουδών μου.

Τον καθηγητή μου κύριο Δημήτριο Φωλίνα, για την εξαιρετική συνεργασία που είχαμε, την υπομονή του, την ηρεμία του μαζί με τις πολύτιμες συμβουλές και γνώσεις του, που είχαν ως αποτέλεσμα την εκπόνηση της παρούσας διατριβής.

Το Ανοικτό Πανεπιστήμιο Κύπρου, που με την οργάνωσή του μου έδωσε την ευκαιρία να εμβαθύνω σε νέες γνώσεις και με το πολύ οργανωμένο eclass παρείχε τους καλύτερους πόρους, κατά τη διάρκεια της φοίτησης μου.

Τέλος θα ήθελα να ευχαριστήσω τους συναδέλφους μου από την Υποδιεύθυνση Ασφάλειας Προσωπικών δεδομένων για τον χρόνο που αφιέρωσαν με το ερωτηματολόγιο για να ασχοληθούν παρά το μεγάλο φόρτο εργασίας που είχαν.

Περιεχόμενα

Εισαγωγή.....1

1 Βιβλιογραφική Επισκόπηση.....**3**

1.0 Εισαγωγή Κεφαλαίου.....**3**

1.1 Ορισμός Ηλεκτρονικής Διακυβέρνησης 4

1.1.1 Εννοιολογική προσέγγιση, μοντέλα και τύποι, οφέλη και προκλήσεις 6

1.2 Ασφάλεια στο Ηλεκτρονικό Επιχειρείν και στην Ηλεκτρονική διακυβέρνηση 12

1.3 Ασφάλεια Προσωπικών Δεδομένων 15

1.4 Ασφάλεια Προσωπικών δεδομένων στην Ηλεκτρονική διακυβέρνηση.....19

1.5 Θεωρητικό Πλαίσιο.....21

2 Μεθοδολογία Έρευνας **22**

2.1 Προτεινόμενη Μεθοδολογία (Δευτερογενής & Πρωτογενής).....22

2.2 Δείγμα 24

2.3 Εργαλεία Έρευνας 24

2.4 Μεθοδολογία Έρευνας 26

3 Αποτελέσματα Έρευνας **28**

3.0 Εισαγωγή Κεφαλαίου.....28

3.1 Δευτερογενής Έρευνα: Πολιτικές Ασφάλειας & Προστασίας Δεδομένων στον ΟΤΕ.....29

3.1.1 Πολιτική Ασφάλειας 29

3.1.2 Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών 36

3.1.3 Διαχείριση Εξαιρέσεων από την Πολιτική Ασφάλειας 48

3.1.4 Εταιρικοί Δεσμευτικοί Κανόνες για την Προστασία Προσωπικών Δεδομένων εντός του Ομίλου της Deutsche Telekom 49

3.2 Εφαρμογή του GDPR εντός ΟΤΕ 49

3.2.1 Αιτιολογία Επεξεργασίας Προσωπικών Δεδομένων εντός ΟΤΕ 49

3.2.2 Επιχειρησιακές Μονάδες Πρόσβασης Προσωπικών Δεδομένων εντός ΟΤΕ 51

3.2.3 Μεταφορά Προσωπικών Δεδομένων σε τρίτες χώρες 51

3.2.4 Τα δικαιώματά πολιτών σχετικά με την προστασία των δεδομένων τους 52

3.2.5 Τα δικαιώματά πολιτών σχετικά με την προστασία των δεδομένων τους 52

3.3 Πρωτογενής Έρευνα: Αποτελέσματα Ερωτηματολογίου 53

4 Συζήτηση Αποτελεσμάτων 61

4.1 Σκοπός και Οφέλη Εφαρμογής του GDPR..... 61

4.2 Αποτελέσματα Έρευνας..... 62

5 Συμπεράσματα Έρευνας –Προτάσεις 63

5.1 Συμπεράσματα Έρευνας 63

5.2 Περιορισμοί Έρευνας..... 65

5.3 Προτάσεις - Εκπαίδευση προσωπικού..... 65

5.4 Μελλοντικές Προτάσεις 66

Παραρτήματα

Α Γλωσσάρι Βασικών Εννοιών του GDPR 67

Β Νομοθεσία & Άλλες Διοικητικές Πράξεις 75

Γ Ερωτηματολόγιο..... 90

Βιβλιογραφία 92

ΕΙΣΑΓΩΓΗ

Η αλματώδης εξέλιξη της τεχνολογίας είχε ως αποτέλεσμα τη χρήση της σε κάθε τομέα που αφορά την εξυπηρέτηση των καθημερινών ενεργειών των πολιτών. Στο πλαίσιο αυτό, τέθηκε υπό αμφισβήτηση η πληθώρα των προσωπικών δεδομένων των πολιτών που ανταλλάσσονται στη διάρκεια των καθημερινών τους συναλλαγών και κατά πόσο αυτά διατηρούνται υπό ασφάλεια. Συνεπώς , οι σύγχρονες κοινωνίες έρχονται αντιμέτωπες με τις εξής προκλήσεις:

α) την απλοποίηση των διαδικασιών,
β) την αύξηση της διαφάνειας,
γ) τη μείωση της γραφειοκρατίας,
δ) τη μείωση του διοικητικού κόστους,
ε) την πάταξη της διαφθοράς.

Στην παρούσα διπλωματική διατριβή γίνεται προσπάθεια που έχει ως σκοπό να παρουσιάσει και να συνδυάσει μεταξύ τους βασικές έννοιες της θεωρίας της Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας Πληροφοριών που αφορούν στις παρεχόμενες υπηρεσίες στο δημόσιο τομέα. Δίνοντας λοιπόν έμφαση στον τομέα των Τηλεπικοινωνιών και συγκεκριμένα στον ΟΤΕ, που αποτελεί και αντικείμενο της παρούσας διατριβής, γίνεται μια εννοιολογική προσέγγιση της Ηλεκτρονικής Διακυβέρνησης όσον αφορά τα μοντέλα, τους τύπους, τα οφέλη και τις προκλήσεις. Εν συνεχεία, αποτυπώνεται η ανάγκη και η σημαντικότητα για περαιτέρω ασφάλεια των προσωπικών δεδομένων των πολιτών. Έτσι, παρουσιάζεται η θέσπιση τόσο σε Ευρωπαϊκό όσο και σε εθνικό επίπεδο, του Γενικού Κανονισμού Προστασίας Δεδομένων ο οποίος τέθηκε σε εφαρμογή από τις 25/5/2018 και έχει επιφέρει αλλαγές στη διαχείριση των ευαίσθητων προσωπικών δεδομένων.

Λαμβάνοντας υπόψη τα ανωτέρω, καθώς και το γεγονός ότι δεν έχει προηγηθεί κατά το παρελθόν παρόμοια έρευνα στον ΟΤΕ, πραγματοποιήθηκε δευτερογενής έρευνα η οποία αφορά την καταγραφή των Πολιτικών Ασφάλειας & Προστασίας Δεδομένων που εφαρμόζονται εντός του ΟΤΕ κι έχουν ως στόχο να παράσχουν ένα υψηλό επίπεδο ασφάλειας στους πολίτες , καθώς και στους εργαζόμενους, τις υπηρεσίες, τα προϊόντα, τα περιουσιακά στοιχεία και τις δραστηριότητες του ΟΤΕ. Επιπροσθέτως, πραγματοποιήθηκε και πρωτογενής ποιοτική έρευνα με τη χρήση ερωτηματολογίων που απαντήθηκαν από τους εργαζόμενους της Υποδιεύθυνσης Ασφάλειας Προσωπικών Δεδομένων του ΟΤΕ.

Τα αποτελέσματα της έρευνας αυτής αρχικά ενδιαφέρουν τη διοικητική ομάδα του ΟΤΕ, έτσι ώστε να υπερτονιστούν οι κρίσιμοι παράγοντες που συμβάλουν στην επιτυχία του συστήματος Ασφάλειας Προσωπικών Δεδομένων και στη λήψη των κατάλληλων μέτρων να για την περαιτέρω βελτίωση του. Δεύτερον, τους νομοθετικούς φορείς έτσι ώστε να αξιολογήσουν τα αποτελέσματα από την πρόσφατη αλλαγή της κείμενης νομοθεσίας. Τρίτον, όλους τους δημόσιους φορείς, για σύγκριση των διαδικασιών και την υιοθέτηση των βέλτιστων και πιο αποτελεσματικών πρακτικών. Τέταρτον, τους πολίτες αλλά και τους εξωτερικούς συνεργάτες του ΟΤΕ, ώστε να ενημερωθούν για τα δικαιώματα και την περαιτέρω προστασία των προσωπικών τους δεδομένων . Τέλος, την ακαδημαϊκή κοινότητα λόγω έλλειψης εκτενούς βιβλιογραφίας στη μελέτη πραγματικών περιπτώσεων Τηλεπικοινωνιακών Οργανισμών και του συστήματος ασφάλειας των προσωπικών δεδομένων.

Η διατριβή αποτελείται συνολικά από πέντε κεφάλαια. Στο πρώτο κεφάλαιο, περιλαμβάνεται η βιβλιογραφική έρευνα που αποσκοπεί στη σύνδεση βασικών εννοιών της Ηλεκτρονικής Διακυβέρνησης και των Πολιτικών Ασφάλειας προσωπικών δεδομένων. Στο δεύτερο κεφάλαιο αναλύεται η μεθοδολογία που εφαρμόστηκε στην έρευνα. Στο τρίτο κεφάλαιο παρουσιάζονται τα αποτελέσματα της έρευνας, αρχικά της δευτερογενούς και στη συνέχεια της πρωτογενούς η οποία πραγματοποιήθηκε με τη χρήση ερωτηματολογίου. Στο τέταρτο κεφάλαιο γίνεται συζήτηση τω αποτελεσμάτων της πρωτογενούς και της δευτερογενούς έρευνας. Τέλος, στο πέμπτο κεφάλαιο αναλύονται τα κυριότερα συμπεράσματα που προέκυψαν από την έρευνα και αναφέρονται οι προτάσεις για μελλοντική έρευνα

Κεφάλαιο 1

Βιβλιογραφική Επισκόπηση

"Καθένας έχει δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας. Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά, καθώς και της παραγωγής, ανταλλαγής και διάδοσής τους αποτελεί υποχρέωση του Κράτους"

Σύνταγμα της Ελλάδας, Άρθρο 5^{A}

1.0 Εισαγωγή Κεφαλαίου

Στο παρόν κεφάλαιο πραγματοποιείται εκτενής βιβλιογραφική έρευνα που έχει ως σκοπό να παρουσιάσει και να συνδυάσει μεταξύ τους βασικές έννοιες της θεωρίας της Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας Πληροφοριών που αφορούν στις παρεχόμενες υπηρεσίες στο δημόσιο τομέα. Δίνοντας λοιπόν έμφαση στον τομέα των Τηλεπικοινωνιών και συγκεκριμένα στον ΟΤΕ, που αποτελεί και αντικείμενο της παρούσας διατριβής, γίνεται μια εννοιολογική προσέγγιση της Ηλεκτρονικής Διακυβέρνησης όσον αφορά τα μοντέλα, τους τύπους, τα οφέλη και τις προκλήσεις. Επιπλέον, παρουσιάζονται οι μηχανισμοί ασφάλειας στο Ηλεκτρονικό Επιχειρείν και στην Ηλεκτρονική διακυβέρνηση. Τέλος, δίνεται έμφαση στην πρόσφατη θέσπιση, του Γενικού Κανονισμού για τα Προσωπικά Δεδομένα, από το Ευρωπαϊκό Κοινοβούλιο καθώς και τα οφέλη και τις προκλήσεις που έχει επιφέρει τόσο σε επίπεδο πολιτών όσο και σε επίπεδο Φορέων.

1.1 Τι είναι η ηλεκτρονική διακυβέρνηση;

Η Ηλεκτρονική διακυβέρνηση, ορίζεται ως εξής: Το σύνολο των δραστηριοτήτων που λαμβάνουν χώρα μέσω Τεχνολογίας Πληροφορικής και Επικοινωνιών ανάμεσα σε κάθε επίπεδο της κυβέρνησης, των πολιτών και της επιχειρηματικής κοινότητας, όπως: απόκτηση και παροχή προϊόντων και υπηρεσιών, διάθεση και λήψη παραγγελιών, παροχή και λήψη πληροφοριών και ολοκλήρωση των χρηματοοικονομικών συναλλαγών . Μπορεί να οριστεί ως – η δυνατότητα απόκτησης κρατικών υπηρεσιών , μέσω μη παραδοσιακών ηλεκτρονικών μέσων, επιτρέποντας έτσι την πρόσβαση σε κυβερνητικές πληροφορίες και την ολοκλήρωση δημοσίων συναλλαγών σε οποιοδήποτε μέρος, οποιαδήποτε στιγμή και με συμμόρφωση ως προς την απαίτηση για ίση πρόσβαση από όλους.

Οι λειτουργίες της Ηλεκτρονικής-διακυβέρνησης είναι η εξής:
Πρόσβαση των πολιτών σε κυβερνητικές πληροφορίες. Η παροχή πρόσβασης σε κυβερνητικές πληροφορίες είναι η πιο διαδεδομένη ψηφιακή μέθοδος ηλεκτρονικής διακυβέρνησης.

Διευκόλυνση της γενικής συμμόρφωσης. Η ηλεκτρονική -διακυβέρνηση μπορεί επίσης να σημαίνει την παροχή ηλεκτρονικής πρόσβασης σε υπηρεσίες που διευκολύνουν τη συμμόρφωση με ένα σύνολο οδηγιών ή κανονισμών.

Πρόσβαση των πολιτών σε προσωπικά οφέλη. Η ηλεκτρονική μεταφορά οφελών και οι online αιτήσεις για τη χορήγηση κρατικής βοήθειας είτε για την αποζημίωση του εργαζομένου, είναι παραδείγματα των υπηρεσιών που παρέχουν στον πολίτη ηλεκτρονική πρόσβαση σε προσωπικά οφέλη.

Προμήθειες συμπεριλαμβανομένων των διαγωνισμών, της αγοράς, και της πληρωμής. Οι Εφαρμογές προμηθειών επιτρέπουν σε κυβερνητικούς φορείς να δρέπουν τα οφέλη που πραγματοποιήθηκαν στον ιδιωτικό τομέα, μέσω εφαρμογών ηλεκτρονικού εμπορίου. Η ηλεκτρονική καταγραφή των πωλητών, οι παρατηρήσεις και οι ποινικοποιήσεις των διαγωνισμών ,οι ηλεκτρονικές αγορές και πληρωμές είναι συναλλαγές κυβέρνησης προς

κυβέρνηση και κυβέρνησης προς επιχειρήσεις που εξυπηρετούν τόσο τις ανάγκες των κυβερνητικών παραγόντων καθώς και τους ιδιωτικούς εμπορικούς εταίρους των.

Η συμμετοχή των πολιτών. Η ηλεκτρονική δημοκρατία περιλαμβάνει την πρόσβαση σε πληροφορίες και δεδομένα των εκλεγμένων μελών, φόρουμ συζητήσεων, εγγραφή ψηφοφόρων και online ψηφοφορία. Οι υπηρεσίες αυτές έχουν σκοπό να εξυπηρετούν την κοινωνία στο σύνολό της.

Βλέποντάς το από τεχνική άποψη, η ηλεκτρονική διακυβέρνηση είναι ένα ολοκληρωμένο εργαλείο που περιλαμβάνει τρία ενθαρρυντικά συστατικά της νέας τεχνολογίας: τις υποδομές, τις λύσεις και την εκμετάλλευση των δημοσίων δικτύων. Μία σωστή υποδομή ηλεκτρονικής διακυβέρνησης προωθεί την εγκατάσταση συγκεκριμένων εφαρμογών για την αντιμετώπιση ιδιαίτερων προβλημάτων και θεμάτων της κυβερνητικής διαχείρισης. Έτσι, κατά την παροχή πρόσβασης στο Internet και υπηρεσιών ηλεκτρονικού ταχυδρομείου σε δημόσια δίκτυα, οι πιο θετικές επιπτώσεις θα προέλθουν από τις λύσεις και τις υπηρεσίες που μπορεί να αποκτηθούν από την εκμετάλλευση των δημοσίων δικτύων μέσω αυτών των εργαλείων επικοινωνίας. Με βάση την εσωτερική και εξωτερική κυβερνητική τηλεπικοινωνία και Διαδικτυακή υποδομή, μέσω της αξιοποίησης των δημόσιων κυβερνητικών δικτύων μπορεί να δώσουν λύσεις για την παροχή δημόσιων υπηρεσιών.

Η ηλεκτρονική-διακυβέρνηση είναι πέρα από το πεδίο εφαρμογής της ηλεκτρονικής κυβέρνησης. Αν και η ηλεκτρονική κυβέρνηση ορίζεται ως μια απλή παροχή κρατικών υπηρεσιών και της ενημέρωσης του κοινού με τη χρήση ηλεκτρονικών μέσων, η ηλεκτρονική διακυβέρνηση επιτρέπει την άμεση συμμετοχή του πολίτη σε πολιτικές δραστηριότητες πέρα από την κυβέρνηση περιλαμβάνοντας την ηλεκτρονική-δημοκρατία, ηλεκτρονική -ψηφοφορία, και την on-line πολιτική δραστηριότητα. Έτσι, σε γενικές γραμμές, η έννοια της ηλεκτρονικής διακυβέρνησης θα συμπεριλάβει την κυβέρνηση, τη συμμετοχή των πολιτών, τα πολιτικά κόμματα και το Κοινοβούλιο.

Συνοψίζοντας την έννοια της ηλεκτρονικής διακυβέρνησης, καταλήγουμε στα εξής: η ηλεκτρονική -διακυβέρνηση δεν αφορά μόνο τα κυβερνητικά web sites . Δεν πρόκειται μόνο για την παροχή υπηρεσιών μέσω του Internet. Δεν πρόκειται μόνο για την ψηφιακή

πρόσβαση σε κυβερνητικές πληροφορίες ή τις ηλεκτρονικές πληρωμές. Θα αλλάξει τόσο τον τρόπο με τον οποίο οι πολίτες σχετίζονται με τις κυβερνήσεις όσο και τον τρόπο με τον οποίο σχετίζονται οι πολίτες μεταξύ τους. Η ηλεκτρονική διακυβέρνηση θα επιτρέψει στους πολίτες να επικοινωνούν με την κυβέρνηση, να συμμετέχουν στην κυβερνητική χάραξη πολιτικής και στη δημοκρατική πολιτική διαδικασία. Ως εκ τούτου, στην ευρύτερη έννοια του όρου, η ηλεκτρονική -διακυβέρνηση έχει περισσότερες συνέπειες από την ηλεκτρονική κυβέρνηση.

Η κατανόηση του ορισμού της ηλεκτρονικής κυβέρνησης που συμπυκνώνει μια ευρύτερη διάταξη της ανανέωσης μπορεί να είναι πιο χρήσιμη για να διακρίνονται αυτές οι δύο διαφορετικές έννοιες οι οποίες κατά τα αλλά συνδέονται μεταξύ τους. Η ηλεκτρονική -διακυβέρνηση αναφέρεται στη χρήση από τις κυβερνητικές υπηρεσίες των τεχνολογιών της πληροφορίας, όπως το Διαδίκτυο, τα κινητά και τους ηλεκτρονικούς υπολογιστές, που έχουν την ικανότητα να μετατρέπουν τις σχέσεις με τους πολίτες, τις επιχειρήσεις, καθώς και με άλλα σκέλη της κυβέρνησης. Οι τεχνολογίες αυτές μπορούν να χρησιμεύσουν σε πολλούς και διάφορους σκοπούς: την καλύτερη παράδοση των κυβερνητικών υπηρεσιών στους πολίτες, τη βελτίωση των σχέσεων και των αλληλεπιδράσεων με τις επιχειρήσεις και τη βιομηχανία, την ενδυνάμωση των πολιτών μέσω της πρόσβασης στην πληροφορία ή ακόμη και την πιο αποτελεσματική διαχείριση της κυβέρνησης. Το όφελος που προκύπτει μπορεί να είναι μικρότερη διαφθορά, αυξημένη διαφάνεια, μεγαλύτερη αύξηση των εσόδων και / ή μειώσεις του κόστους.

1.1.1 Εννοιολογική προσέγγιση, μοντέλα και τύποι, οφέλη και προκλήσεις.

Η Ηλεκτρονική Διακυβέρνηση αποτελεί μία προσπάθεια στο γενικότερο πλαίσιο εκμετάλλευσης των σύγχρονων τεχνολογιών προκειμένου να μπορεί να μπορεί ο απλός ο πολίτης να διεκπεραιώσει τις υποχρεώσεις του προς τους Δημόσιους Φορείς με χρήση των υπολογιστών και του διαδικτύου κερδίζοντας έτσι πολύτιμο χρόνο και αποφεύγοντας την γραφειοκρατία. Επίσης με τον τρόπο αυτό υπάρχει μεγαλύτερη

ασφάλεια στην πραγματοποίηση των συναλλαγών, είναι όλα πιο διαφανή και μπορεί να καταπολεμηθεί η διαφθορά αφού όλες οι ενέργειες μπορούν να ελεγχθούν.

Αναλυτικότερα, βλέπουμε ότι η κυβέρνηση καθορίζει και προωθεί την εφαρμογή των οκτώ τύπων της ηλεκτρονικής διακυβέρνησης οι οποίες μπορεί να αποφέρουν σημαντικά οφέλη για την κυβέρνηση, τους πολίτες, τις επιχειρήσεις, τους εργαζόμενους και άλλους μη κερδοσκοπικούς οργανισμούς καθώς και τις πολιτικές και κοινωνικές οργανώσεις. Οι Τύποι της ηλεκτρονικής διακυβέρνησης μπορούν να ταξινομηθούν σε 8 κατηγορίες και είναι οι εξής:

1) Κυβέρνηση-προς-Πολίτη (G2C): Παρέχει τη δυνατότητα να τεθούν on line οι δημόσιες υπηρεσίες, ιδίως μέσω της παροχής ηλεκτρονικών υπηρεσιών για την προσφορά πληροφοριών και επικοινωνιών.

2) Πολίτης-προς-Κυβέρνηση (C2G): Παρέχει τη δυνατότητα να τεθούν on line οι δημόσιες υπηρεσίες, ιδίως μέσω της παροχής ηλεκτρονικών υπηρεσιών, για την ανταλλαγή των πληροφοριών και επικοινωνιών.

3) Κυβέρνηση-προς-Επιχειρήσεις (G2B): Ηλεκτρονικά ενεργές συναλλαγές και διαδικασίες, όπως η ηλεκτρονική ανάθεση συμβάσεων και η ανάπτυξη μιας ηλεκτρονικής αγοράς για τις δημόσιες προμήθειες. Η μορφή αυτή διεξάγει τις αναθέσεις δημόσιων προμηθειών με ηλεκτρονικά μέσα, για την ανταλλαγή πληροφοριών και εμπορευμάτων .

4) Επιχειρήσεις προς Κυβέρνηση (B2G):) όλες οι μορφές ηλεκτρονικής επικοινωνίας μεταξύ επιχειρήσεων και κράτους (π.χ. για διεκπεραίωση ηλεκτρονικά των φορολογικών τους). Το κράτος ενημερώνει τις επιχειρήσεις ηλεκτρονικά για διαγωνισμούς, προκηρύξεις κλπ, ενώ αυτές υποβάλλουν ηλεκτρονικά τις αιτήσεις τους.

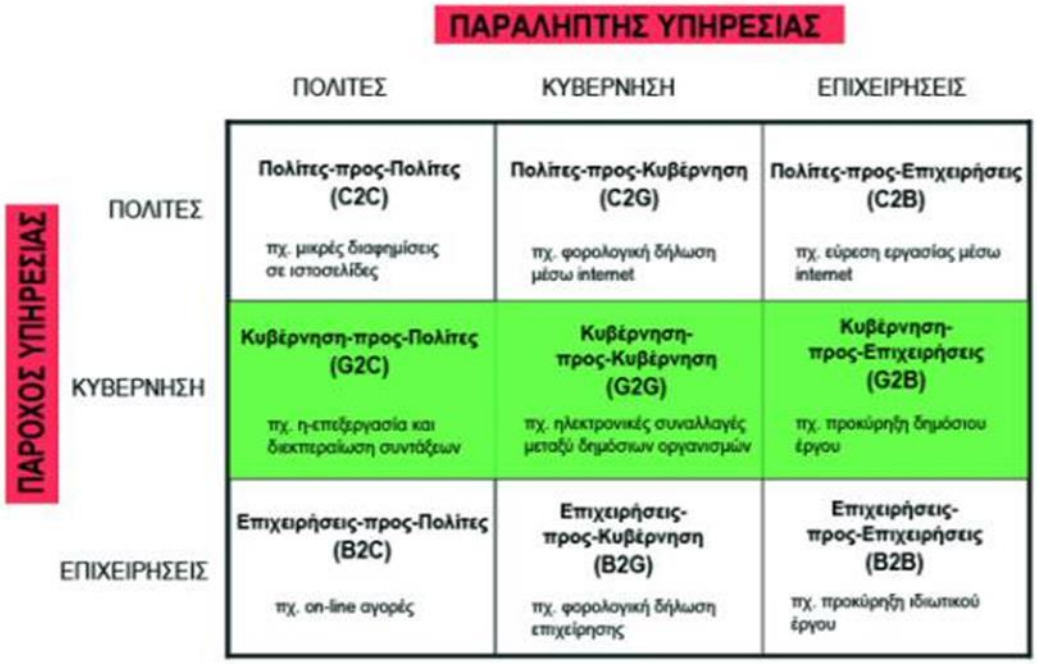
5) Κυβέρνηση προς εργαζόμενους (G2E): προάγει πρωτοβουλίες που θα διευκολύνουν τη διαχείριση των δημόσιων υπηρεσιών και την εσωτερική επικοινωνία με τους κυβερνητικούς υπαλλήλους, προκειμένου να κάνουν τις εφαρμογές της e-career και του συστήματος επεξεργασίας των αιτήσεων «χωρίς χαρτί» .

6) Η κυβέρνηση-προς-Κυβέρνηση (G2G): Παρέχει στις κυβερνητικές υπηρεσίες και οργανισμούς συνεργασία και επικοινωνία μέσω μιας μεγάλης βάσης δεδομένων της κυβέρνησης , έτσι ώστε να αποκτήσουν πλεονεκτήματα στην αποδοτικότητα και την αποτελεσματικότητα. Περιλαμβάνει επίσης εσωτερική ανταλλαγή πληροφοριών και αγαθών.

7) Κυβέρνηση-προς-μη κερδοσκοπικές οργανώσεις (G2N): η κυβέρνηση παρέχει πληροφορίες και επικοινωνία μεταξύ των μη κερδοσκοπικών οργανώσεων, των πολιτικών κόμματων και των κοινωνικών οργανώσεων.

8) Μη κερδοσκοπικές οργανώσεις -προς-Κυβέρνηση: (N2G): Ανταλλαγή πληροφοριών και επικοινωνίας μεταξύ της κυβέρνησης και των μη κερδοσκοπικών οργανώσεων, τω πολιτικών κόμματων και των κοινωνικών οργανώσεων.

Από τους παραπάνω τύπους της ηλεκτρονικής διακυβέρνησης, μπορούμε να καταλήξουμε στο γεγονός ότι οι εφαρμογές της ηλεκτρονικής διακυβέρνησης θα πρέπει να επικεντρωθούν σε πέντε σχέσεις μεταξύ καταναλωτών και Κυβέρνησης : Πολίτες-προς-Κυβέρνηση, Επιχειρήσεις-προς-Κυβέρνηση, Κυβέρνηση-προς-μη κερδοσκοπικές οργανώσεις, Κυβέρνηση –προς- Κυβέρνηση και την Κυβέρνηση-προς-Εργαζόμενους.



Επιπλέον, έχουν προταθεί κάποια διαφορετικά Μοντέλα Ηλεκτρονικής Διακυβέρνησης τα οποία αφορούν την οργάνωση και λειτουργία της:

i. *Μοντέλο Τριών Δακτυλίων*

Το μοντέλο αυτό προτάθηκε από τους Koh και Balthazard. Αποτελεί ένα απλό, κατανοητό και επεξηγηματικό πλαίσιο οργάνωσης των χαρακτηριστικών λειτουργιών που

παρέχονται από το διαδίκτυο . Σύμφωνα με το μοντέλο, οι εφαρμογές του διαδικτύου μπορούν να διαχωριστούν σε τρεις κύριες κατηγορίες χρήσης:

– Πληροφοριακή χρήση: Οι οργανισμοί χρησιμοποιούν το διαδίκτυο για την διάχυση της πληροφορίας με σκοπό την εκπαίδευση, την ψυχαγωγία, την επιρροή ή απλά την επαφή-επικοινωνία με τον καταναλωτή . Αποτελεί την πιο πρώιμη μορφή τεχνολογικής εφαρμογής και για πολλούς οργανισμούς είναι μέχρι και σήμερα η επικρατέστερη εφαρμογή μεταξύ των παρεχόμενων.

– Συναλλαγές: Χρήση του διαδικτύου για την υποστήριξη μιας καθοδηγούμενης συνέχειας διαδικασιών μεταξύ χρηστών και συστήματος, η οποία έχει εν τέλει ως αποτέλεσμα τη δημιουργία και μεταφορά προστιθέμενης αξίας . Με χρήση του διαδικτύου, ο πολίτης μπορεί να παρακολουθήσει, να ενημερωθεί αλλά και να δώσει εντολή για την πληρωμή των λογαριασμών του απέναντι στο δημόσιο. Η συναλλαγματική αυτή χρήση των εφαρμογών του διαδικτύου φέρει στο προσκήνιο το θέμα της ασφάλειας.

– Διαδικασίες: Μέσω του διαδικτύου παρέχονται νέοι μηχανισμοί που μπορούν να συνάπτουν έως και πολύπλοκες επιχειρηματικές διαδικασίες . Κύρια του χαρακτηριστικά αποτελούν η ευρέως διαδεδομένη χρήση του Διαδικτύου, η ικανότητα παρουσίασης και παράθεσης της πληροφορίας με πολυμεσικό τρόπο , η οικειότητα του κοινού με τις νέες τεχνολογίες και η διαθεσιμότητα πολλαπλών εύχρηστων εργαλείων.

ii. *Μοντέλο Εστίασης και Κεντρικότητας*

Οι δημόσιες υπηρεσίες σε Ευρώπη και Βόρεια Αμερική σταδιακά μεταλλάσσονται κάτω από τις συνεχείς πιέσεις των τεχνολογιών του Διαδικτύου . Δημιουργήθηκε έτσι, ένα δισδιάστατο πλαίσιο αναφοράς προκειμένου να γίνει φανερή η επίδραση του Διαδικτύου . Στον ένα άξονα προτείνεται η διάσταση της ηλεκτρονικής κυβέρνησης σε αντιπαράθεση με αυτήν της ηλεκτρονικής διακυβέρνησης . Στη δεύτερη διάσταση αντιπαρατίθεται η σχέση στην οποία επίκεντρο είναι ο πολίτης (πολιτο-κεντρική άποψη) με αυτήν του

οργανισμού (οργανοκεντρική άποψη) .Για κάθε ένα από τα τεταρτημόρια που δημιουργούνται, εξετάζονται και μελετώνται τα θέματα που προκύπτουν.

1ο Τεταρτημόριο: Η Ηλεκτρονική Κυβέρνηση αφορά κυρίως την αποδοτικότητα και αποτελεσματικότητα των διοικητικών θεμάτων της δημόσιας διοίκησης . Οι ιστοσελίδες που έχουν δημιουργηθεί και είναι πληροφοριακής φύσεως με θέματα όπως η σχέση με την πολιτική της κυβέρνησης, το κατά πόσο οι πολιτικές και το περιεχόμενο είναι στατικό ή δυναμικό κλπ. . Κάποιοι παράγοντες που καθορίζουν την επιτυχία της ΗΚ, αφορούν την κατασκευή ιστοσελίδων, την μηχανές αναζήτησης κλπ, που θα φέρουν τον πολίτη στην διοικητική περιοχή ενδιαφέροντος όσο το δυνατόν πιο γρήγορα. Έτσι προκύπτουν δυο ζητήματα: η βελτίωση της παροχής προστιθέμενης αξίας από την κυβέρνηση προς τους πολίτες, καθώς και η αύξηση της αποτελεσματικότητας ενός κυβερνητικού ιστότοπου.

2ο Τεταρτημόριο: Οι διαδικτυακές υπηρεσίες παρέχουν το προνόμιο ενός διαφορετικού είδους συμβουλευτικής, εξυπηρετώντας την άμεση ανταπόκριση σε τοπικό, εθνικό ή ακόμα και διεθνές επίπεδο . Ένα ουσιαστικό μέρος της πολιτοκεντρικής διακυβέρνησης είναι η ανάπτυξη online κοινοτήτων οι οποίες λειτουργούν είτε συμβουλευτικά είτε για παροχή πληροφοριών . Συνεπώς οι κυβερνήσεις θα πρέπει να συμπεριλάβουν όλες τις κοινωνικές ομάδες στις κοινότητες αυτές και να επαναπροσδιορίσουν τις σχέσεις τους μαζί τους.

3ο Τεταρτημόριο : Το τρίτο πλαίσιο, ερευνά την επίδραση που το Διαδίκτυο μπορεί να έχει στη μορφή ενός οργανισμού που ανήκει στο δημόσιο τομέα, όποια και αν είναι η έως τώρα εικόνα του . Η ΗΚ λοιπόν πρέπει να αντιμετωπιστεί σαν μια προσπάθεια προώθησης ενός κλίματος αλλαγής . Οι τεχνολογίες δικτύωσης και διασύνδεσης φορέων, ευνοούν μια μορφή προσέγγισης που στηρίζεται στην παροχή υπηρεσιών μέσω δικτύων συνεργασίας και σε παραδοσιακές γραφειοκρατικές προσεγγίσεις.

4ο Τεταρτημόριο : Εδώ εξετάζεται πως ένας κυβερνητικός οργανισμός θα ανταποκριθεί στις νέες απαιτήσεις για διακυβέρνηση, όπως αυτές διαμορφώνονται από μια συνεχώς αυξανόμενη διασυνδεδεμένη πολιτεία καθώς και οι αλλαγές στις παραδοσιακές ιεραρχίες για τα επόμενα χρόνια . Με νέες τεχνολογίες ασφαλής πρόσβασης, αναμένεται

η ασφάλεια, η αυθεντικότητα και η εμπιστευτικότητα να αποτελέσουν πλέον θέμα ρουτίνας, καθιστώντας έτσι αξιόπιστη τη χρήση τεχνολογιών ψηφοφορίας και έρευνας αγοράς.

iii. *Μοντέλο Ηλεκτρονικής Κυβερνητικής Ετοιμότητας*

Η επιτυχής υλοποίηση Διαδικτυακής ΗΚ απαιτεί προσεκτικό σχεδιασμό και καθοδήγηση των οργανωσιακών στόχων, διαδικασιών και τεχνολογιών. Αναπτύχθηκε έτσι ένα θεωρητικό μοντέλο της ΗΚ ετοιμότητας το οποίο αναγνωρίζει τα κύρια συστατικά στοιχεία της ΗΚ καθώς εξελίσσεται από ένα απλό site που παρέχει πληροφορίες, σε μια προηγμένη διαδικτυακή πύλη ολοκληρωμένων υπηρεσιών.

Εντοπίζοντας θέματα και πιθανά προβλήματα, ένας οργανισμός μπορεί να εκμεταλλευτεί καλύτερα τα πληροφοριακά συστήματα και να αυξήσει την αποδοτικότητα κι επιτυχία. Καθώς οι οργανισμοί αποκτούν οικειότητα με την τεχνολογία, επεκτείνουν τις εφαρμογές τους φτάνοντας στο τελικό στάδιο, όπου όλες οι Διαδικτυακές εφαρμογές είναι στενά διασυνδεδεμένες. Για την παρακολούθηση του μετασχηματισμού αυτού απαιτούνται προσεκτικά σχεδιασμένες στρατηγικές, σε συμφωνία με τους επιχειρηματικούς στόχους, τις προσπάθειες για ανάπτυξη και βελτίωση και μια αποτελεσματική τεχνολογική υποδομή.

Η λειτουργία του Δημόσιου Διοικητικού τομέα αλλά τόσο του επιχειρηματικού όσο και των πολιτών έχει επωφεληθεί σημαντικά από την εφαρμογή της Ηλεκτρονικής Διακυβέρνησης. Τα οφέλη που παρέχονται από την Η.Δ. είναι:

1) Βελτίωση της ποιότητας των παρεχόμενων υπηρεσιών.
2) Μείωση του κόστους των δημόσιων υπηρεσιών.
3) Η ελάττωση της άμεσης επαφής των πολιτών με τις δημόσιες υπηρεσίες.
4) Η αναδιοργάνωση και ο εξορθολογισμός των διεργασιών της δημόσιας διοίκησης.
5) Αύξηση της αποδοτικότητας και της αποτελεσματικότητας των δημόσιων υπηρεσιών.

6) Μείωση του χρόνου διεκπεραίωσης των διαδικασιών και επέκταση της διαθεσιμότητας των δημόσιων υπηρεσιών(24 ώρες χωρίς τοπικούς περιορισμούς)

7) Συμμετοχή του κοινωνικού συνόλου στην διαμόρφωση των δημόσιων πολιτικών.

8) Η προώθηση της δημοκρατίας η ελάττωση της διαφθοράς.

9) Η δυνατότητα ελέγχου και απόδοσης ευθυνών στη δημόσια διοίκηση.

10) Μείωση της επιβάρυνσης στο περιβάλλον (π.χ. λιγότερο χαρτί, μειωμένες μετακινήσεις).

1.2 Ασφάλεια στο Ηλεκτρονικό Επιχειρείν και στην Ηλεκτρονική διακυβέρνηση

Η ανάπτυξη των νέων Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) και η καθημερινή και απρόσκοπτη χρήση του Διαδικτύου, έδωσε μία νέα διάσταση στη φύση του Επιχειρείν, το Ηλεκτρονικό Επιχειρείν όπου η επιχειρηματική δραστηριότητα πραγματοποιείται με ηλεκτρονικά μέσα.

Το Ηλεκτρονικό Επιχειρείν , το οποίο αποτελεί ευρύτερο όρο του Ηλεκτρονικού Εμπορίου περιλαμβάνει όχι μόνο την αγορά και πώληση προϊόντων, υπηρεσιών, πληροφοριών αλλά και την εξυπηρέτηση πελατών, την επικοινωνία και συνεργασία με επιχειρηματικούς εταίρους καθώς και την διεξαγωγή ενδο-επιχειρησιακών ηλεκτρονικών συναλλαγών.

Η ηλεκτρονική διακυβέρνηση ως υποέννοια του Ηλεκτρονικού Επιχειρείν, αποτελεί το ‘εργαλείο’ πραγμάτωσης της νέας σχέσης εκσυγχρονισμού πολίτη και κράτους, της βελτίωσης των διαδικασιών, επικοινωνίας μεταξύ των δημοσίων υπηρεσιών, φορέων και οργανισμών. Αυτό επιτυγχάνεται μέσω της εστίασης σε ζητήματα διασυνδεσιμότητας και διαλειτουργικότητας των πληροφοριακών συστημάτων του δημόσιου τομέα με αποτέλεσμα την ταχύτερη, οικονομικότερη, διάφανη, ασφαλέστερη και ποιοτικά αναβαθμισμένη εξυπηρέτηση των πολιτών. Η ψηφιοποίηση του τεράστιου όγκου πληροφοριών που κατέχει η κεντρική, περιφερειακή και τοπική εξουσία παρέχουν τη δυνατότητα για πιο αποτελεσματική και ορθολογική διοίκηση.

Κατά τη διάρκεια εκτέλεσης οποιασδήποτε ηλεκτρονικής συναλλαγής μπορεί να προκύψει οποιαδήποτε απειλή η οποία να προσπαθεί να υποκλέψει και να εκμεταλλευτεί οποιαδήποτε ευαίσθητη πληροφορία που εμφανίζεται σε μια ηλεκτρονική συναλλαγή. Οι μορφές τέτοιων απειλών ποικίλουν, όμως παρακάτω αναφέρονται οι πιο συνηθισμένοι κίνδυνοι ηλεκτρονικών συναλλαγών

- Υποκλοπή δεδομένων
- Καταστροφή ή αλλοίωση δεδομένων
- Κακόβουλες εισβολές σε δίκτυα(hacking)
- Απάτη με πιστωτικές κάρτες
- Το phising(ψάρεμα)
- Αυτόνομα κακόβουλα προγράμματα(Ιοί, δούρειοι ίπποι)

Για το λόγο αυτό, έχουν αναπτυχθεί διάφοροι μηχανισμοί ασφαλείας που βοηθούν στην πραγματοποίηση έγκυρων και ασφαλών συναλλαγών στα πλαίσια του Ηλεκτρονικού Επιχειρείν και της Ηλεκτρονικής Διακυβέρνησης:

Κρυπτογραφία: Μόλις αρχίσουμε να στέλνουμε ιδιωτικά και εμπιστευτικά δεδομένα μέσω του Internet, πρέπει να εξασφαλίσουμε ότι τα δεδομένα θα είναι ασφαλή από τα αδιάκριτα μάτια. Τα σημερινά σχέδια κρυπτογράφησης είναι αρκετά σύνθετα. Χρησιμοποιούνται σύνθετοι αλγόριθμοι που λειτουργούν ως κλειδί αντικατάστασης. Μέσω χρήσης προγραμμάτων λογισμικού εκτελούνται περίπλοκοι μαθηματικοί αλγόριθμοι για να δημιουργηθούν δύο κλειδιά κρυπτογράφησης. Αυτά τα κλειδιά έχουν τη δυνατότητα να κωδικοποιούν (κρυπτογραφούν) και να αποκωδικοποιούν (αποκρυπτογραφούν) ηλεκτρονικά μηνύματα . Τα δύο κλειδιά σχετίζονται μεταξύ τους κατά τέτοιο τρόπο ώστε το ένα να έχει τη δυνατότητα να αποκρυπτογραφεί τα μηνύματα που κρυπτογραφούνται από το άλλο. Το ένα κλειδί διατηρείται ιδιωτικό, και το άλλο δημοσιοποιείται.

Ψηφιακή/ηλεκτρονική υπογραφή: Η ψηφιακή ή αλλιώς ηλεκτρονική υπογραφή έχει οριστεί ως το ψηφιακό πιστοποιητικό και είναι για τον ηλεκτρονικό κόσμο το αντίστοιχο του διαβατηρίου για τον φυσικό κόσμο. Εκδίδεται από έναν Πάροχο Υπηρεσιών Πιστοποίησης (αρχή ψηφιακής πιστοποίησης) που εγγυάται για τα στοιχεία του κατόχου

του, ακριβώς όπως η αρμόδια κρατική αρχή εγγυάται για την έκδοση του διαβατηρίου. Η κατοχή του ψηφιακού πιστοποιητικού διασφαλίζεται από την αποκλειστική κατοχή συγκεκριμένων ψηφιακών δεδομένων (ιδιωτικό κλειδί) από το φυσικό πρόσωπο. Ο Πάροχος δημοσιεύει ψηφιακά δεδομένα σχετικά με την επαλήθευση της κατοχής του πιστοποιητικού (δημόσιο κλειδί) και εγγυάται για τα στοιχεία του φυσικού προσώπου (Επίσημος ιστότοπος eett). Οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού.

Ψηφιακά πιστοποιητικά :Τα ψηφιακά πιστοποιητικά είναι ηλεκτρονικά αρχεία που χρησιμοποιούνται για τον εντοπισμό των ανθρώπων και των πόρων για δίκτυα όπως το Διαδίκτυο. Τα ψηφιακά πιστοποιητικά επιτρέπουν επίσης την ασφαλή και εμπιστευτική επικοινωνία μεταξύ των δύο μερών με τη χρήση κρυπτογράφησης. Ένα πρότυπο πιστοποιητικό συνήθως περιλαμβάνει μια ποικιλία από πληροφορίες σχετικά με τον ιδιοκτήτη του όπως:

- Το όνομα του κατόχου και άλλες πληροφορίες αναγνώρισης που, όπως η διεύθυνση URL του διακομιστή Web .
- Το Δημόσιο κλειδί του κατόχου που μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση ευαίσθητων πληροφοριών για τον κάτοχο του πιστοποιητικού.
- Το όνομα της Αρχής Πιστοποίησης που εξέδωσε το πιστοποιητικό .
- Η περίοδος ισχύος (ή διάρκεια ζωής) του πιστοποιητικού .

Το ψηφιακό πιστοποιητικό αποτελεί την ηλεκτρονική βεβαίωση η οποία συνδέει δεδομένα επαλήθευσης με ένα άτομο και επιβεβαιώνει την ταυτότητά του. Το ψηφιακό πιστοποιητικό που κατέχει και επιδεικνύει ένας χρήστης (μια οντότητα) πιστοποιεί την ταυτότητα του σε τρίτους και παρέχει τα μέσα σε αυτούς να επιβεβαιώνουν αυτή την ταυτότητα. Το δημόσιο κλειδί κάθε χρήστη είναι δημόσια διαθέσιμο, και προκειμένου αυτό να συνδέεται με κάποιο πρόσωπο, περιέχεται μέσα σε ένα πιστοποιητικό ψηφιακής ταυτότητας. Το πιστοποιητικό ψηφιακής ταυτότητας που αναφέρθηκε δεν είναι τίποτε άλλο από το ψηφιακό πιστοποιητικό το οποίο εκδίδεται και διαχειρίζεται στα πλαίσια μιας υποδομής δημόσιου κλειδιού.

- Πρωτόκολλο SSL : Το SSL προσφέρει συνοπτικά τις ακόλουθες υπηρεσίες:
  - Πιστοποίηση του server από τον client.

■ Πιστοποίηση του client από τον server.

■ Εγκαθίδρυση ασφαλούς κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ των δύο μερών.

Το πρωτόκολλο SSL έχει σχεδιαστεί για να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί σαν client και το άλλο σαν server. Η εξασφάλιση του απορρήτου γίνεται με την κρυπτογράφηση όλων των μηνυμάτων στο επίπεδο SSL Record Protocol. Παρέχει, επιπλέον, υποχρεωτική πιστοποίηση της ταυτότητας του server και προαιρετικά της ταυτότητας του client, μέσω έγκυρων πιστοποιητικών από έμπιστες Αρχές Έκδοσης Πιστοποιητικών (Certificates Authorities). Υποστηρίζει πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών για αντιμετώπιση όλων των διαφορετικών αναγκών. Τέλος, εξασφαλίζει την ακεραιότητα των δεδομένων, εφαρμόζοντας την τεχνική των Message Authentication Codes (MACs), ώστε κανείς να μην μπορεί να αλλοιώσει την πληροφορία χωρίς να γίνει αντιληπτός. Το SSL μπορεί να τοποθετηθεί στην κορυφή οποιουδήποτε πρωτοκόλλου μεταφοράς, δεν εξαρτάται από την ύπαρξη του TCP/IP και τρέχει κάτω από πρωτόκολλα εφαρμογών όπως το HTTP, FTP και TELNET.

1.3 Ασφάλεια προσωπικών δεδομένων

Η ραγδαία επέκταση των νέων τεχνολογιών, η ανάπτυξη της οικονομικής δραστηριότητας, η διασυνοριακή διαβίβαση προσωπικών δεδομένων και η τάση ενίσχυσης της δημόσιας ασφαλείας καθιστούν επιτακτική την ασφαλή επεξεργασία και προστασία των προσωπικών δεδομένων. Το θέμα της ασφαλούς επεξεργασίας των προσωπικών δεδομένων ρυθμίστηκε αρχικά στα άρθρα 10 του ν. 2472/1997 και 12 του ν.3471/2006, οι οποίοι νόμοι ενσωμάτωσαν στο ελληνικό δίκαιο την Ευρωπαϊκή Οδηγία 95/46/ΕΚ η οποία έθεσε κανόνες για την προστασία των προσωπικών δεδομένων σε όλες τις χώρες της Ευρωπαϊκής Ένωσης.

Σύμφωνα με το άρθρο 10 του ν.2472/1997, η επεξεργασία των προσωπικών δεδομένων διεξάγεται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνον κατ' εντολή του.

Όσοι επεξεργάζονται προσωπικά δεδομένα (υπεύθυνοι επεξεργασίας), ανεξαρτήτως αν απαλλάσσονται από την υποχρέωση γνωστοποίησης και λήψης άδειας (άρθρο 7Α του ν.2472/1997), οφείλουν να λαμβάνουν μέτρα που να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Η εκτίμηση του επιπέδου του κινδύνου των προσωπικών δεδομένων επιτυγχάνεται με την ανάλυση επικινδυνότητας (risk analysis). Η ανάλυση επικινδυνότητας έχει ως στόχο την εκτίμηση των κινδύνων και των απειλών στις οποίες είναι εκτεθειμένο το πληροφοριακό σύστημα στο οποίο λαμβάνει χώρα η επεξεργασία των προσωπικών δεδομένων. Βασιζόμενος στα αποτελέσματα της ανάλυσης επικινδυνότητας, ο υπεύθυνος επεξεργασίας μπορεί να εκτιμήσει τα μέτρα ασφαλείας που πρέπει να λάβει ώστε να μειώσει τον κίνδυνο σε ένα αποδεκτό επίπεδο.

Επιπλέον, οι υπεύθυνοι επεξεργασίας, οφείλουν να:
επιλέγουν πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου, λαμβάνουν τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια και την προστασία των προσωπικών δεδομένων από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.
Αν η επεξεργασία διεξάγεται για λογαριασμό του υπευθύνου από πρόσωπο μη εξαρτώμενο από αυτόν, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως. Η ανάθεση προβλέπει ότι ο ενεργών την επεξεργασία την διεξάγει μόνο κατ' εντολή του υπευθύνου και ότι οι λοιπές υποχρεώσεις του άρθρου 10 του ν.2472/1997 βαρύνουν αναλόγως και αυτόν.

Νέος Ευρωπαϊκός Γενικός Κανονισμός για τα Προσωπικά Δεδομένα

Στις 14 Απριλίου 2016, το Ευρωπαϊκό Κοινοβούλιο ενέκρινε το Γενικό Κανονισμό για τα Προσωπικά δεδομένα και άρχισε να εφαρμόζεται την άνοιξη του 2018.
Ο κανονισμός περιγράφει τα δικαιώματα του υποκειμένου των δεδομένων, δηλαδή του ατόμου του οποίου τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία. Αυτά τα

ενισχυμένα δικαιώματα παρέχουν στα άτομα μεγαλύτερο έλεγχο επί των προσωπικών τους δεδομένων, μεταξύ άλλων μέσω:

- ✓ την ανάγκη ύπαρξης σαφούς συγκατάθεσης του ενδιαφερομένου για την επεξεργασία των προσωπικών του δεδομένων
- ✓ της ευκολότερης πρόσβασης του ενδιαφερομένου στα προσωπικά του δεδομένα
- ✓ των δικαιωμάτων διόρθωσης, διαγραφής και «λήθης»
- ✓ του δικαιώματος εναντίωσης, μεταξύ άλλων στη χρησιμοποίηση των δεδομένων προσωπικού χαρακτήρα για την «κατάρτιση προφίλ»
- ✓ του δικαιώματος φορητότητας των δεδομένων από πάροχο σε πάροχο.

Θεσπίζει επίσης την υποχρέωση των υπεύθυνων επεξεργασίας των δεδομένων να παρέχουν διαφανείς και εύκολα προσβάσιμες πληροφορίες στα υποκείμενα των δεδομένων όσον αφορά την επεξεργασία των δεδομένων τους.
Ο Νέος Κανονισμός ορίζει αναλυτικά τις γενικές υποχρεώσεις που έχουν οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία των δεδομένων προσωπικού χαρακτήρα για λογαριασμό αυτών. Και οι δύο έχουν την υποχρέωση τήρησης κατάλληλων μέτρων ασφαλείας ανάλογα με τον κίνδυνο τον οποίον ενέχουν οι πράξεις επεξεργασίας δεδομένων τις οποίες εκτελούν.

Οι υπεύθυνοι επεξεργασίας σε ορισμένες περιπτώσεις, πρέπει να κοινοποιούν τα περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα εντός 72 ωρών από την ανακάλυψη του περιστατικού παραβίασης και απώλειας προσωπικών δεδομένων στις αρμόδιες αρχές και στα υποκείμενα των δεδομένων αν η φύση των δεδομένων που χάθηκαν το απαιτεί.

Επίσης για τις εταιρείες και τις δημόσιες αρχές που εκτελούν πράξεις επεξεργασίας δεδομένων που ενέχουν κινδύνους θα πρέπει να έχουν ορίσει υπεύθυνο προστασίας δεδομένων. Για τους υπεύθυνους επεξεργασίας ή τους εκτελούντες την επεξεργασία δεδομένων οι οποίοι παραβιάζουν τους κανόνες για την προστασία των δεδομένων προβλέπονται πολύ αυστηρές κυρώσεις. Στους υπευθύνους επεξεργασίας δεδομένων μπορεί να επιβληθεί πρόστιμο που μπορεί να ανέλθει σε 20 εκατ. € ή στο 4% του συνολικού ετήσιου κύκλου εργασιών τους. Για την επιβολή διοικητικού προστίμου,

καθώς και σχετικά με το ύψος του διοικητικού προστίμου για κάθε μεμονωμένη περίπτωση, λαμβάνονται υπόψη ενδεικτικά τα ακόλουθα:

- ✓ η φύση, η βαρύτητα και η διάρκεια της παράβασης, λαμβάνοντας υπόψη τη φύση, την έκταση ή το σκοπό της σχετικής επεξεργασίας, καθώς και τον αριθμό των υποκειμένων των δεδομένων που έθιξε η παράβαση και το βαθμό ζημίας που υπέστησαν,
- ✓ ο δόλος ή η αμέλεια που προκάλεσε την παράβαση,
- ✓ οποιεσδήποτε ενέργειες στις οποίες προέβη ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία για να μετριάσει τη ζημία που υπέστησαν τα υποκείμενα των δεδομένων,
- ✓ ο βαθμός ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, λαμβάνοντας υπόψη τα τεχνικά και οργανωτικά μέτρα που εφαρμόζουν,
- ✓ τυχόν σχετικές προηγούμενες παραβάσεις του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία,
- ✓ ο βαθμός συνεργασίας με την αρχή ελέγχου για την επανόρθωση της παράβασης και τον περιορισμό των πιθανών δυσμενών επιπτώσεών της,
- ✓ οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζει η παράβαση,
- ✓ ο τρόπος με τον οποίο η εποπτική αρχή πληροφορήθηκε την παράβαση, ειδικότερα εάν και κατά πόσο ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία κοινοποίησε την παράβαση,
- ✓ σε περίπτωση που διατάχθηκε προηγουμένως η λήψη των μέτρων που αναφέρονται κατά του εμπλεκόμενου υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σχετικά με το ίδιο αντικείμενο, η συμμόρφωση με τα εν λόγω μέτρα,
- ✓ η τήρηση εγκεκριμένων κωδίκων δεοντολογίας ή εγκεκριμένων μηχανισμών πιστοποίησης σύμφωνα και
- ✓ κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο που προκύπτει από τις περιστάσεις της συγκεκριμένης περίπτωσης, όπως τα οικονομικά οφέλη που αποκομίστηκαν ή ζημιών που αποφεύχθηκαν, άμεσα ή έμμεσα, από την παράβαση.

Ο κανονισμός αναγνωρίζει το δικαίωμα των υποκειμένων των δεδομένων να υποβάλλουν καταγγελία σε εποπτική αρχή καθώς και το δικαίωμά τους για δικαστική προσφυγή και αποζημίωση έτσι οι εταιρίες είναι εκτεθειμένες σε αγωγές από τρίτους των οποίων χάθηκαν τα προσωπικά τους δεδομένα.

1.4 Ασφάλεια προσωπικών δεδομένων στην Ηλεκτρονική διακυβέρνηση

Στις μέρες μας όπου ο πολίτης χρησιμοποιεί πλήθος υπηρεσιών και παράγει έναν ολοένα και αυξανόμενο όγκο ηλεκτρονικών δεδομένων, χωρίς τις περισσότερες φορές να γνωρίζει την ύπαρξή τους, την επεξεργασία ή τη διακίνησή τους, το νέο υποχρεωτικό στην εφαρμογή του κανονιστικό πλαίσιο για την προστασία δεδομένων επηρεάζει εντός της ΕΕ όχι μόνο τα Κράτη και τους δημόσιους οργανισμούς, αλλά και τις περισσότερες επιχειρήσεις, μικρές ή μεγάλες. Ο ΓΚΡΔ συμβάλει στην ενιαία ρύθμιση των όρων της επιχειρηματικής και οικονομικής δραστηριότητας στο πλαίσιο της ενιαίας ψηφιακής αγοράς, αίροντας εμπόδια για την απρόσκοπτη ροή της πληροφορίας.

Πλέον, υπάρχει ρητή αναφορά της υποχρέωσης για λήψη μέτρων ασφάλειας όπως:

- Η ψευδωνυμοποίηση και κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα
- Η διασφάλιση, σε συνεχή βάση, του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας
- Σε περίπτωση φυσικού ή τεχνικού συμβάντος, η δυνατότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εφικτέ χρόνο
- Η τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

Πρέπει επιπλέον να οριστεί Υπεύθυνος Προστασίας Δεδομένων (DPO)για τις υπηρεσίες Ηλεκτρονικής Διακυβέρνησης. Ο Υπεύθυνος Προστασίας Δεδομένων μπορεί να βοηθήσει στην υλοποίηση του ΓΚΠΔ. Ο ρόλος του είναι συμβουλευτικός και όχι αποφασιστικός. Οι αποφάσεις λαμβάνονται πάντα από τη Διοίκηση. Μπορεί όμως να συνεισφέρει στην ταχύτερη συμμόρφωση του φορέα με τις προτάσεις του. Αποτελεί υποχρέωση για κάθε Δημόσιο φορέα να διαθέτει DPO ανεξάρτητα του μεγέθους του.

Επιπλέον, απαραίτητη είναι και η αναθεώρηση των πολιτικών προστασίας δεδομένων στους τομείς της ΗΔ. Ο Φορέας εξετάζει τι είδους ενημέρωση παρέχει σήμερα στους πολίτες. Στον ΓΚΠΔ περιλαμβάνεται αλαλαγή υποχρέωσης και απαιτούνται περισσότερα στοιχεία να παρέχονται στους πολίτες προς ενημέρωση.

Ο φορέας οφείλει να δημοσιοποιεί τα στοιχεία του DPO του στην ιστοσελίδα του και στην Αρχή Προστασίας Δεδομένων. Όταν ο Φορέας συλλέγει προσωπικά δεδομένα από τρίτες πηγές πρέπει να αναζητήσει τον κατάλληλο τρόπο για να παρέχεται ενημέρωση προς τους πολίτες.
Ο κάθε φορέας Ηλεκτρονικής Διακυβέρνησης πρέπει να είναι σε ετοιμότητα σε περίπτωση παραβίασης της προστασίας προσωπικών δεδομένων. Έτσι οφείλει:

- να ανιχνεύει και να αξιολογεί αν ένα περιστατικό είναι παραβίαση προσωπικών διδομένων
- να το γνωστοποιεί στην Αρχή Προστασίας Διδομένων Προσωπικού Χαρακτήρα σε χρονικό διάστημα 72 ωρών
- να ενημερώνει τους πολίτες όσο πιο γρήγορα γίνεται για περιστατικά παραβίασης που μπορεί να τους επηρεάσουν

Συνοψίζοντας, η αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα στην Ε.Ε. απαιτεί τον λεπτότερη καθορισμό των δικαιωμάτων των υποκειμένων, όπως και των υποχρεώσεων όσων εμπλέκονται στην επεξεργασία δεδομένων. Ο ΓΚΠΔ προβλέπει ένα σύνθετο πλέγμα δικαιωμάτων και υποχρεώσεων. Η Δημόσια Διοίκηση οφείλει να προετοιμαστεί συστηματικά και μεθοδικά, προκειμένου να ανταποκριθεί στις νέες πολλαπλές προκλήσεις, καθώς το οργανωτικό έλλειμμα συνιστά σημαντικό κίνδυνο για την παραβίαση των προσωπικών δεδομένων.

1.5 Θεωρητικό Πλαίσιο

Συνοψίζοντας το παρόν κεφάλαιο, βλέπουμε ότι δόθηκε ιδιαίτερη προσοχή στη βιβλιογραφική ανάλυση των εννοιών οι οποίες αποτελούν τον βασικό πυλώνα της παρούσης διατριβής. Πιο συγκεκριμένα, παρουσιάστηκε αναλυτικά η έννοια και η δομή της Ηλεκτρονικής Διακυβέρνησης, στο πλαίσιο παροχής υπηρεσιών προς τους πολίτες.

Επιπρόσθετα, αναλύθηκε σε βάθος η έννοια της Ασφάλειας Πληροφοριών στα πλαίσια του Ηλεκτρονικού Επιχειρείν και ειδικά της Ηλεκτρονικής Διακυβέρνησης. Έγινε διεξοδική ανάλυση των κινδύνων που συντρέχουν κατά τη διάρκεια ηλεκτρονικών συναλλαγών, καθώς και των μηχανισμών ασφάλειας που έχουν αναπτυχθεί ώστε να συμβάλουν στην αντιμετώπισή τους.

Τέλος, δόθηκε ιδιαίτερη έμφαση στο νομοθετικό πλαίσιο το οποίο έχει θεσπιστεί τόσο σε Ευρωπαϊκό όσο και σε εθνικό επίπεδο κι έχει ως στόχο την προάσπιση των δικαιωμάτων των πολιτών όσον αφορά τα προσωπικά τους δεδομένα , καθώς και την παροχή ηλεκτρονικών υπηρεσιών και συναλλαγών που στηρίζονται στη διαφάνεια, την εμπιστευτικότητα και την ακεραιότητα.

Κεφάλαιο 2

Μεθοδολογία Έρευνας

Σε αυτό το κεφάλαιο θα αναλυθεί η μεθοδολογία που χρησιμοποιήσαμε ώστε να αξιολογηθεί η ορθή εφαρμογή του GDPR στον Όμιλο Εταιρειών ΟΤΕ. Θα αναλύσουμε το δείγμα που χρησιμοποιήθηκε, θα μιλήσουμε για τα εργαλεία έρευνας που χρησιμοποιήσαμε ώστε να διεξαχθεί η έρευνα και τέλος θα αναλύσουμε και τον ρόλο του ερευνητή και το πόσο σημαντικός είναι ώστε να διεξαχθούν ορθά συμπεράσματα.

2.1 Προτεινόμενη Μεθοδολογία (Δευτερογενής & Πρωτογενής)

Στην Δευτερογενή έρευνα γίνεται αξιολόγηση των συγκεντρωμένων στοιχείων που έχουν ήδη αντληθεί από υπάρχοντα δημοσιευμένα στοιχεία στα πλαίσια προηγούμενης πρωτογενούς έρευνας όπως βιβλία, ειδικές έρευνες, το διαδίκτυο και άλλες πηγές όπως διάφορες κρατικές υπηρεσίες, εξειδικευμένους οργανισμούς κ.α. Το πλεονέκτημα της Δευτερογενούς έρευνας είναι ότι έχει πολύ χαμηλό έως μηδενικό κόστος καθώς με την βοήθεια του διαδικτύου μπορεί να συγκεντρωθεί πληθώρα πληροφοριών και με την κατάλληλη επεξεργασία να οδηγήσει σε χρήσιμα συμπεράσματα τα οποία θα οδηγήσουν στην διεξαγωγή χρήσιμων αποφάσεων, είναι εύκολη και μπορεί να διεξαχθεί από την ίδια την εταιρεία. Το μειονέκτημα της είναι δεν μπορεί να συγκεντρώσει τόσο λεπτομερή και εξειδικευμένα στοιχεία όσο θα συγκέντρωνε η Πρωτογενής έρευνα.

Στην Πρωτογενή έρευνα συλλέγονται δεδομένα και πληροφορίες που υπάρχουν ήδη. Ο ερευνητής συλλέγει τις πληροφορίες και τα δεδομένα μέσω συνεντεύξεων και ερωτηματολογίων. Η Πρωτογενής έρευνα χωρίσετε σε ποιοτική και σε ποσοτική.

Η Ποσοτική έρευνα χρησιμοποιείτε από τον ερευνητή όταν οι πληροφορίες που θέλει να συλλέξει είναι ακριβείς και συγκεκριμένες. Τα ποσοτικά αυτά δεδομένα χρησιμοποιούνται για να γίνουν στατιστικές αναλύσεις οι οποίες θα εξάγουν αξιόπιστα αποτελέσματα. Για να συμβεί όμως αυτό θα πρέπει το δείγμα που θα επιλεχθεί να είναι αντιπροσωπευτικό.

Μέσω της Ποιοτικής έρευνας, την οποία και επιλέξαμε για την έρευνά μας, συλλέγουμε δεδομένα τα οποία στοχεύουν στην κατανόηση σε βάθος των κοινωνικών φαινομένων. Η Ποιοτική προσέγγιση είναι κατά βάση μία διερευνητική μέθοδος. Τα δεδομένα προέρχονται από αναλύσεις στοιχείων, συνεντεύξεις, συμμετοχικές παρατηρήσεις, περιπτωσιολογικές μελέτες. Στόχος της ποιοτικής έρευνας είναι κατανόηση διερευνώντας την εμπειρία των ατόμων και τα υποκειμενικά νοήματα που τη συγκροτούν.

Η Ποιοτική έρευνα στηρίζεται σε δύο βασικά χαρακτηριστικά:

1) Ο κύριος σκοπός της είναι να διερευνήσει κάποιες πλευρές του κοινωνικού συστήματος που μελετά.

2) Ο ερευνητής αποτελεί το μέσο με το οποίο διεξάγεται η έρευνα.

Και τα δύο αυτά χαρακτηριστικά είναι σημαντικά για την διαδικασία της έρευνας και θεωρούν τον ερευνητή όχι μονο σαν έναν απλό δέκτη της έρευνας αλλά ο ερευνητής είναι αυτός που δομεί την έρευνα.

Οι τρόποι διεξαγωγής της συγκεκριμένης έρευνας σύμφωνα με τον Chisnal είναι οι ακόλουθοι :

1. Χρήση ερωτηματολογίου
2. Συνεντεύξεις σε βάθος
3. Με τη μέθοδο της παρατήρησης
4. Με το πειραματισμό

Για την δική μας περίπτωση χρησιμοποιήσαμε την μέθοδο της Ποιοτικής έρευνας η οποία έγινε με την χρήση ερωτηματολογίου.

2.2 Δείγμα

Το δείγμα που χρησιμοποιήθηκε για την διεξαγωγή του ερωτηματολογίου είναι οι εργαζόμενοι της Υποδιεύθυνσης Ασφάλειας Προσωπικών Δεδομένων του Ομίλου ΟΤΕ η οποία απαρτίζεται από 15 άτομα, 1 διευθύντρια και 14 υφιστάμενους.

Ο ΟΤΕ δίνει πολύ μεγάλη έμφαση στη ασφάλεια των προσωπικών δεδομένων. Οι εργαζόμενοι της υποδιεύθυνσης είναι άτομα καταρτισμένα στην νομική διαχείριση της ασφάλειας των προσωπικών δεδομένων με πολυετή πείρα και γνώση του αντικειμένου. Ο ρόλος τους είναι να είναι συνεχώς ενημερωμένοι όσο αφορά τυχών νέες προσθήκες στη νομοθεσία, να εκπαιδεύουν το σύνολο του προσωπικού του Ομίλου με τις διατάξεις του νόμου αλλά και να εξασφαλίζουν ότι σε όλες τις διαδικασίες που υπάρχουν στον Όμιλο τηρείται η νομοθεσία κατά γράμμα.

2.3 Εργαλεία Έρευνας

Στην δευτερογενή έρευνα ανατρέξαμε και ερευνήσαμε την ισχύουσα νομοθεσία, έγινε διαδικτυακή έρευνα των εκδοθέντων ανακοινώσεων του Ομίλου καθώς επίσης έγινε έρευνα στον εσωτερικό ιστότοπο του Ομίλου. Σε συνεργασία με τους συναδέλφους της αρμόδιας Υποδιεύθυνσης για την καταγραφή κα ανάλυση των διαδικασιών που εφαρμόζονται και της ισχύουσας νομοθεσίας.

Για την πρωτογενή έρευνα σχεδιάσαμε ένα ερωτηματολόγιο υπό την μορφή συνέντευξης που αποτελείτε από 14 ερωτήσεις ανοικτού τύπου που απευθύνονται στους εργαζομένους της Υποδιεύθυνσης Ασφάλειας Προσωπικών δεδομένων. Οι 3 πρώτες ερωτήσεις έχουν να κάνουν με την γνωριμία μας με τον ερωτώμενο.

- Ποιος είναι ο ρόλος σας στην εταιρεία με τι ασχολείστε (συνοπτικά)
- Πόσα χρόνια εργάζεστε στο ΟΤΕ
- Πόσα χρόνια έχετε στην συγκεκριμένη θέση

Οι υπόλοιπες 11 αφορούν την αποτύπωση των διαδικασιών που τηρούνται στον Όμιλο καθώς επίσης μας αναφέρουν και για την επιτυχία εφαρμογής των διαδικασιών.

• Παρακαλούμε προσδιορίστε τις μεθόδους που χρησιμοποιείτε για τη συλλογή των δεδομένων προσωπικού χαρακτήρα (επιγραμματικά).

• Ποια είναι τα πλεονεκτήματα για την εταιρεία από την εφαρμογή του GDPR.

• Ποιες είναι οι κατηγορίες των προσωπικών δεδομένων που επεξεργάζονται από τον ΟΤΕ;

• Υπάρχει έγγραφη πολιτική ασφαλείας της επιχείρησης σας για την προστασία των δεδομένων προσωπικού χαρακτήρα; Τι αναφέρει;

• Η επιχείρησή σας τηρεί συγκεκριμένη διαδικασία όσον αφορά την ασφαλή διαγραφή ή την ηθελημένη καταστροφή προσωπικών δεδομένων; Αν ναι ποια είναι;

• Σε συνέχεια της παραπάνω ερώτησης οι εργαζόμενοι ερωτήθηκαν για τα Τεχνικά και Οργανωτικά μέτρα που λαμβάνει η εταιρεία

• Σας έχει γίνει εκπαίδευση για την προστασία προσωπικών δεδομένων; Αν ναι κάθε πότε γίνεται ;

• Υπάρχει υπεύθυνος Επεξεργασίας (Controller) και Υπεύθυνος Προστασίας Δεδομένων(DPO) και ποιος είναι ο ρόλος τους;

• Με ποιους συνεργάτες σας έχετε υπογράψει συμβάσεις εμπιστευτικότητας και εχεμύθειας π.χ. Συμφωνητικό Επεξεργασίας Δεδομένων και σε τι αναφέρεται αυτό;

• Τι είναι το Συμφωνητικό Επεξεργασίας Δεδομένων(Data Processing Agreement) που υπογράφετε με τους εξωτερικούς συνεργάτες και τους προμηθευτές ;

• Παρακαλώ περιγράψτε συνοπτικά τα βήματα ασφαλείας που ακολουθούνται από τους εργαζόμενους σε περίπτωση που αποκτούν πρόσβαση σε προσωπικά δεδομένα.

Η αποστολή των ερωτηματολογίων έγινε το 1ο δεκαπενθήμερο του Φεβρουαρίου του 2019 και η διαδικασία συμπλήρωσής του έγινε ως εξής:

- Κατόπιν τηλεφωνικής επικοινωνίας και έγκρισης από την Διευθύντρια της Υποδιεύθυνσης αποστάλθηκαν σε όλους τους συναδέλφους τα ερωτηματολόγια στα υπηρεσιακά τους email.

- Έπειτα από τηλεφωνική επικοινωνία και την εξαιρετική συνεργασία που είχαμε με όλους τους συναδέλφους συγκεντρώσαμε 15 ερωτηματολόγια εκ των οποίων το 1 μέσω τηλεφωνικής συνέντευξης και τα υπόλοιπα συμπληρώθηκαν και αποστάλθηκαν ηλεκτρονικά.

Η συνεργασία όλων ήταν υποδειγματική και όλοι οι συνάδελφοι του τμήματος συμμετείχαν στην έρευνα και απάντησαν το ερωτηματολόγιο.

2.4 Μεθοδολογία Έρευνας

Στην ποιοτική έρευνα ο ρόλος του ερευνητή είναι ιδιαίτερα σημαντικός. Πρέπει να είναι άμεσος να έχει προσωπική εμπλοκή στην έρευνα και να είναι υποκειμενικός. Οι συμμετέχοντες είναι ερευνητικοί συνεργάτες και ο ερευνητής αναζητεί την γνώση και την συνεργασίας τους. Μέσω της δευτερογενής έρευνα προσπαθεί να εντοπίσει τυχόν ελλείψεις στην διαδικασία της ασφάλειας των προσωπικών δεδομένων ώστε να τα αναφέρει και να προτείνει διορθώσεις.

Κύριος στόχος της έρευνα είναι να γίνει συλλογή καταγραφεί επεξεργασία και αξιολόγηση των αποτελεσμάτων και να εξαχθούν συμπεράσματα και προτάσεις που θα βοηθήσουν την διοίκηση να βελτιώσει τις υπάρχουσες διαδικασίες.

Όπως αναφέραμε και στις προηγούμενες ενότητες η συλλογή και επεξεργασία των δεδομένων που συλλέξαμε έγινε μέσω διανομής ερωτηματολογίων στους εργαζόμενους της Υποδιεύθυνσης Ασφάλειας και Προσωπικών Δεδομένων του Ομίλου ΟΤΕ και με την παροχή τηλεφωνικής συνέντευξης στην Προϊσταμένη της Υποδιεύθυνσης.

Τα ερωτηματολόγια στάλθηκαν όλα στα προσωπικά/υπηρεσιακά τους email στις 4 Φεβρουαρίου του 2019. Δυστυχώς εκείνη την περίοδο ο Όμιλος ΟΤΕ διοργάνωνε ένα μεγάλο event και η συγκεκριμένη Υποδιεύθυνση είχε μεγάλο φόρτο εργασίας καθώς βραβεύτηκε από τον Πρόεδρο του Ομίλου. Παρόλα αυτά η συνεργασία και η προθυμία των συναδέλφων να συμμετάσχουν στην συμπλήρωση του ερωτηματολογίου ήταν μεγάλη και η βοήθειά τους πολύτιμη. Είμασταν σε διαρκή επικοινωνία και έτσι 28 Μαρτίου του 2019 παραλάβαμε συμπληρωμένο και το τελευταίο ερωτηματολόγιο.

Η διεξαγωγή της τηλεφωνικής συνέντευξης είχε την μεγαλύτερη καθυστέρηση καθώς το φόρτο εργασίας της Προϊσταμένης του τμήματος, όπως είναι λογικό, ήταν μεγάλο και σε

συνδυασμό με το μεγάλο φόρτο εργασίας που είχα και εγώ στην εργασία μου εκείνη την περίοδο δυσκόλεψε λίγο την κατάσταση. Τελικά καταφέραμε να επικοινωνήσουμε 10 Απριλίου του 2019 και είχαμε μία εποικοδομητική συζήτηση με πολύ ωραία συμπεράσματα.

Έτσι το αποτέλεσμα ήταν να μας απαντήσουν και οι 15 συνάδελφοι που απαρτίζουν την Υποδιεύθυνση Προστασίας Προσωπικών Δεδομένων. Αν και το δείγμα των ερωτηθέντων δεν είναι ιδιαίτερα μεγάλο οι συνάδελφοι είναι πλήρως ενημερωμένοι και γνώστες του αντικειμένου μας έδωσαν μία ξεκάθαρη εικόνα για την εφαρμογή του GDPR στον Όμιλο εταιρειών ΟΤΕ και μας βοήθησαν στο να κατανοήσουμε τα οφέλη της εφαρμογής του.

Κεφάλαιο 3

Αποτελέσματα Έρευνας

3.0 Δομή Κεφαλαίου

Στο παρόν κεφάλαιο γίνεται ανάλυση και παρουσιάζονται τα αποτελέσματα τόσο της πρωτογενούς όσο και της δευτερογενούς έρευνας που υλοποιήθηκε στα πλαίσια της παρούσας διατριβής.

Κατ' αρχάς εστιάζουμε στις πολιτικές Ασφάλειας & Προστασίας Δεδομένων που εφαρμόζοντα εντός του ΟΤΕ κι έχουν ως στόχο να παράσχουν ένα υψηλό επίπεδο ασφάλειας στους πολίτες , καθώς και στους εργαζόμενους, τις υπηρεσίες, τα προϊόντα, τα περιουσιακά στοιχεία και τις δραστηριότητες του. Στα πλαίσια αυτά, αναλύεται και η πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών που έχει ως στόχο την προστασία των δεδομένων επικοινωνίας και των Συστημάτων που τα διαχειρίζονται από πιθανούς κινδύνους, ούτως ώστε να διασφαλίζεται το απόρρητο των επικοινωνιών. Επιπλέον, το 2009 ο ΟΤΕ δημιούργησε ένα τυποποιημένο και υψηλό επίπεδο προστασίας των προσωπικών δεδομένων κι έτσι παρουσιάζεται ο «Κώδικας Δεοντολογίας για την Προστασία των Δικαιωμάτων του Ατόμου κατά την Επεξεργασία των Προσωπικών Δεδομένων του εντός του ΟΤΕ» (Privacy Code of Conduct - PCoC) .

Εν συνεχεία, αναλύεται το σύνολο του φάσματος εφαρμογής του GDPR εντός ΟΤΕ. Βλέπουμε λοιπόν τις αιτιολογίες επεξεργασίας Προσωπικών Δεδομένων εντός ΟΤΕ, τις επιχειρησιακές μονάδες πρόσβασης Προσωπικών Δεδομένων εντός ΟΤΕ, το χρονικό διάστημα για το οποίο διατηρούνται τα προσωπικά δεδομένα στις βάσεις δεδομένων του ΟΤΕ καθώς και τα δικαιώματά πολιτών σχετικά με την προστασία των δεδομένων τους.

Εν κατακλείδι, για να κατανοήσουμε περισσότερο τον τρόπο λειτουργίας του GDPR στον Όμιλο ΟΤΕ ζητήσαμε από τους εργαζομένους της Υποδιεύθυνσης Ασφάλειας Προσωπικών Δεδομένων να μας απαντήσουν σε ένα ερωτηματολόγιο προσαρμοσμένο στις λειτουργίες του τμήματος, το οποίο απαντήθηκε από το σύνολο των εργαζομένων. Παρουσιάζονται λοιπόν αναλυτικά τα αποτελέσματα της πρωτογενούς έρευνας που πραγματοποιήθηκε για τους σκοπούς της παρούσας διατριβής.

3.1 Δευτερογενής Έρευνα: Πολιτικές Ασφάλειας & Προστασίας Δεδομένων στον ΟΤΕ

Η Εταιρική Πληροφορία ως περιουσιακό στοιχείο, πρέπει να διασφαλιστεί ως προς την Εμπιστευτικότητα, την Ακεραιότητα και την Διαθεσιμότητά της από τους κινδύνους που απορρέουν κατά την επεξεργασία της και την χρήση πληροφοριακών συστημάτων. Η ασφάλεια και η προστασία των δεδομένων α\στον ΟΤΕ διασφαλίζεται μέσω των ακόλουθων Πολιτικών:

• 3.1.1 Πολιτική Ασφάλειας

Στόχος της είναι να διασφαλίσει ένα υψηλό επίπεδο ασφάλειας για τους πελάτες μας, καθώς και για τους εργαζόμενους, τις υπηρεσίες, τα προϊόντα, τα περιουσιακά στοιχεία και τις δραστηριότητες της εταιρείας. Οι κατευθυντήριες γραμμές για την ασφάλεια βασίζονται σε δέκα Αρχές:

Βασική Αρχή 1: Σύννομη συμπεριφορά Η σύννομη συμπεριφορά είναι παράγοντας που εγγυάται την ασφάλεια στην Εταιρεία, ιδιαιτέρως για την αποτελεσματική καταπολέμηση της απάτης, την προστασία των δεδομένων και των πληροφοριών και τη διαφύλαξη του απορρήτου των τηλεπικοινωνιών. Κατά τη διερεύνηση ύποπτων εγκληματικών δραστηριοτήτων ή σοβαρών παραβιάσεων καθηκόντων, οποιαδήποτε

μέτρα ασφαλείας που δύνανται να θίγουν τα δικαιώματα του ατόμου υλοποιούνται μόνο στην περίπτωση που είναι απολύτως αναγκαία.

Βασική Αρχή 2: Προστασία δεδομένων Απαγορεύεται η μη εξουσιοδοτημένη πρόσβαση και χρήση δεδομένων προσωπικού χαρακτήρα πελατών και εργαζομένων, καθώς και των δεδομένων επικοινωνίας.

Βασική αρχή 3: Εμπιστοσύνη πελατών Η εμπιστοσύνη των πελατών ενισχύεται μέσω της αξιοπιστίας των προϊόντων και των υπηρεσιών της Εταιρείας και της αποτελεσματικής προστασίας των δεδομένων τους. Τα δεδομένα προστατεύονται καλύτερα από οποιονδήποτε από τους ανταγωνιστές μας.

Βασική αρχή 4: Κουλτούρα ασφάλειας Η ασφάλεια αποτελεί ακρογωνιαίο λίθο της εταιρικής κουλτούρας και εκπληρώνεται μέσω της έντιμης και ακέραιης συμπεριφοράς των εργαζομένων. Κάθε προϊστάμενος αποτελεί παράδειγμα για τους εργαζόμενους, εφαρμόζοντας τις απαιτήσεις ασφάλειας.

Βασική αρχή 5: Διαφάνεια στην ανάθεση αρμοδιοτήτων Οι αρμοδιότητες ανατίθενται με διαφάνεια, ώστε κάθε εργαζόμενος να γνωρίζει σε ποιον πρέπει να απευθύνεται.

Βασική αρχή 6: Αρχή της αναγκαιότητας της γνώσης (need-to-know) Η πρόσβαση σε πληροφορίες και δεδομένα παρέχεται εφόσον ο εργαζόμενος είναι εξουσιοδοτημένος να τις διαχειρίζεται και με βάση την αρχή αναγκαιότητας της γνώσης (need-to know), προκειμένου να είναι απολύτως αναγκαίες στο πλαίσιο των εργασιακών του καθηκόντων. Τα δικαιώματα πρόσβασης είναι περιορισμένα, εκχωρούνται εγκαίρως και επανεξετάζονται περιοδικά.

Βασική αρχή 7: Ανταγωνιστικό πλεονέκτημα μέσω της τεχνολογίας Χρησιμοποιείται η αιχμή των τεχνολογιών ασφάλειας, ώστε η Εταιρεία να πρωτοπορεί σε σύγκριση με τον ανταγωνισμό.

Βασική αρχή 8: Αποδοτικότητα μέτρων ασφάλειας Τα μέτρα ασφάλειας υλοποιούνται με στόχο να είναι αποτελεσματικά, διατηρώντας την κατάλληλη σχέση κόστους-οφέλους και αξιοποιώντας τη δυνατότητα συνεργιών.

Βασική αρχή 9: Δημιουργία αξίας Οι απαιτήσεις ασφάλειας ενσωματώνονται στις εταιρικές διεργασίες, προκειμένου να διασφαλιστεί η υλοποίηση, προώθηση και πώληση αξιόπιστων προϊόντων και υπηρεσιών, σε μακροχρόνια βάση.

Βασική αρχή 10: Διεθνή πρότυπα ασφάλειας Η υλοποίηση του συστήματος διαχείρισης ασφάλειας στην Εταιρεία βασίζεται σε διεθνώς αναγνωρισμένα πρότυπα για την ασφάλεια.

Για να επιτευχθούν εφαρμόζουμε προληπτικά και ελεγκτικά μέτρα, καθώς και μέτρα για τη μείωση της συνολικής έκθεσης σε κινδύνους και για τη βελτίωση της οργάνωσης της εταιρείας, των λειτουργιών και της παροχής υπηρεσιών. Αυτό γίνεται μέσα από συγκεκριμένους στόχους προστασίας που αφορούν: Ανθρώπους, Πληροφορίες, Συστήματα Πληροφορικής και Τηλεπικοινωνιών, Εγκαταστάσεις, Υποδομές & Εξοπλισμός, Περιουσιακά στοιχεία και Επιχειρησιακή Συνέχεια. Απαιτείται η συμμόρφωση των εργαζομένων, εξωτερικών συνεργατών και προμηθευτών με την Πολιτική Ασφάλειας, η οποία θα πρέπει να λειτουργεί ως ένα εργαλείο διαμόρφωσης επιχειρησιακής κουλτούρας και ως εγχειρίδιο για δράσεις σε θέματα ασφάλειας.

Η αυξανόμενη ψηφιοποίηση και το μεταβαλλόμενο περιβάλλον εργασίας δημιουργούν νέες προκλήσεις για τη διαχείριση των πληροφοριών. Η γρήγορη αξιοποίηση πολύτιμων πληροφοριών μπορεί να αποτελέσει καθοριστικό ανταγωνιστικό πλεονέκτημα. Η αρχή της "αναγκαιότητας της γνώσης" πρέπει να εναρμονίζεται με την αυξανόμενη ανάγκη ταχείας ανταλλαγής πληροφοριών με πολλαπλούς αποδέκτες. Διαβαθμίζουμε τις πληροφορίες ανάλογα με την ανάγκη προστασίας τους. Με βάση την διαβάθμιση, προστατεύουμε τις πληροφορίες και εκπαιδεύουμε τους υπαλλήλους μας για τον ορθό χειρισμό τους. Εκτός από την "εμπιστευτικότητα" των πληροφοριών, προστατεύουμε επίσης την "διαθεσιμότητα" και την "ακεραιότητα" (πληρότητα και γνησιότητα), καθώς και την "αυθεντικότητά" τους (επαλήθευση αποστολέα/παραλήπτη). Η συλλογή και διατήρηση πληροφοριών πραγματοποιείται μόνο για επιχειρησιακές ανάγκες.

Επίπεδα Διαβάθμισης

- Η σήμανση των πληροφοριών ως προς την εμπιστευτικότητα ορίζεται από τον δημιουργό της πληροφορίας, λαμβάνοντας υπόψη την διαβάθμισή της (π.χ. Εμπιστευτικό).
- Η αρμόδια επιχειρησιακή μονάδα που υπάγεται στον Executive Director Επιχειρησιακής Ασφάλειας & Συνέχειας Ομίλου ΟΤΕ ορίζει τα επίπεδα διαβάθμισης των πληροφοριών (π.χ. Εσωτερικό, Εμπιστευτικό).

Σχεδιασμός Μέτρων Ασφάλειας

- Τα μέτρα για την προστασία της πληροφορίας επιλέγονται με γνώμονα την καταλληλότητά τους και την ανάλυση των κινδύνων.
- Η αρμόδια επιχειρησιακή μονάδα που υπάγεται στον Executive Director Επιχειρησιακής Ασφάλειας & Συνέχειας Ομίλου ΟΤΕ καθορίζει τα προτεινόμενα μέτρα προστασίας.
- Κάθε οργανωτική Μονάδα εφαρμόζει τα κατάλληλα μέτρα προστασίας.
- Πρέπει να ορίζονται και να τεκμηριώνονται μέτρα προστασίας για τις πληροφορίες που διαβαθμίζονται ως Αυστηρά Εμπιστευτικές (π.χ. αυθεντικοποίηση δύο παραγόντων, κρυπτογράφηση).

Η αρμόδια επιχειρησιακή μονάδα που υπάγεται στον Executive Director Επιχειρησιακής Ασφάλειας & Συνέχειας Ομίλου ΟΤΕ εγκρίνει εργαλεία επικοινωνίας, συνεργασίας και αποθήκευσης, τα οποία παρέχονται για επαγγελματικούς σκοπούς.

Η αρμόδια επιχειρησιακή μονάδα που υπάγεται στον Executive Director Επιχειρησιακής Ασφάλειας & Συνέχειας Ομίλου ΟΤΕ παρέχει υποστήριξη φιλική προς τον χρήστη για τον κατάλληλο χειρισμό της πληροφορίας.

Τα Συστήματα Πληροφορικής & Τηλεπικοινωνιών, συμπεριλαμβανομένων των δικτύων, εφαρμογών και των προϊόντων, αποτελούν τη ραχοκοκαλιά για την ανταλλαγή ηλεκτρονικών πληροφοριών παγκοσμίως. Η ικανότητα λειτουργίας όλων των τομέων της οικονομίας και της ίδιας της Εταιρείας εξαρτώνται από την απρόσκοπτη λειτουργία των Συστημάτων Πληροφορικής & Τηλεπικοινωνιών. Λόγω της πολυπλοκότητας και του

υψηλού επιπέδου καινοτομίας, η υποδομή είναι εκτεθειμένη σε διάφορες απειλές (τεχνική αστοχία ή κακόβουλες ενέργειες).

Οι σημαντικότεροι τομείς ασφάλειας και οι απαιτήσεις στα Συστήματα Πληροφορικής & Τηλεπικοινωνιών είναι:

Σαφείς και τεκμηριωμένες αρμοδιότητες

Για κάθε Σύστημα Πληροφορικής & Τηλεπικοινωνιών, πρέπει να ορίζονται σαφείς αρμοδιότητες, όσον αφορά τον επιχειρησιακά υπεύθυνο και τεχνικά υπεύθυνο, καθώς και να υπάρχει κατάλογος των στοιχείων (asset inventory) που το απαρτίζουν. Ο επιχειρησιακά υπεύθυνος είναι υπεύθυνος σε όλες τις φάσεις του κύκλου ζωής του συστήματος και για όλα τα θέματα ασφάλειας, σε σχέση με τα δεδομένα που διαχειρίζεται το σύστημα. Ο ρόλος της τεχνικά υπευθύνου είναι να υλοποιεί κατάλληλα τις απαιτήσεις ασφάλειας στο σύστημα.

Επεξεργασία πληροφοριών στα Συστήματα Πληροφορικής & Τηλεπικοινωνιών

Η δημιουργία, επεξεργασία, μετάδοση, αποθήκευση και καταστροφή των πληροφοριών πρέπει να είναι σύμφωνη με τις απαιτήσεις ασφάλειας .

Επάρκεια των μέτρων ασφαλείας

Τα τεχνικά και οργανωτικά μέτρα για την ασφάλεια των πληροφοριών και την προστασία των δεδομένων πρέπει να είναι κατάλληλα και οικονομικά εύλογα. Ως εκ τούτου, ο καθορισμός των μέτρων ασφαλείας στα Συστήματα Πληροφορικής & Τηλεπικοινωνιών πρέπει να πραγματοποιείται βάσει εκτίμησης του ρίσκου και με γνώμονα την επάρκειά τους.

Σχεδιασμός των Συστημάτων Πληροφορικής & Τηλεπικοινωνιών

- Η ασφάλεια πρέπει να ενσωματώνεται σε όλες τις φάσεις του κύκλου ζωής ενός Συστήματος Πληροφορικής & Τηλεπικοινωνιών και ιδιαίτερα στην αρχική φάση του σχεδιασμού. Τα Συστήματα Πληροφορικής & Τηλεπικοινωνιών που αναπτύσσονται στην Εταιρεία ή για λογαριασμό της Εταιρείας πρέπει να σχεδιάζονται και να τεκμηριώνονται με τέτοιο τρόπο, έτσι ώστε όλες οι λειτουργίες και ρυθμίσεις που σχετίζονται με την ασφάλεια και όλοι οι κίνδυνοι

που προκύπτουν από τη χρήση τους, να είναι εύκολα κατανοητοί από την πλευρά του χρήστη. Οι λειτουργίες και ρυθμίσεις, που σχετίζονται με την ασφάλεια, των υπηρεσιών και προϊόντων πρέπει να καθορίζονται προσεκτικά, να υλοποιούνται και να ελέγχονται κατάλληλα πριν από το λανσάρισμά τους.

- Τα Συστήματα Πληροφορικής & Τηλεπικοινωνιών, οι υπηρεσίες, τα προϊόντα, καθώς και οι διαδικασίες εξυπηρέτησης και πωλήσεων που σχετίζονται με αυτά, πρέπει να προστατεύονται κατάλληλα από την κακή χρήση από πελάτες, συνεργάτες, υπαλλήλους και τρίτα μέρη.
- Οι χρήστες πρέπει να γνωρίζουν σαφώς τις ευθύνες τους και τα καθήκοντά τους και να συνεργάζονται για τη διατήρηση της ασφάλειας στα IT/NT συστήματα.
- Τα συστήματα αυθεντικοποίησης πρέπει να υποστηρίζουν τη λειτουργία του Single Sign-On και single log-on.

Προφίλ και δικαιώματα πρόσβασης

- Τα δικαιώματα πρόσβασης στα Συστήματα Πληροφορικής & Τηλεπικοινωνιών πρέπει να ορίζονται σε προφίλ και να υλοποιούνται με κατάλληλες διαδικασίες φυσικής και λογικής πρόσβασης.
- Όλα τα καθορισμένα προφίλ και δικαιώματα πρόσβασης πρέπει να ακολουθούν την αρχή του διαχωρισμού των καθηκόντων. Για την ανάθεση του προφίλ πρέπει να λαμβάνεται υπόψη η θέση του χρήστη και η αρχή της αναγκαιότητας της γνώσης (need-to-know).
- Τα προφίλ με διαχειριστικά δικαιώματα πρέπει να διαχωρίζονται από τα προφίλ με πρόσβαση σε λειτουργικότητες. Τα προφίλ με προνομιακά δικαιώματα πρόσβασης ή δικαιώματα έκτακτης ανάγκης πρέπει να περιορίζονται στο ελάχιστο και να παρακολουθούνται επαρκώς βάσει σχετικής διαδικασίας επαλήθευσής τους.

Αυθεντικοποίηση

- Οι μηχανισμοί αυθεντικοποίησης (κωδικοί πρόσβασης, πιστοποιητικά, κλπ.) πρέπει να είναι μόνο προσωποποιημένοι (εκτός από τις περιπτώσεις όπου αυτό δεν είναι τεχνικά εφικτό, π.χ. για προνομιακή πρόσβαση και πρόσβαση έκτακτης ανάγκης). Πρέπει να δημιουργούνται με ασφαλή τρόπο και απαγορεύεται αυστηρά η προώθηση ή η αποκάλυψή τους σε άλλα πρόσωπα.

- Οι κωδικοί πρόσβασης πρέπει να αλλάζουν τακτικά. Σε υποψία αποκάλυψής τους, πρέπει να αλλάζουν.
- Η διάρκεια ισχύος των μηχανισμών αυθεντικοποίησης πρέπει να είναι περιορισμένη.

Οι διαταραχές/διακοπές λειτουργίας έχουν τη πιθανότητα να θέσουν σε κίνδυνο την επιχειρησιακή λειτουργία της Εταιρείας και να βλάψουν την επωνυμία της Εταιρείας στην αγορά. Για το λόγο αυτό, πρέπει να διασφαλίζεται η ακεραιότητα και διατήρηση της λειτουργικότητας των κρίσιμων επιχειρησιακών διαδικασιών και υπηρεσιών, καθώς και των τεχνολογιών της πληροφορικής και των επικοινωνιών, σε περίπτωση διαταραχών ή / και διακοπών λειτουργιών, εφαρμόζοντας τους ακόλουθους τομείς ασφαλείας και τις αντίστοιχες απαιτήσεις:

Διαχείριση Επιχειρησιακής Συνέχειας

Στόχος της Διοίκησης Επιχειρησιακής Συνέχειας είναι να διασφαλίζει τη συνέχεια των κρίσιμων επιχειρησιακών διαδικασιών και την αδιάλειπτη διάθεση των κρίσιμων προϊόντων και των υπηρεσιών, μέσω της συνεχούς ανάλυσης, αξιολόγησης και αντιμετώπισης των σχετικών κινδύνων. Η Διαχείριση Επιχειρησιακής Συνέχειας εντοπίζει πιθανές απειλές, προσδιορίζει τον αντίκτυπό τους στην Εταιρεία και τις υπηρεσίες και εγγυάται τη συνεχή παροχή υπηρεσιών σε αποδεκτό, προκαθορισμένο επίπεδο, σε περίπτωση απρόσμενων συμβάντων. Η διάρκεια διακοπής μιας κρίσιμης επιχειρησιακής διαδικασίας ή υπηρεσίας, πρέπει να διατηρείται στο ελάχιστο αποδεκτό διάστημα. Η συνέχεια των κρίσιμων επιχειρησιακών διαδικασιών ή υπηρεσιών πρέπει να εξασφαλίζεται με τα κατάλληλα μέτρα επιχειρησιακής συνέχειας.

Διαχείριση Συμβάντων

Στόχος της Διαχείρισης Συμβάντων είναι να παρακολουθεί την κατάσταση της ασφάλειας, να ενημερώνει τους εργαζόμενους ή / και τους εμπλεκόμενους, καθώς και να εξασφαλίζει πιθανή εμπλοκή της Διαχείρισης Έκτακτης Ανάγκης και Κρίσεων. Η ζημιά από τα συμβάντα ασφαλείας μειώνεται με την άμεση αντίδραση και παρέμβαση. Τα περιστατικά ασφάλειας πρέπει να τεκμηριώνονται κατάλληλα. Η διαχείριση συμβάντων πρέπει να διασφαλίζεται επαρκώς.

Διαχείριση Έκτακτης Ανάγκης και Κρίσεων

Ο στόχος της διαχείρισης έκτακτων συμβάντων και κρίσεων είναι να ελαχιστοποιούνται οι επιπτώσεις στην επιχείρηση, τους εργαζόμενους και τους πελάτες, που απορρέουν από συμβάντα έκτακτης ανάγκης ή κρίσης και να λήγει η κατάσταση έκτακτης ανάγκης ή / και κρίσης όσο το δυνατόν γρηγορότερα. Η διαχείριση έκτακτης ανάγκης και κρίσεων πρέπει να διασφαλίζεται επαρκώς.

• 3.1.2 Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών

Η Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, έχει ως στόχο την προστασία των δεδομένων επικοινωνίας και των Συστημάτων που τα διαχειρίζονται από πιθανούς κινδύνους, ούτως ώστε να διασφαλίζεται το απόρρητο των επικοινωνιών. Η Πολιτική αφορά τους χρήστες, συνδρομητές, εργαζόμενους και συνεργάτες της εταιρείας. Η Πολιτική αποτελείται από επιμέρους Πολιτικές, οι οποίες ορίζουν τις απαιτήσεις ασφάλειας που πρέπει να ικανοποιούνται για κάθε επιμέρους κατηγορία ειδικών θεμάτων, οι οποίες είναι:

• Πολιτική Αποδεκτής Χρήσης

Η Πολιτική Αποδεκτής Χρήσης καθορίζει τις υποχρεώσεις του ΟΤΕ αλλά και τις αρχές, τους κανόνες και τις συνέπειες για τους εργαζόμενους και συνεργάτες του, στους οποίους εκχωρείται τι δικαίωμα πρόσβασης σε Σύστηματα και δεδομένα επικοινωνίας, και αποβλέπει στην αποτροπή καταχρηστικής άσκησης των δικαιωμάτων τους και της τέλεσης πράξεων που παραβιάζουν ή συνιστούν κίνδυνο παραβίασης του απορρήτου των επικοινωνιών των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών.

Οι εργαζόμενοι και συνεργάτες του ΟΤΕ οφείλουν να συμμορφώνονται με την Πολιτική, συμπεριλαμβανομένων των σχετικών διαδικασιών, μέτρων ασφαλείας και οδηγιών. Η εταιρεία εξασφαλίζει ότι οι εργαζόμενοι και οι συνεργάτες λαμβάνουν γνώση με κάθε τρόπο και έχουν αποδεχτεί την Πολιτική ως προς την εργασία τους, πριν την απόκτηση

πρόσβασης σε Συστήματα και σε δεδομένα επικοινωνίας, όπως μέσω της αποδοχής όρων χρήσης, υπογραφής συμφωνητικού, ενημέρωση μέσω εσωτερικού forum. Υποχρέωση της εταιρείας είναι να ενημερώνει και να εκπαιδεύει τους εργαζομένους και τους συνεργάτες σχετικά με την εφαρμογή της Πολιτικής και τις τροποποιήσεις αυτής.

Επίσης οι εργαζόμενοι κα οι συνεργάτες που έχουν πρόσβαση στα Συστήματα και τα τηλεπικοινωνιακά δεδομένα των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών δεν επιτρέπετε να αποκαλύπτουν καμία πληροφορία ή στοιχεία που πέφτει στην αντίληψή τους ως αποτέλεσμα της φύσης της εργασίας τους. Και τέλος και οι εργαζόμενοι και οι συνεργάτες έχουν την υποχρέωση να ενημερώνουν το αρμόδιο προσωπικό του ΟΤΕ σε περίπτωση που αντιληφθούν οποιοδήποτε κενό ασφαλείας που μπορεί να θέσει το απόρρητο των επικοινωνιών των συνδρομητών η χρηστών των παρεχόμενων δικτύων ή υπηρεσιών.

Συγκεκριμένα για τους συνεργάτες θα πρέπει να καταγράφονται σε ένα ενημερωμένο αρχείο τα φυσικά και νομικά πρόσωπα που εμπλέκονται στο να παρέχουν τις υπηρεσίες τους αποκτούν πρόσβαση σε δεδομένα επικοινωνίας συνδρομητών ή χρηστών παρεχόμενων δικτύων ή υπηρεσιών.

Επιπλέον με τους συνεργάτες θα πρέπει να υπογράφονται συμβάσεις που τους δεσμεύουν στην μη αποκάλυψη της τήρησης του απορρήτου περιλαμβάνει όρους εμπιστευτικότητας, απαιτήσεις και μέτρα ασφαλείας που διασφαλίζουν το απόρρητο των επικοινωνιών την εμπιστευτικότητα των δεδομένων επικοινωνίας κατά την επικοινωνία και επεξεργασία αυτών από τους συνεργάτες καθώς επίσης την οριστική διαγραφή και καταστροφή αυτών μετά την λήξη της συνεργασίας.

Ο ΟΤΕ έχει την υποχρέωση ως προς τους συνδρομητές και τους χρήστες των παρεχόμενων υπηρεσιών ή δικτύων να τους ενημερώνει κατά την σύναψη της μεταξύ τους σύμβασης αλλά και ανα τακτά χρονικά διαστήματα σχετικά με τα μέτρα που ενδείκνυται να λάβουν για την προστασία του απορρήτου των επικοινωνιών τους, ιδίως σχετικά με κανόνες ορθής χρήσης των τεχνολογιών και πόρων σχετικά με την ασφάλεια των πληροφοριών που σχετίζονται με την διασφάλιση του απορρήτου των επικοινωνιών.

Ως προς την διαχείριση αποθηκευτικών μέτρων το Πρότυπο διαχείρισης καθορίζει τα μέτρα και τις διαδικασίες σχετικά με την χρήση, διακίνηση και καταστροφή των

αποθηκευτικών μέσων, ηλεκτρονικών ή χειρόγραφων εντύπων που περιέχουν δεδομένα επικοινωνίας ή άλλες πληροφορίες που μπορεί να οδηγήσουν σε αποκάλυψη δεδομένων επικοινωνίας χρηστών ή συνδρομητών των παρεχόμενων υπηρεσιών και δικτύων ώστε να αποτρέπεται η αποκάλυψή τους σε μη εξουσιοδοτημένα άτομα.

• Πολιτική Φυσικής Ασφάλειας

Η Πολίτική Φυσικής Ασφάλειας καθορίζει τα απαιτούμενα μέτρα για την αποτροπή της μη εξουσιοδοτημένης φυσικής πρόσβασης στις εγκαταστάσεις του ΟΤΕ, στις οποίες είναι εγκατεστημένα τα Συστήματα, εξαιρουμένων εκείνων που χρησιμοποιούνται αποκλειστικά για την εξυπηρέτηση του κοινού, τον έλεγχο της πρόσβασης σε αυτές καθώς και την προστασία των Συστημάτων.

• Πολιτική Λογικής Πρόσβασης

Η Πολιτική Λογικής Πρόσβασης καθορίζει τη διαβάθμιση των επιπέδων πρόσβασης και θέτει τις απαιτήσεις για τον έλεγχο πρόσβασης στα συστήματα του ΟΤΕ. Ισχύει για τους εργαζόμενους και συνεργάτες του οι οποίοι στο πλαίσιο της εργασίας τους αποκτούν πρόσβαση στα συστήματα και στα σχετικά δεδομένα και τις πληροφορίες.

Για την απόκτηση πρόσβασης σε ένα Σύστημα χρησιμοποιούνται κατάλληλοι μηχανισμοί ελέγχου πρόσβασης και αυθεντικοποίησης των εργαζομένων και συνεργατών. Κατ' ελάχιστον, ο έλεγχος πρόσβασης και αυθεντικοποίησης επιτυγχάνεται με τη χρήση ενός λογαριασμού πρόσβασης που αποτελείται από ένα ζγος ονόματος χρήστη και κωδικού πρόσβασης ή άλλου μηχανισμού που εξασφαλίζει αντίστοιχο επίπεδο ασφαλείας. Πρέπει να τηρείται Αρχείο που αναφέρει αναλυτικά τους μηχανισμούς ελέγχου πρόσβασης και αυθεντικοποίησης για κάθε Σύστημα.

Οι χρησιμοποιούμενοι κωδικοί πρόσβασης θα πρέπει να είναι ισχυροί και να έχουν δημιουργηθεί με τρόπο που να αποτρέπει τον προσδιορισμό τους με εύκολο τρόπο. Ειδικότερα, οι κωδικοί πρόσβασης πρέπει να δημιουργούνται με συνδυασμό δύο (2) τουλάχιστον διαφορετικών ειδών χαρακτήρων (αριθμοί, γράμματα, ειδικοί χαρακτήρες). Οι κωδικοί πρόσβασης θα πρέπει να έχουν υποχρεωτικά να επαρκές ελάχιστο μήκος. Θα πρέπει να απαγορεύεται η χρήση πρόσφατων κωδικών στη διαδικασία αλλαγής τους. Δε θα πρέπει να ακολουθούνται συγκεκριμένα υποδείγματα κατά τη δημιουργία των κωδικών πρόσβασης. Οι κωδικοί πρόσβασης θα πρέπει να αλλάζουν περιοδικά, σε

συχνότητα που καθορίζεται ρητά ανά Σύστημα και αναφέρεται σε Αρχείο. Στο Αρχείο καταγράφονται οι τρόποι με τους οποίους επιβάλλεται η περιοδική αλλαγή των κωδικών πρόσβασης. Σε χαρακτηριστικές περιπτώσεις όπως είναι, ενδεικτικά, η αφαίρεση χρήστη ή η παραβίαση ενός λογαριασμού πρόσβασης, θα πρέπει να προβλέπεται η άμεση αλλαγή του αντίστοιχου κωδικού πρόσβασης. Στην περίπτωση επαναλαμβανόμενης απαγωγής λανθασμένων κωδικών πρόσβασης ο λογαριασμός πρόσβασης θα αδρανοποιείται και θα μπορεί να χρησιμοποιηθεί μόνο μετά την πάροδο ενός προκαθορισμένου χρονικού διαστήματος.

Όσον αφορά την δημιουργία και Διαχείριση Λογαριασμών Πρόσβασης θα πρέπει να :

- ✓ Τηρείται Αρχείο με περιγραφή των κανόνων σύμφωνα με τους οποίους γίνεται η δημιουργία ενός ονόματος χρήστη.
- ✓ Πρέπει να τηρείται Αρχείο με περιγραφή των κανόνων σύμφωνα με τους οποίους γίνεται η δημιουργία ενός κωδικού πρόσβασης.
- ✓ Πρέπει να τηρείται διαδικασία σύμφωνα με την οποία αποδίδεται με ασφάλεια σε κάθε εργαζόμενο και συνεργάτη το όνομα χρήστη και ο κωδικός πρόσβασης που τον αφορά.
- ✓ Πρέπει να τηρείται διαδικασία σύμφωνα με την οποία επιτυγχάνεται η τακτική αλλαγή των κωδικών πρόσβασης και εν γένει η διαχείρισή τους.
- ✓ Πρέπει να τηρείται Αρχείο με περιγραφή των όρων χρήσης των κωδικών πρόσβασης από τους εργαζόμενους και συνεργάτες.
- ✓ Πρέπει να τηρείται διαδικασία σύμφωνα με την οποία διενεργείται έλεγχος για την ορθή εφαρμογή των παραπάνω κανόνων και διαδικασιών, σε συμφωνία με τις αρχές της Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας.
- ✓ Σε κάθε εργαζόμενο και συνεργάτη εκχωρείται προσωπικός λογαριασμός πρόσβασης ανά Σύστημα, ούτως ώστε να είναι δυνατή η αντιστοίχιση συγκεκριμένου προσώπου με τις ενέργειες που τελούνται σε κάθε Σύστημα.
- ✓ Τα ονόματα χρήστη δεν πρέπει να υποδηλώνουν τον ρόλο στο Σύστημα των εργαζομένων και συνεργατών (ενδεικτικό, δεν πρέπει να είναι παράγωγα της λέξης (admin).
- ✓ Η δημιουργία ομαδικών ή/και προκαθορισμένων λογαριασμών πρόσβασης πρέπει να αποφεύγεται. Σε περίπτωση που αυτό δεν είναι εφικτό, θα πρέπει να δικαιολογείται.

- ✓ Πρέπει να εξασφαλίζεται η αντιστοίχιση του συγκεκριμένου φυσικού προσώπου που αποκτά πρόσβαση σε ένα Σύστημα με ομαδικό ή προκαθορισμένο λογαριασμό με τις ενέργειες που τελούνται σε αυτό, με άλλον κατάλληλο μηχανισμό, ο οποίος τεκμηριώνεται σε Αρχείο.

Εκτός της διαχείρισης των Λογαριασμών Πρόσβασης σημαντική είναι και η διαχείριση των χρηστών που χρησιμοποιούν τα Συστήματα. Έτσι η Διαδικασία Διαχείρισης Χρηστών Συστημάτων :

- ✓ Πρέπει να τηρείται Διαδικασία Διαχείρισης Χρηστών Συστήματος.
- ✓ Στη Διαδικασία Διαχείρισης Χρηστών Συστημάτων περιγράφεται με σαφήνεια ο τρόπος προσθήκης νέων χρηστών, η διαγραφή χρηστών καθώς και η απονομή και μεταβολή των δικαιωμάτων ή επιπέδων πρόσβασης.
- ✓ Για την παροχή, τροποποίηση και κατάργηση δικαιωμάτων πρόσβασης απαιτείται υποχρεωτικό η προηγούμενη έγκριση απο αρμόδιο εργαζόμενο της Εταιρείας.
- ✓ Στη Διαδικασία Διαχείρισης Χρηστών Συστημάτων προβλέπεται η υποχρέωση τήρησης Αρχείου των αιτήσεων που αφορούν σε κάθε μεταβολή στην κατάσταση πρόσβασης των χρηστών Συστημάτων.
- ✓ Πρέπει να τηρείται Αρχείο στο οποίο καταγράφονται οι κατηγορίες των χρηστών και τα δικαιώματα πρόσβασης αυτών για κάθε Σύστημα.
- ✓ Πρέπει να τηρείται Αρχείο στο οποίο καταγράφονται οι τρόποι πρόσβασης των εργαζομένων και συνεργατών σε δεδομένα επικοινωνίας των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών.
- ✓ Πρέπει να τηρείται Αρχείο με την αντιστοίχιση των λογαριασμών πρόσβασης των εργαζόμενων και συνεργατών στους οποίους αυτοί έχουν αποδοθεί, ούτως ώστε να είναι δυνατό να διαπιστώνεται ποιος είναι ο κάτοχος κάθε λογαριασμού πρόσβασης και για ποιο χρονικό διάστημα.

Σε όλα τα παραπάνω θα πρέπει να υπάρχει μία διαδικασία Ελέγχου Ορθής Εφαρμογής της Πολιτικής Λογικής Πρόσβασης στην οποία περιγράφονται με σαφήνεια οι περιοδικοί έλεγχοι που πραγματοποιούνται, σε συμφωνία με τις αρχές της Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών και γι’ αυτό υπάρχει αρχείο καταγραφής των προσβάσεων των χρηστών

των Συστημάτων σε αυτά, στο οποίο καταγράφονται, κατ' ελάχιστον, το όνομα χρήστη που απέκτησε την πρόσβαση, και η ημερομηνία και ώρα εκκίνησης και τερματισμού της πρόσβασης

Η Διαδικασία ελέγχου Ορθής εφαρμογής της Πολιτικής Λογικής Πρόσβασης καλύπτει :

1. τον έλεγχο των δικαιωμάτων πρόσβασης των χρηστών, ήτοι, εάν το δικαίωμα πρόσβασης κάθε χρήστη είναι πράγματι αυτό που του αποδόθηκε,
2. τον έλεγχο των λογαριασμών πρόσβασης, ήτοι, την αντιπαραβολή του Αρχείου που περιλαμβάνει τις εγκεκριμένες αιτήσεις με τους λογαριασμούς που προκύπτουν από έκαστο Σύστημα,
3. Τον δειγματοληπτικό έλεγχο των αρχείων καταγραφής πρόσβασης (access log) για την ανακάλυψη ενδεχομένων μη αιτιολογημένων προσβάσεων.

Τέλος οι απαιτήσεις σχετικά με τους Συνδρομητές ή Χρήστες των παρεχόμενων δικτύων ή υπηρεσιών είναι ότι θα πρέπει να διατηρείται Αρχείο που αναφέρει αναλυτικά τους μηχανισμούς ελέγχου πρόσβασης και αυθεντικοποίησης που χρησιμοποιούνται για την πρόσβαση των συνδρομητών ή χρηστών στις υπηρεσίες και τα δίκτυα που παρέχει ο ΟΤΕ, να ακολουθείται συγκεκριμένη διαδικασία διαχείρισης των λογαριασμών πρόσβασης των συνδρομητών και χρηστών στις υπηρεσίες και τα δίκτυα στην οποία θα περιγράφεται κατ' ελάχιστον με σαφήνεια ο τρόπος προσθήκης και κατάργησης λογαριασμών πρόσβασης καθώς και η απόδοση του ονόματος χρήστη και του κωδικού πρόσβασης στους συνδρομητές ή χρήστες των παρεχόμενων δικτύων και υπηρεσιών, να ενημερώνει με κάθε μέσο τους συνδρομητές ή χρήστες των παρεχόμενων δικτύων ή υπηρεσιών σχετικό με την αναγκαιότητα αλλαγής του κωδικού πρόσβασης καθώς και σχετικό με ενδεδειγμένους κανόνες δημιουργίας ισχυρών κωδικών πρόσβασης.

Να υπάρχει διαδικασία σύμφωνα με την οποία διενεργείται περιοδικός έλεγχος σχετικό με την αλλαγή του κωδικού πρόσβασης που αποδίδεται στους συνδρομητές ή χρήστες των παρεχόμενων δικτύων ή υπηρεσιών και εξασφαλίζει την εκ νέου ενημέρωσή τους σχετικά με την αναγκαιότητα αλλαγής των κωδικών πρόσβασης σε περίπτωση που δεν έχουν προβεί στην σχετική αλλαγή. Σε περίπτωση που δίνεται η δυνατότητα στους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών να αποκτήσουν πρόσβαση σε δεδομένα επικοινωνίας τους (ενδεικτικό, εξερχόμενες κλήσεις, ηλεκτρονικό Ταχυδρομείο) μέσω συγκεκριμένης φόρμας, πρέπει να χρησιμοποιούνται

ευρέως αποδεκτοί μηχανισμοί ασφαλούς αυθεντικοποίησης και κρυπτογράφησης. Και όλα αυτά να είναι καταγεγραμμένα σε ένα Αρχείο.

• Πολιτική Απομακρυσμένης Λογικής Πρόσβασης

Η Πολιτική Απομακρυσμένης λογικής Πρόσβασης καθορίζει τη διαβάθμιση των επιπέδων πρόσβασης και θέτει τις απαιτήσεις για τον έλεγχο απομακρυσμένης πρόσβασης στα Συστήματα του ΟΤΕ. Ισχύει για τους εργαζομένους και συνεργάτες οι οποίοι στο πλαίσιο της εργασία τους αποκτούν απομακρυσμένη πρόσβαση στα Συστήματα και στα σχετικά δεδομένα και τις πληροφορίες.

Οι απαιτήσεις ως προς την Πολιτική Απομακρυσμένης Πρόσβασης των εργαζομένων και των συνεργατών αναλύεται ως εξής :

- Η απομακρυσμένη πρόσβαση εργαζομένων και συνεργατών στα Συστήματα πρέπει να περιορίζεται στις περιπτώσεις όπου αυτό είναι απαραίτητο για τις υπηρεσιακές ανάγκες της Εταιρείας.
- Πρέπει να διατηρείται Αρχείο στο οποίο καταγράφονται τα Συστήματα στα οποία επιτρέπεται η απομακρυσμένη πρόσβαση, και οι τεχνικοί τρόποι απομακρυσμένης πρόσβασης εργαζομένων και συνεργατών της Εταιρίας, για κάθε Σύστημα στο οποίο έχει επιτραπεί η απομακρυσμένη πρόσβαση.
- Τηρείται Αρχείο με τους εργαζομένους και συνεργάτες (ονοματεπώνυμο και ιδιότητα), οι οποίοι έχουν εξουσιοδοτηθεί για χρήση της απομακρυσμένης πρόσβασης. Στο εν λόγω Αρχείο καταγράφονται τα δικαιώματα πρόσβασης που τους αντιστοιχούν για κάθε Σύστημα .
- Η απομακρυσμένη πρόσβαση των εργαζομένων και συνεργατών πραγματοποιείται με χρήση μηχανισμών ασφαλούς αυθεντικοποίησης και κρυπτογράφησης (π.χ. μέσω VPN).
- Πρέπει να εξασφαλίζεται ότι κάθε σύνδεση εργαζομένων και συνεργατών στα Συστήματα επιτρέπεται μόνο εφόσον η σύνδεση αυτή δεν παραβιάζει κάποιον από τους κανόνες ασφάλειας του δικτύου.
- Η απομακρυσμένη πρόσβαση των συνεργατών πρέπει να επιτρέπεται μόνο για συγκεκριμένο χρονικό διάστημα και να γίνεται είτε με τη χρήση προσωρινών κωδικών, οι οποίοι θα μεταβάλλονται μετά το πέρας του προκαθορισμένου

χρονικού διαστήματος είτε με την απενεργοποίηση των λογαριασμών μετά το πέρας του διαστήματος αυτού.

- Η απομακρυσμένη πρόσβαση των συνεργατών στα Συστήματα της Εταιρίας επιτρέπεται μόνο κατόπιν έγκρισης των σχετικών αιτημάτων, στο οποίο θα αναγράφεται ο λόγος της πρόσβασης, το Σύστημα στο οποίο θα πραγματοποιηθεί η πρόσβαση καθώς και το χρονικό διάστημα που απαιτείται. Πρέπει να τηρείται Αρχείο με όλες τις πληροφορίες της παρούσας παραγράφου.

Και τέλος για την διαχείριση Λογαριασμών Απομακρυσμένης Πρόσβασης θα πρέπει να ακολουθείται συγκεκριμένη διαδικασία διαχείρισης των λογαριασμών απομακρυσμένης πρόσβασης των εργαζομένων και συνεργατών, σύμφωνα με τις απαιτήσεις της παρούσας Πολιτικής και θα πρέπει να διενεργούνται τριμηνιαίοι έλεγχοι στα δικαιώματα απομακρυσμένης πρόσβασης των χρηστών σε συμφωνία με τις αρχές της Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής. Οι έλεγχοι περιλαμβάνουν:

I. αντιστοίχιση των λογαριασμών απομακρυσμένης πρόσβασης και του Αρχείου των εργαζομένων και συνεργατών που έχουν εξουσιοδοτηθεί να χρησιμοποιούν την απομακρυσμένη πρόσβαση,
II. έλεγχος της υλοποίησης των απαιτούμενων μεταβολών των κωδικών και ενεργοποιήσεων των λογαριασμών απομακρυσμένης πρόσβασης των συνεργατών.

• <u>Πολιτική Διαχείρισης & Εγκατάστασης Συστημάτων</u>

Σκοπός της Πολιτικής είναι να προσδιορίσει τις απαιτήσεις και τρία να ικανοποιούνται κατά τη σχεδίαση, ανάπτυξη προμήθεια, εγκατάσταση, λειτουργία, διαχείριση, υποστήριξη αναβάθμιση, επικαιροποίηση, διαγραφή και απόσυρση των Συστημάτων προκειμένου να διασφαλίζεται το απόρρητο των επικοινωνιών και οι απαιτήσεις ασφάλειας.

Κατά τη διαχείριση και εγκατάσταση Συστημάτων, η Εταιρία λαμβάνει τα απαραίτητα μέτρα προκειμένου να ελαχιστοποιείται ο κίνδυνος διαρροής πληροφοριών που σχετίζονται με το απόρρητο των επικοινωνιών των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών.

Οι αλλαγές (εισαγωγή/μεταβολή /διαγραφή) στο λογισμικό/υλικό των Συστημάτων θα πρέπει να πραγματοποιούνται χωρίς υπαίτια καθυστέρηση.

Η Εταιρία διατηρεί και εφαρμόζει της παρακάτω διαδικασίες:

- Διαδικασία Προμήθειας - Ανάπτυξης υλικού και λογισμικού των Συστημάτων, για την προμήθεια-ανάπτυξη υλικού και λογισμικού.
- Διαδικασία Δοκιμών, Αποδοχής και Ελέγχου Ορθής Λειτουργίας Υλικού και Λογισμικού των Συστημάτων, για την εγκατάσταση-λειτουργία Υλικού και Λογισμικού
- Διαδικασία Ελέγχου Συντήρησης Υποστήριξης Λειτουργίας Υλικού και Λογισμικού των Συστημάτων, για την Συντήρηση-Υποστήριξη-Λειτουργία Υλικού και Λογισμικού
- Διαδικασία διαγραφής Απόσυρσης Υλικού και λογισμικού των Συστημάτων, για την Διαγραφή-Απόσυρση Υλικού και Λογισμικού

• <u>Πολιτική Διαχείρισης Περιστατικών Ασφάλειας</u>

Η Πολιτική Διαχείρισης Περιστατικών Ασφάλειας έχει ως σκοπό:

- να καταγραφούν οι λεπτομέρειες κάθε περιστατικού ασφαλείας
- να διερευνηθούν τα αίτια και να προσδιοριστούν οι τεχνικές ή/και οργανωτικές αδυναμίες στις οικείες ενδεχομένως οφείλεται το περιστατικό ασφάλειας,
- να καθοριστούν οι συνέπεια και να υλοποιηθούν οι ενέργειες αποκατάστασης με συγκεκριμένο χρονοδιάγραμμά, ανάλογα με την περίπτωση και να ενημερωθούν:

1. ο Υπεύθυνος Διασφάλισης του Απορρήτου των Επικοινωνιών και τα αρμόδια στελέχη της Εταιρείας,
2. οι αρμόδιες Αρχές και
3. οι θιγμένοι συνδρομητές ή χρήστες σύμφωνα με την κείμενη νομοθεσία.

Σε περίπτωση περιστατικού ασφάλειας, πρέπει να ενημερώνεται η Α.Δ.Α.Ε., υποβάλλοντος έγγραφο με τίτλο «Έκθεση Άμεσης Αναφοράς Περιστατικού Ασφάλειας, Στην οποία καταγράφονται, κατ' ελάχιστον, πληροφορίες, σύμφωνα με τα δεδομένα που είναι διαθέσιμα κατά τον χρόνο πραγματοποίησης της ενημέρωσης. Μετά την ολοκλήρωση της αντιμετώπισης και της διερεύνησης του περιστατικού, πρέπει να υποβάλλεται στην Α.Δ.Α.Ε. έγγραφο με τίτλο «Τελική Έκθεση Αναφοράς Περιστατικού

Ασφάλειας», στο οποίο καταγράφονται με λεπτομέρεια όλες οι πληροφορίες , καθώς και κάθε πρόσθετη πληροφορία που τυχόν έχει στη διάθεσή ο ΟΤΕ.

Στη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας πρέπει να ορίζονται τα αρμόδια στελέχη του ΟΤΕ στα οποία θα πρέπει να αναφέρονται άμεσα τα περιστατικά ασφάλειας, καθώς και τα σχετικά στοιχεία επικοινωνίας αυτών. Η Εταιρία πρέπει να παρέχει στους συνδρομητές ή χρήστες των παρεχόμενων δικτύων ή υπηρεσιών της τη δυνατότητα να καταγγέλλουν με απλά μέσα την ενδεχόμενη παραβίαση του απορρήτου των επικοινωνιών τους. Πρέπει να ελέγχεται σε τακτά χρονικά διαστήματα η ετοιμότητα ενεργοποίησης της Διαδικασίας Διαχείρισης Περιστατικών Ασφάλειας, σε συμφωνία με τις αρχές της Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής.

• Πολιτική Ασφάλειας Δικτύου

Σκοπός της Πολιτικής Ασφάλειας Δικτύου είναι ο λογικός διαχωρισμός των δικτύων από εξωτερικά δίκτυα και η κατάτμηση των δικτύων σε ζώνες ασφαλείας ή υποδίκτυα, ανάλογα το επίπεδο ασφαλείας που απαιτείται, με στόχο την απομόνωση των συστημάτων σε ζώνες ασφαλείας, τον διαχωρισμό αυτών σε δικτυακό επίπεδο και τον έλεγχο της ροής δεδομένων μεταξύ αυτών

• Πολιτική Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών

Η Πολιτική Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών καθορίζει της απαιτήσεις και το πλαίσιο διεξαγωγής ελέγχων που διενεργεί η Εταιρία, με σκοπό την ορθή τήρηση των επιμέρους πολιτικών και διαδικασιών, τη διαπίστωση επάρκειας και αποτελεσματικότητας των μηχανισμών ασφαλείας και τον έλεγχο των τεχνικών ευπαθειών στα Συστήματα.

Πρέπει να πραγματοποιείται έλεγχος εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, ο οποίος καταγράφεται σε Αρχείο, καλύπτει όλο το εύρος εφαρμογής της Πολιτικής και πραγματοποιείται ανά δύο έτη. Ο έλεγχος περιλαμβάνει τη χρήση και την εξέταση των αρχείων καταγραφής κάθε Συστήματος, κατά περίπτωση σε συσχετισμό με άλλα αρχεία που προβλέπονται στην Πολιτική.Επίσης οι έλεγχοι είναι δυνατό να πραγματοποιούνται από εξωτερικό φορέα ή από εξουσιοδοτημένους εργαζόμενους της Εταιρείας. Στην περίπτωση διεξαγωγής του

ελέγχου από εξωτερικό φορέα, λαμβάνεται μέριμνα από την Εταιρία αναφορικά με ζητήματα τήρησης της εμπιστευτικότητας και μη διαρροής πληροφοριών και δεδομένων, μέσω σχετικής σύμβασης. Καθ' όλη τη διάρκεια διεξαγωγής του ελέγχου από τον εξωτερικό φορέα, πρέπει να παρίσταται εξουσιοδοτημένος εργαζόμενος της Εταιρείας,

Στην περίπτωση διεξαγωγής του ελέγχου από ειδικό εξουσιοδοτημένους εργαζόμενους της Εταιρείας, αυτοί θα πρέπει να είναι κατάλληλα εκπαιδευμένοι και να λαμβάνονται υπόψη παράγοντες αντικειμενικότητας και αμεροληψίας (π.χ. οι ελεγκτές δεν θα πρέπει να ανήκουν στην Οργανωτική Μονάδα της οποίας το Συστήματα ελέγχονται ή να έχουν συμμετάσχει στην ανάπτυξη κώδικα και στην εγκατάσταση ή λειτουργία του Συστήματος).

Τα στάδια προετοιμασίας κάθε ελέγχου περιλαμβάνουν τα ακόλουθα:

Τον καθορισμό του Συστήματος και των διαδικασιών/μηχανισμών διασφάλισης του απορρήτου που θα ελεγχθούν και των ελέγχων για την εύρεση τεχνικών ευπαθειών

• Το χρονοδιάγραμμα διεξαγωγής του ελέγχου

• Τη συλλογή των απαιτούμενων πληροφοριών και δεδομένων και

• Τον ορισμό των προσώπων που απαρτίζουν την ομάδα ελέγχου.

Σε περίπτωση που προκύψουν ευρήματα από τον έλεγχο, ο ΟΤΕ ορίζει της απαιτούμενες ενέργειες (όπως είναι ενδεικτικά η αναθεώρηση διαδικασιών/οδηγιών, η επικαιροποίηση λογισμικού, η τροποποίηση παραμέτρων τεχνικής διαμόρφωσης, η μερική ή ολική αντικατάσταση Συστήματος ή εφαρμογής) , Το χρονοδιάγραμμα πραγματοποίησής τους, τις αρμοδιότητες των εργαζομένων και των συνεργατών για την πραγματοποίηση των διορθωτικών ενεργειών και τα πρόσωπα που θα είναι ειδικά εξουσιοδοτημένα να ελέγχουν την ορθή υλοποίηση των ενεργειών της παρούσας παραγράφου. Αναλόγως της φύσης και της κρισιμότητας των ευρημάτων, το υπόχρεο πρόσωπο ενεργοποιεί την Πολιτική Διαχείρισης Περιστατικών Ασφάλειας.

• Πολιτική Αντιμετώπισης Κακόβουλου Λογισμικού

Η Πολιτική Αντιμετώπισης Κακόβουλου λογισμικού καθορίζει τις απαιτήσεις και περιγράφει τα Τεχνικό και οργανωτικά μέτρα που απαιτούνται προκειμένου να προστατεύονται τα Συστήματα της Εταιρίας έναντι του κακόβουλου λογισμικού.

Ο ΟΤΕ λαμβάνει όλα τα απαραίτητα οργανωτικά και τεχνικά μέτρα ασφάλειας, τα οποία αποσκοπούν στην αποτροπή, ανίχνευση και αντιμετώπιση του κακόβουλου λογισμικού. Οφείλει να ενημερώνει τους εργαζόμενους αναφορικά με τους κινδύνους το κακόβουλο λογισμικό καθώς και για τις υποχρεώσεις τους σε σχέση με τα μέτρα προστασίας έναντι του κακόβουλου λογισμικού. Σε συμφωνία με τις αρχές της Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής να πραγματοποιεί έλεγχο της ακεραιότητας του λογισμικού των Συστημάτων. Ο έλεγχος αυτός έχει ως σκοπό τη διαπίστωση της μη ύπαρξης λογισμικού στα Συστήματα πέραν αυτού που έχει επισήμως προμηθευτεί. Χρείαζεται να ορίσει τους κατάλληλους μηχανισμούς για τον περιορισμό της εξάπλωσης του κακόβουλου λογισμικού, σε περίπτωση ανίχνευσής του. Στην περίπτωση αυτή θα πρέπει να πραγματοποιείται άμεση αξιολόγηση του περιστατικού και αναλόγως της χρησιμότητάς του, να ενεργοποιείται η Πολιτική Διαχείρισης Περιστατικών Ασφάλειας. Και τέλος οφείλει να διατηρεί Αρχείο στο οποίο καταγράφονται οι λεπτομέρειες εφαρμογής των απαιτήσεων της Πολιτικής.

• Πολιτική Χρήσης Κρυπτογραφίας

Η Πολιτική Χρήσης Κρυπτογραφία ορίζει την υποχρέωση του ΟΤΕ να χρησιμοποιεί κατάλληλους αλγόριθμους και συστήματα κρυπτογραφίας για την επαρκή προστασία των δεδομένων επικοινωνίας και άλλων πληροφοριών που μπορεί να οδηγήσουν σε αποκάλυψη δεδομένων επικοινωνίας των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών (π.χ. κώδικα πρόσβασης δεδομένα διάρθρωσης Συστημάτων) κατά την αποθήκευση και μεταφορά τους ας Συστήματα, καθώς και το ελάχιστα χαρακτηριστικά ασφάλεια των συστημάτων κρυπτογραφίας.

Η Εταιρεία πρέπει να εφαρμόζουν συστήματα κρυπτογράφησης για την επαρκή προστασία των δεδομένων επικοινωνίας κατά την αποθήκευση και μεταφορά τους μέσω δικτύων. Πρέπει να εφαρμόζεται στα Συστήματα με βάση τα αποτελέσματα που προκύπτουν από την αποτίμηση κινδύνου σε συμφωνία με τις αρχές της παρ. 5.2 της Πολιτικής Σε περίπτωση που χρησιμοποιούνται αλγόριθμοι και συστήματα κρυπτογράφησης συμπεριλαμβανομένων και των αλγορίθμων ψηφιακής υπογραφής, λαμβάνονται υπόψη τα διεθνώς ευρέως αποδεκτά πρότυπα. Το μήκος κλειδιού που

χρησιμοποιείται θα πρέπει να λαμβάνει υπόψη τα διεθνώς και ευρέως αποδεκτά πρότυπα, ανάλογα με τον χρησιμοποιούμενο αλγόριθμο κρυπτογράφησης και με τα αποτελέσματα της εκτίμησης κινδύνου, σε συμφωνία με τις αρχές της παρ. 5.2 της Πολιτικής Η Εταιρία οφείλω να αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση στα κλαδιά τα οποία χρησιμοποιούνται για κρυπτογράφηση, αυθεντικοποίηση ή ψηφιακή υπογραφή.

Σε περίπτωση που χρησιμοποιούνται ασύμμετροι κρυπτογραφικοί αλγόριθμοι (α) για λογική πρόσβαση σε Συστήματα, (β) για κρυπτογράφηση η (γ) για ψηφιακή υπογραφή, κάθε ζεύγος ιδιωτικού/δημόσιου κλειδιού θα πρέπει να αντιστοιχεί σε έναν μοναδικό χρήστη και το αντίστοιχο ιδιωτικό κλειδί θα πρέπει να είναι γνωστό μόνο στον εικόνα χρήστη, στον οποίο αντιστοιχεί.

Σε περίπτωση που η Εταιρία χρησιμοποιεί ψηφιακά πιστοποιητικά δημόσιων κλειδιών, τα οποία παράγονται από παρόχους υπηρεσιών πιστοποίησης, οφείλει να εξασφαλίζει οτι ο πάροχος υπηρεσιών πιστοποίησης συμμορφώνεται με την κείμενη νομοθεσία. Σε περίπτωση που η Εταιρία παράγει και διαχειρίζεται κλειδιά κρυπτογράφησης τα οποία χρησιμοποιούνται σε Συστήματα, θα πρέπει να καταρτίζει και να τηρεί κατάλληλες διαδικασίες για τη δημιουργία, πιστοποίηση, διανομή και ανάκληση των κρυπτογραφικών κλειδιών.

• 3.1.3 Διαχείριση Εξαιρέσεων από την Πολιτική Ασφάλειας

Κάθε αδυναμία συμμόρφωσης με τις απαιτήσεις της Πολιτικής, συμπεριλαμβανομένων των επιμέρους Πολιτικών και των διαδικασιών που την υλοποιούν, η οποία, ενδεικτικά, μπορεί να οφείλεται σε μη εφαρμοσιμότητα ή σε τεχνική αδυναμία κάλυψης συγκεκριμένων απαιτήσεων, καταγράφεται και τεκμηριώνεται επαρκώς ως εξαίρεση από την Πολιτική. Για τη διαχείριση των εξαιρέσεων, πρέπει να εφαρμόζεται σχετική διαδικασία καταγραφής και τεκμηρίωσής τους. Για κάθε εξαίρεση από την Πολιτική, πρέπει να υπάρχει κατάλληλα τεκμηριωμένο αίτημα από τον αρμόδιο Διευθυντή. Σε αυτό πρέπει να περιγράφονται κατ΄ ελάχιστο οι λόγοι που κάνουν την απόκλιση αναγκαία, τα μέτρα που λαμβάνονται για τον περιορισμό του ρίσκου και τις προϋποθέσεις άρσης της εξαίρεσης. Το αίτημα πρέπει να εγκρίνεται από τον αρμόδιο Chief Officer και να γίνεται αποδεκτό από τον Διευθυντή Ασφάλειας Πληροφοριών & Αποτροπής Τηλεπικοινωνιακής Απάτης Ομίλου ΟΤΕ.

• 3.1.4 Εταιρικοί Δεσμευτικοί Κανόνες για την Προστασία Προσωπικών Δεδομένων εντός του Ομίλου της Deutsche Telekom

Με την εφαρμογή του «Κώδικα Δεοντολογίας για την Προστασία των Δικαιωμάτων του Ατόμου κατά την Επεξεργασία των Προσωπικών Δεδομένων του εντός του Ομίλου ΟΤΕ» (Privacy Code of Conduct - PCoC) το 2009, ο Όμιλος ΟΤΕ έχει δημιουργήσει ένα τυποποιημένο και υψηλό επίπεδο προστασίας των προσωπικών δεδομένων. Οι νέοι «Εταιρικοί Δεσμευτικοί Κανόνες για την Προστασία Προσωπικών Δεδομένων εντός του Ομίλου της Deutsche Telekom» (Binding Corporate Rules Privacy - BCRP) αποτελούν τη συνέχεια του PCoC και το αντικαθιστούν.

Οι νέοι «Εταιρικοί Δεσμευτικοί Κανόνες για την Προστασία Προσωπικών Δεδομένων εντός του Ομίλου της Deutsche Telekom» αποτελούν τις νομικές απαιτήσεις για τη ανταλλαγή των προσωπικών δεδομένων τόσο εντός του Ομίλου Deutsche Telekom όσο κι εκτός Ομίλου. Περιέχουν τις ελάχιστες ισχύουσες απαιτήσεις σύμφωνα με την ευρωπαϊκή νομοθεσία για την επαρκή προστασία των προσωπικών δεδομένων. Από τον Δεκέμβριο του 2013 ισχύουν εντός της Deutsche Telekom και σταδιακά τίθενται σε ισχύ και στις υπόλοιπες εταιρείες του Ομίλου. Οι «Εταιρικοί Δεσμευτικοί Κανόνες για την Προστασία Προσωπικών Δεδομένων εντός του Ομίλου της Deutsche Telekom» έχουν υιοθετηθεί από τα Διοικητικά Συμβούλια του ΟΤΕ και της COSMOTE.

3.2 Εφαρμογή του GDPR εντός ΟΤΕ

3.2.1 Αιτιολογία Επεξεργασίας Προσωπικών Δεδομένων εντός ΟΤΕ

Η επεξεργασία των προσωπικών δεδομένων εφαρμόζεται σε οιονδήποτε υπόκειται σε κάποιου είδους σχέση με τον ΟΤΕ (εργασιακή, πελατειακή, εξωτερικών συνεργατών κ.ά.) και σύμφωνα με τα προβλεπόμενα στον Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR) και την Εθνική Νομοθεσία. Έτσι, έχουμε τις εξής περιπτώσεις:

α. **Για την έναρξη, λειτουργία και τον τερματισμό της συμβατικής σχέσης με τον ΟΤΕ**

Ο ΟΤΕ επεξεργάζεται τα δεδομένα για τους σκοπούς της εργασιακής ή άλλης συμβατικής σχέσης και συγκεκριμένα για την έναρξη, λειτουργία και τον τερματισμό αυτής και την εκπλήρωση των δικαιωμάτων και υποχρεώσεων των Εταιρειών, που προκύπτουν από νόμο ή συλλογική σύμβαση εργασίας. Συνεπώς, επεξεργάζεται τα δεδομένα στο πλαίσιο της διαχείρισης του ανθρώπινου δυναμικού των Εταιρειών, της ανάπτυξής του, καθώς και σε εταιρικές επικοινωνίες.

β. **Στο πλαίσιο έννομου συμφέροντος των Εταιρειών (άρθρο 6(1)(f) GDPR)**

Όταν απαιτείται, ο ΟΤΕ επεξεργάζεται τα δεδομένα για να προστατευτεί το έννομο συμφέρον των Εταιρειών ή τρίτων νομικών ή φυσικών προσώπων. Παράδειγμα:

- ✓ Μέτρα για την ασφάλεια κτιρίων και εγκαταστάσεων (π.χ. έλεγχος πρόσβασης)
- ✓ Μέτρα για τη διαχείριση κινδύνων (π.χ. εσωτερικός έλεγχος που διενεργείται από την Υπηρεσία Εσωτερικού Ελέγχου)
- ✓ Μέτρα για την ασφάλεια των συστημάτων (π.χ. έλεγχος αρχείων καταγραφής προσβάσεων και ενεργειών)

γ. **Σε συμμόρφωση με νομική υποχρέωση (άρθρο 6 (1) (c) GDPR)**

Ως αντισυμβαλλόμενος, ο ΟΤΕ οφείλει να συμμορφώνεται με νομικές υποχρεώσεις, που προκύπτουν, για παράδειγμα, από φορολογική νομοθεσία (π.χ. παρακράτηση και απόδοση φόρου εισοδήματος), από ασφαλιστική νομοθεσία (π.χ. παρακράτηση και απόδοση ασφαλιστικών εισφορών) κλπ.

δ. **Σε συνέχεια παροχής συγκατάθεσης από μέρους σας (άρθρο 6 (1) (a) GDPR)**

Είναι επίσης θεμιτό ο ΟΤΕ να επεξεργάζεται τα δεδομένα σε συνέχεια παροχής από μέρους ρητής συγκατάθεσης (π.χ. για την επεξεργασία δεδομένων σας στην Deutsche Telekom), εφόσον η συγκατάθεση έχει δοθεί νόμιμα. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε και ισχύει για το μέλλον.

3.2.2 Επιχειρησιακές Μονάδες Πρόσβασης Προσωπικών Δεδομένων εντός ΟΤΕ

Οι επιχειρησιακές μονάδες που έχουν πρόσβαση στα προσωπικά δεδομένα είναι αυτές που έχουν την αρμοδιότητα για την εκπλήρωση των συμβατικών και νομικών υποχρεώσεων που προκύπτουν από την εργασιακή ή άλλη συμβατική σχέση που μας συνδέει. Για την επεξεργασία των δεδομένων, οι Εταιρείες μπορούν, σύμφωνα με το άρθρο 28 του GDPR, να χρησιμοποιούν τρίτες εταιρίες - συνεργάτες (όπως για παράδειγμα το Κέντρο Εξυπηρέτησης Εργαζομένων My HR). Ακόμη και σε αυτή την περίπτωση, οι Εταιρείες εξακολουθούν να είναι υπεύθυνες για την προστασία των δεδομένων. Κατά την επεξεργασία των δεδομένων, κάθε συνεργάτης μας (φυσικό ή νομικό πρόσωπο) ακολουθεί τις σαφείς οδηγίες του ΟΤΕ. Για να διασφαλιστεί ότι αυτό τηρείται σε κάθε περίπτωση, έχουν δεσμευτεί οι συνεργάτες του ΟΤΕ με συμβατικές ρήτρες και διενεργούνται τακτικοί έλεγχοι. Συνεργάτες του ΟΤΕ είναι νομικά ή φυσικά πρόσωπα, τα οποία δραστηριοποιούνται στις εξής κατηγορίες: Υπηρεσίες Πληροφορικής, Υπηρεσίες Διαχείρισης Ανθρώπινου Δυναμικού, Συμβουλευτικές Υπηρεσίες αξιολόγησης και ανάπτυξης Ανθρώπινου Δυναμικού Υπηρεσίες Εκπαίδευσης, Συμβουλευτικές Υπηρεσίες, Εταιρίες Φύλαξης Εγκαταστάσεων, Εξωτερικές υπηρεσίες Προστασίας και Πρόληψης (ΕΞΥΠΠ) κλπ. Εφόσον είναι απαραίτητο, διαβιβάζονται τα στοιχεία σε άλλες εταιρείες, οι οποίες επιτρέπεται να επεξεργάζονται τα δεδομένα με δική τους ευθύνη. Αυτές είναι εταιρείες των ακόλουθων κατηγοριών υπηρεσιών: Εξωτερικοί Ελεγκτές, Συμβουλευτικές Εταιρείες.

3.2.3 Μεταφορά Προσωπικών Δεδομένων σε τρίτες χώρες

Κατ' αρχήν, η επεξεργασία των δεδομένων γίνεται στην Ελλάδα και σε άλλες ευρωπαϊκές χώρες. Κατ' εξαίρεση, η επεξεργασία των δεδομένων σε χώρες εκτός Ευρώπης (Τρίτες Χώρες), γίνεται είτε εφόσον υπάρχει νομική απαίτηση (για παράδειγμα, από τυχόν φορολογική νομοθεσία), είτε εφόσον έχει δοθεί η συγκατάθεσή των υποκείμενων, είτε εφόσον αυτό απαιτείται από τη εργασιακή ή άλλη συμβατική σχέση. Ακόμα και στην περίπτωση που προσωπικά δεδομένα διαβιβαστούν σε Τρίτη Χώρα σύμφωνα με τα ανωτέρω, οι Εταιρείες πληρούν όλους τους όρους της ασφαλούς διαβίβασης με βάση την

ισχύουσα νομοθεσία και διαβιβάζουν τα δεδομένα σε τρίτες χώρες για τις οποίες η Ευρωπαϊκή Επιτροπή έχει αποφασίσει ότι το επίπεδο προστασίας είναι επαρκές (άρθρο 45 GDPR). Εάν η Ευρωπαϊκή Επιτροπή δεν έχει αποφασίσει σχετικά, οι Εταιρείες μεταφέρουν προσωπικά δεδομένα σε τρίτη χώρα μόνο εφόσον εξασφαλίσουν με άλλους τρόπους που προβλέπονται στην ισχύουσα νομοθεσία ότι το επίπεδο προστασίας είναι επαρκές (όπως πχ είναι η υπογραφή των τυποποιημένων συμβατικών ρητρών της Ευρωπαϊκής Επιτροπής, καθώς και με άλλους τρόπους). Για τη μεταφορά δεδομένων εντός του Ομίλου DT, οι Εταιρείες χρησιμοποιούν τους Δεσμευτικούς Κανόνες Προστασίας Προσωπικών Δεδομένων εντός του Ομίλου DT.

3.2.4 Για πόσο χρόνο διατηρούνται τα προσωπικά δεδομένα στις βάσεις δεδομένων του ΟΤΕ;

Ο ΟΤΕ επεξεργάζεται τα προσωπικά δεδομένα για όσο χρόνο είναι απαραίτητο για την εκπλήρωση των συμβατικών και νομικών υποχρεώσεων που προκύπτουν από την εργασιακή ή άλλη συμβατική σχέση. Όταν πλέον το παραπάνω δεν συντρέχει, τα δεδομένα διαγράφονται, εκτός αν υπάρχει λόγος προσωρινής επεξεργασίας για την εκπλήρωση νομικής υποχρέωσης διατήρησης (που προκύπτει για παράδειγμα από φορολογική, ασφαλιστική νομοθεσία, στο πλαίσιο δίκης ή και το ειδικότερο νομικό / ρυθμιστικό πλαίσιο που τυχόν διέπει Οργανωτική λειτουργία (π.χ. για τη διασφάλιση του απορρήτου των επικοινωνιών ή την ακεραιότητα και ασφάλεια των δικτύων). Το διάστημα διατήρησης μπορεί να φτάνει μέχρι τα 40 χρόνια.

3.2.5 Τα δικαιώματά πολιτών σχετικά με την προστασία των δεδομένων τους

- ✓ Δικαίωμα πρόσβασης (το δικαίωμα πρόσβασης αφορά στις κατηγορίες των προσωπικών δεδομένων που επεξεργάζονται οι Εταιρείες, στο σκοπό της επεξεργασίας, στους αποδέκτες των δεδομένων, στη διάρκεια διατήρησης των δεδομένων)
- ✓ Δικαίωμα στη διόρθωση ή στη συμπλήρωση ελλιπών δεδομένων

- ✓ Δικαίωμα ανάκλησης της συγκατάθεσης με ισχύ για το μέλλον
- ✓ Δικαίωμα διαγραφής των δεδομένων, με τις εξής προϋποθέσεις:

• Τα δεδομένα δεν είναι πλέον απαραίτητα για τον επιδιωκόμενο σκοπό ή επεξεργάζονται με μη νόμιμο τρόπο, ή

- Έχει ανακληθεί ν συγκατάθεσή τους (εκτός αν υπάρχει άλλη νομική βάση για την επεξεργασία), ή
- Στην περίπτωση της επεξεργασίας των δεδομένων, στη βάση έννομου συμφέροντος των Εταιρειών, εφόσον οι πολίτες εναντιώνονται στην επεξεργασία και δεν συντρέχει υπέρτερο έννομο συμφέρον για την επεξεργασία, ή
- Τα προσωπικά δεδομένα πρέπει να διαγραφούν σε συμμόρφωση με νομική υποχρέωση
- Δικαίωμα για τον περιορισμό της επεξεργασίας των δεδομένων, όταν συντρέχουν ειδικές συνθήκες και η διαγραφή δεν είναι δυνατή ή η υποχρέωση διαγραφής αμφισβητείται
- Δικαίωμα στη φορητότητα, με τις προϋποθέσεις του άρθρου 20 του GDPR

Δικαίωμα εναντίωσης στην επεξεργασία των προσωπικών δεδομένων, στις περιπτώσεις που ορίζονται στο άρθρο 21 του GDPR, εάν, λόγω ειδικών συνθηκών που συντρέχουν, υπάρχει λόγος παύσης της επεξεργασίας. Στην περίπτωση αυτή, ο ΟΤΕ θα παύσει την επεξεργασία των δεδομένων, εκτός εάν υφίστανται εξαιρετικοί και σημαντικοί λόγοι για τη συνέχιση της επεξεργασίας.

Δικαίωμα υποβολής παραπόνου στην αρμόδια Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στην ηλεκτρονική διεύθυνση complaints@dpa.gr .

3.3 Πρωτογενής Έρευνα: Αποτελέσματα Ερωτηματολογίου

Στα πλαίσια της πρωτογενούς έρευνας και για να κατανοήσουμε περισσότερο τον τρόπο λειτουργίας του GDPR στον Όμιλο ΟΤΕ ζητήσαμε από τους εργαζομένους της Υποδιεύθυνσης Ασφάλειας Προσωπικών Δεδομένων να μας απαντήσουν σε ένα ερωτηματολόγιο προσαρμοσμένο στις λειτουργίες του τμήματος, το οποίο απαντήθηκε από το σύνολο των εργαζομένων.

Σκοπός του ερωτηματολογίου είναι να αναδειχθεί και περαιτέρω αναλυθεί η εφαρμογή του Γενικού Κώδικα Προστασίας Δεδομένων στον τηλεπικοινωνιακό Όμιλο.

Αναλύοντας το προφίλ των ερωτώμενων που συμμετείχαν, προκύπτει ότι από τους 15 εργαζομένους οι 14 είναι υπάλληλοι (93%) και οι 1 προϊστάμενος Τμήματος (7%). Τα συνολικά χρόνια απασχόλησης τους στον ΟΤΕ κυμαίνονται από 2 έως 20 χρόνια, με μέσο όρο τα 10,35 χρόνια, ενώ στην παρούσα θέση το εύρος κυμαίνεται στα 8.5 χρόνια. Όλοι έχουν τις ίδιες αρμοδιότητες και καθήκοντα που είναι να ενημερώνονται συστηματικά και να εφαρμόζουν την νομοθεσία στο σύνολο των υπηρεσιών του Ομίλου. Καθώς επίσης είναι υπεύθυνοι για την εκπαίδευση και των υπολοίπων τμημάτων για την διασφάλιση των προσωπικών δεδομένων των πελατών της. Όσον αφορά την δική τους εκπαίδευση και ενημέρωση γίνεται κάθε 2 έτη.

Οι συνάδελφοι είναι απόφοιτοι πανεπιστημιακής εκπαίδευσης (ΑΕΙ) και οι 7 από αυτούς είναι κάτοχοι μεταπτυχιακών σπουδών. Οι ερωτηθέντες είναι πλήρως καταρτισμένοι και ενημερωμένοι για το τι ορίζει ο νόμος για την εφαρμογή και την υλοποίηση του Γενικού Κώδικα Προστασίας Δεδομένων ώστε να διασφαλίσει την προστασία των προσωπικών δεδομένων των πελατών της.

Στην συνέχεια έχοντας συγκεντρώσει τις απαντήσεις των ερωτηθέντων που αφορούν το πώς εφαρμόζεται και το πώς διαχειρίζεται ο Όμιλος την νομοθεσία περί της Ασφάλειας των Προσωπικών Δεδομένων τόσο για τους πελάτες του αλλά όσο και για τους εργαζόμενους του, παραθέτουμε τις ερωτήσεις αλλά και τις αναλύσεις των απαντήσεων που προέκυψαν.

Παρακαλούμε προσδιορίστε τις μεθόδους που χρησιμοποιείτε για τη συλλογή των δεδομένων προσωπικού χαρακτήρα (επιγραμματικά).

Στην ερώτηση αυτή ζητήθηκε από τους ερωτηθέντες να προσδιορίσουν τις μεθόδους που χρησιμοποιούν ώστε να επιτευχτεί η συλλογή των προσωπικών δεδομένων. Η απάντηση τους στράφηκε σε δύο πυλώνες, στις συμβάσεις πελατών αλλά και στις συμβάσεις των εργαζομένων. Όταν ένας πελάτης εισέρχεται σε ένα κατάστημα του

ομίλου για να επωφεληθεί μία ή και περισσότερες παροχές που μπορεί να του προσφέρει η εταιρεία, κατά την ολοκλήρωση της πώλησης της υπηρεσίας υπογράφεται μία σύμβαση μεταξύ του πελάτη και της εταιρείας που αναγράφεται το είδος της υπηρεσίας που θα δώσουμε στον πελάτη καθώς επίσης και τα προσωπικά στοιχεία του πελάτη. Τα προσωπικά στοιχεία των πελατών αποθηκεύονται σε βάσεις δεδομένων ώστε να μπορεί η εταιρεία ανά πάσα στιγμή να τα επεξεργαστεί και να τα αξιοποιήσει όπως θεωρεί σκόπιμο πάντα σύμφωνα με το νόμο.

Οι συμβάσεις εργασίας από την άλλη μεριά είναι ένας άλλος τρόπος συλλογής προσωπικών δεδομένων. Είναι η συμφωνία μεταξύ της εταιρείας και των εργαζομένων για τους όρους με τους οποίους η εταιρεία προσέλαβε των εργαζόμενο. Και πάλι τα προσωπικά δεδομένα του εργαζόμενου π.χ ΑΜΚΑ, ΑΦΜ κτλ αποθηκεύονται σε βάσεις δεδομένων .

Ποια είναι τα πλεονεκτήματα για την εταιρεία από την εφαρμογή του GDPR.

Κάθε εταιρεία πλέον είναι υποχρεωμένη βάσει νόμου να εφαρμόζει την αρχή προστασίας προσωπικών δεδομένων, μιας και τα δεδομένα είναι το «καύσιμο» της ψηφιακής οικονομίας. Οι ερωτηθέντες καλούνται να μας αναφέρουν τα πλεονεκτήματα που έχει η εταιρεία από την εφαρμογή του GDPR.

Η εφαρμογή του GDPR δίνει το πλεονέκτημα στην εταιρεία να έχει πιο ισχυρή προστασία των δεδομένων της. Η εταιρία μέσω του τμήματος που ασχολείται με την διασφάλιση των προσωπικών δεδομένων εφαρμόζει μεθόδους με τις οποίες θα μπορεί να εξασφαλίσει την προστασία των προσωπικών δεδομένων των εργαζομένων αλλά και των πελατών της. Αυτό είναι πολύ σημαντικό καθώς σε περίπτωση μη συμμόρφωσης με το GDPR, τα πρόστιμα μπορεί να φτάσουν το 4% του παγκόσμιου τζίρου (όταν το αντίστοιχο σημερινό πρόστιμο είναι 150k):

• OTE Group: ~156m

• DT Group: ~2.9billion

Τέλος, η εταιρεία είναι προσανατολισμένη στην εφαρμογή του νόμου για την προστασία των προσωπικών δεδομένων και αυτό ενισχύει την εμπιστοσύνη τόσο των μετόχων όσο και των πελατών της απέναντι στο brand της εταιρείας, το οποίο είναι άλλο ένα πλεονέκτημα από την εφαρμογή του GDPR.

Ποιες είναι οι κατηγορίες των προσωπικών δεδομένων που επεξεργάζονται από τον ΟΤΕ;

Στην ερώτηση αυτή οι εργαζόμενοι ανέφεραν συνοπτικά τις κατηγορίες στις οποίες χωρίζονται τα προς επεξεργασία προσωπικά δεδομένα των πελατών της εταιρίας:

- ✓ Δημογραφικά δεδομένα
  - Όνομα
  - Επώνυμο
  - Διεύθυνση
  - Αριθμός Ταυτότητας

- ✓ Δεδομένα Επικοινωνίας
  - Κλήσεις
  - SMS
  - Δεδομένα Κυψέλης

- ✓ Δεδομένα Συσκευής
  - Μοντέλο Συσκευής
  - IMEI (International Mobile Equipment Identity)

Υπάρχει έγγραφη πολιτική ασφαλείας της επιχείρησης σας για την προστασία των δεδομένων προσωπικού χαρακτήρα; Τι αναφέρει;

Σε αυτή την ερώτηση οι υπάλληλοι του τμήματος για την διασφάλιση των προσωπικών δεδομένων καλούνται να μας αναφέρουν την έγγραφη πολιτική ασφάλειας του ομίλου.
Μας ανέφεραν ότι στην έγγραφη πολιτική ασφαλείας του ομίλου υπάρχουν τα εξής :
Α) Υπάρχουν δεσμευτικοί κανόνες Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Αυτό σημαίνει ότι σύμφωνα με την αρχή προστασίας των προσωπικών δεδομένων είναι συγκεκριμένα τα προσωπικά στοιχεία τα οποία ο όμιλος μπορεί να ζητήσει και υπάρχουν διαδικασίες για την επεξεργασία και διαχείριση των προσωπικών δεδομένων των πελατών αλλά και των εργαζομένων.
Β) Πολιτική Ασφάλειας και ειδικότερη Πολιτική Ασφάλειας για την Διασφάλιση του Απορρήτου των επικοινωνιών. Η προστασία του απορρήτου σε κάθε μορφής επικοινωνία αποτελεί συνταγματικά κατοχυρωμένο δικαίωμα και νόμος ορίζει τις

εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων (άρθρο 19 του Συντάγματος). Στις ηλεκτρονικές επικοινωνίες, σύμφωνα με τη νομοθεσία, απόρρητα θεωρούνται :

• Το περιεχόμενο της επικοινωνίας (περιεχόμενο τηλεφωνικών κλήσεων, ηλεκτρονικού ταχυδρομείου και γενικά οποιασδήποτε επικοινωνίας φωνής, εικόνας, δεδομένων).
• Η ταυτότητα του καλούντος και του καλουμένου.
• Η ταυτότητα του αποστολέα και του παραλήπτη ηλεκτρονικού ταχυδρομείου.
• Τα δεδομένα θέσης της τερματικής συσκευής (γεωγραφικός εντοπισμός).

Η επιχείρησή σας τηρεί συγκεκριμένη διαδικασία όσον αφορά την ασφαλή διαγραφή ή την ηθελημένη καταστροφή προσωπικών δεδομένων; Αν ναι ποια είναι;

Στην ερώτηση αυτή οι εργαζόμενοι εκλήθησαν να απαντήσουν εάν τηρούνται συγκεκριμένες διαδικασίες στην περίπτωση της ασφαλούς διαγραφής και ηθελημένης καταστροφής δεδομένων. Σύμφωνα με τις απαντήσεις τους, οι διαδικασίες που ακολουθούνται είναι οι εξής:

Α) Απομαγνητισμός: Η απλή διαγραφή δεδομένων δεν εξασφαλίζει τη μόνιμη εξαφάνιση κάθε ίχνους αρχείων από τα αποθηκευτικά μέσα καθώς με απλό τρόπο μπορούν τα δεδομένα να επανέλθουν, ειδικά στην περίπτωση των memory cards, των USB και των δίσκων SSD. Έτσι, μέθοδοι όπως ο απομαγνητισμός που εάν εφαρμοστεί με εξειδικευμένο πιστοποιημένο εξοπλισμό, εξασφαλίζει την ολοκληρωτική καταστροφή του μέσου χωρίς δυνατότητα επανάχρησης.

Β) Φυσική καταστροφή : με τη διαδικασία της "Φυσικής Καταστροφής" του μέσου στο οποίο είναι αποθηκευμένα τα προσωπικά δεδομένα , χρησιμοποιούνται ειδικοί σπαστήρες για το καλύτερο δυνατό αποτέλεσμα.

Σε συνέχεια της παραπάνω ερώτησης οι εργαζόμενοι ερωτήθηκαν για τα Τεχνικά και Οργανωτικά μέτρα που λαμβάνει η εταιρεία

Λήψη οργανωτικών μέτρων

• Στον ΟΤΕ έχουμε υιοθετήσει τους εταιρικούς Δεσμευτικούς Κανόνες Προστασίας Δεδομένων (BCRP) και μια σειρά από πολιτικές και διαδικασίες ασφάλειας καθώς και Κανόνες Ορθής συμπεριφοράς Χρηστών

Λήψη τεχνικών μέτρων

• Κρυπτογράφηση

• Καταγραφή ενεργειών που γίνονται σε προσωπικά δεδομένα

• Ψευδωνυμοποίηση:

Είναι μια τεχνική όπου τα αναγνωριστικά αντικαθίστανται από ψευδώνυμες τιμές (π.χ. το όνομα «Παπαδόπουλος»,μετατρέπεται σε «Παναγιωτόπουλος» και παράλληλα διατηρείται σε κάποιο ασφαλές σημείο η αντιστοίχηση της πραγματικής τιμής με την ψευδώνυμη.) Με τη ψευδωνυμοποίηση μπορεί να μειωθεί το ρίσκο και να προστατευθούν τα δεδομένα στις περιπτώσεις που πραγματοποιείται ανάλυση σε μεγάλη κλίμακα (π.χ. BigData)

Σας έχει γίνει εκπαίδευση για την προστασία προσωπικών δεδομένων; Αν ναι κάθε πότε γίνεται ;

Στην ερώτηση αυτή, οι εργαζόμενοι απάντησαν ότι έχουν εκπαιδευτεί για την προστασία των δεδομένων προσωπικού χαρακτήρα και ότι η εκπαίδευση αυτή επαναλαμβάνεται κάθε δύο έτη, ώστε να ενημερώνονται για τις τρέχουσες εξελίξεις, όπως συνέβη και για την νέα εφαρμογή του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων.

Υπάρχει υπεύθυνος Επεξεργασίας (Controller) και Υπεύθυνος Προστασίας Δεδομένων(DPO) και ποιος είναι ο ρόλος τους;

Σύμφωνα με τις απαντήσεις των εργαζομένων, στην εταιρεία έχει οριστεί Υπεύθυνος Προστασίας Δεδομένων (DPO), βάσει των απαιτήσεων του Κανονισμού GDPR. Ο ρόλος του είναι συμβουλευτικός (όχι αποφασιστικός) και δε φέρει προσωπική ευθύνη για τη μη συμμόρφωση με τον Κανονισμό. Υπεύθυνος να διασφαλίζει και να μπορεί να

αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον ΓΚΠΔ είναι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία.

Ο ρόλος του Υπευθύνου Προστασίας Δεδομένων, συνοψίζεται στα εξής:

- ✓ να ενημερώνει και να συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, καθώς και το προσωπικό που απασχολούν, σχετικά με τις υποχρεώσεις τους σύμφωνα με τη νομοθεσία περί προστασίας δεδομένων·
- ✓ να παρακολουθεί τη συμμόρφωση του οργανισμού με το σύνολο της νομοθεσίας που αφορά την προστασία δεδομένων, επίσης κατά τη διάρκεια ελέγχων, δραστηριοτήτων ενημέρωσης και εκπαίδευσης του προσωπικού που συμμετέχει σε πράξεις επεξεργασίας·
- ✓ να λειτουργεί ως σημείο επαφής για αιτήματα φυσικών προσώπων που αφορούν την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα και την άσκηση των δικαιωμάτων τους.

Ο ΥΠΔ δεν πρέπει να λαμβάνει οδηγίες από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία για την άσκηση των καθηκόντων του. Ο ΥΠΔ αναφέρεται απευθείας στο υψηλότερο επίπεδο διοίκησης του οργανισμού.

Υπεύθυνος επεξεργασίας (Controller) είναι η υπηρεσία, ο φορέας, η δημόσια αρχή το φυσικό ή νομικό πρόσωπο που καθορίζουν τους σκοπούς και τον τρόπο επεξεργασίας δεδομένων προσωπικού χαρακτήρα (π.χ. η COSMOTE είναι υπεύθυνος επεξεργασίας των πελατών της και επεξεργάζεται προσωπικά δεδομένα για τη παροχή αυτής της υπηρεσία

Με ποιους συνεργάτες σας έχετε υπογράψει συμβάσεις εμπιστευτικότητας και εχεμύθειας π.χ. Συμφωνητικό Επεξεργασίας Δεδομένων και σε τι αναφέρεται αυτό;

Στην ερώτηση αυτή, οι εργαζόμενοι απάντησαν ότι η εταιρεία έχει υπογράψει Συμφωνητικό Επεξεργασίας Δεδομένων με προμηθευτές κι εξωτερικούς συνεργάτες της εταιρείας.

Τι είναι το Συμφωνητικό Επεξεργασίας Δεδομένων(Data Processing Agreement) που υπογράφετε με τους εξωτερικούς συνεργάτες και τους προμηθευτές ;

Το συμφωνητικό ανάθεσης επεξεργασίας προσωπικών δεδομένων (CDPA) απαιτείται σε περιπτώσεις όπου το αντικείμενο της σύμβασης περιλαμβάνει την επεξεργασία προσωπικών δεδομένων και η υπογραφή του είναι αναγκαία για τη συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (General Data Protection Regulation - GDPR).

"Ως επεξεργασία νοείται κάθε εργασία που πραγματοποιείται σε προσωπικά δεδομένα, όπως για παράδειγμα η συλλογή, η καταχώριση, η αποθήκευση, η εξαγωγή, η χρήση, η διαβίβαση, η διαγραφή, ή η καταστροφή".

Οι περιπτώσεις που απαιτείται CDPA είναι:

Όταν εταιρεία του Ομίλου ΟΤΕ λειτουργεί ως υπεύθυνος επεξεργασίας (Controller)

Όταν εταιρεία του Ομίλου ΟΤΕ λειτουργεί ως εκτελών την επεξεργασία (Processor)

Στις περιπτώσεις όπου ανατίθεται η επεξεργασία δεδομένων σε συνεργάτη (processor) ή πραγματοποιούμε επεξεργασία για λογαριασμό άλλου (π.χ. ICT projects), απαιτείται η υπογραφή συμφωνητικού επεξεργασίας δεδομένων, στο οποίο ορίζονται:

• Κατηγορίες δεδομένων
• Σκοπός επεξεργασίας
• Αποδέκτες
• Τεχνικά & Οργανωτικά μέτρα που λαμβάνει ο συνεργάτης ή η εταιρεία

Παρακαλώ περιγράψτε συνοπτικά τα βήματα ασφαλείας που ακολουθούνται από τους εργαζόμενους σε περίπτωση που αποκτούν πρόσβαση σε προσωπικά δεδομένα.

Τα βήματα που ακολουθούνται όταν οι εργαζόμενοι της εταιρίας έχουν πρόσβαση σε προσωπικά δεδομένα πελατών αποκλειστικά για επιχειρησιακούς λόγους είναι τα εξής:

• Χρησιμοποιούν τον προσωπικό τους λογαριασμό πρόσβασης
• Χρησιμοποιούν ισχυρούς κωδικούς πρόσβασης και δεν τους μοιράζονται
• Χρησιμοποιούν το KeePass για την αποθήκευση των κωδικών πρόσβασης.

ΚΕΦΑΛΑΙΟ 4

ΣΥΖΗΤΗΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

4.1 Σκοπός και Οφέλη Εφαρμογής του GDPR

Η παρούσα έρευνα που πραγματοποιήθηκε στην υποδιεύθυνση Ασφάλειας και Προσωπικών Δεδομένων και είχε ως σκοπό να αναδείξει την σημαντικότητα της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) στον τομέα των Τηλεπικοινωνιών στις διαδικασίες ώστε να εξασφαλιστεί το απόρρητο των επικοινωνιών που αφορούν τόσο σε σχέση με τους πολίτες, το προσωπικό και τους προμηθευτές όσο και τις τεχνολογικές και οργανωτικές βελτιώσεις που θα πρέπει να εφαρμοστούν .

Ο ΟΤΕ χρησιμοποιεί καθημερινά πολλές ηλεκτρονικές εφαρμογές οι οποίες διαχειρίζονται προσωπικά δεδομένα είτε των συνδρομητών είτε των εργαζομένων. Ωστόσο ποικίλουν ανάλογα με την υπηρεσία, το αντικείμενο και τις ανάγκες.

Όσων αφορά πραγματοποίηση επιμορφωτικών σεμιναρίων για την εκπαίδευση του συνόλου του προσωπικού σε νέες διαδικασίες, όλοι απάντησαν ότι αυτά γίνονται περίπου μία φορά το χρόνο με την μορφή e learning.

Η χρήση των ηλεκτρονικών εφαρμογών και διαδικασιών έχει αντικαταστήσει σε μεγάλο βαθμό στη μείωση και στην αντιμετώπιση των πιθανών σφαλμάτων, συμβάλλοντας περαιτέρω στη βελτίωση των παρεχόμενων υπηρεσιών. Καθώς επίσης και στην διασφάλιση της ασφάλειας των προσωπικών δεδομένων.

Τα κυριότερα πλεονεκτήματα των νέων διαδικασιών είναι η διευκόλυνση πρόσβασης στα δεδομένα, η ασφάλεια που παρέχεται για την διασφάλιση των προσωπικών

δεδομένων με την σωστή χρήση και την εφαρμογή κανόνων ασφαλείας από τον χρήστη καθώς και η άμεση και αποτελεσματική αντιμετώπιση πιθανών σφαλμάτων.

Στο πλαίσιο αυτό, λοιπόν, καθίσταται σαφές ότι τα οφέλη της χρήσης των τεχνολογικών εφαρμογών σε συνδυασμό με το νομοθετικό πλαίσιο που είναι υποχρεωμένος κάθε οργανισμός να ακολουθεί είναι σημαντικά για την ομαλή του λειτουργία. Οι πολίτες είναι δυνατόν να εξυπηρετούνται έγκαιρα σε ό, τι ζήτημα προκύπτει και μάλιστα με ασφάλεια. Το γεγονός αυτό συμβάλλει σημαντικά στη μείωση των γραφειοκρατικών μεθόδων και κατ' επέκταση στην αύξηση της ασφάλειας του απορρήτου των προσωπικών δεδομένων τόσο των πολιτών όσο και των εργαζομένων.

4.2 Αποτελέσματα Έρευνας

Τα αποτελέσματα που προέκυψαν έπειτα από την συλλογή των απαντήσεων του ερωτηματολογίου δείχνουν το πόσο σημαντικό είναι η εφαρμογή της νομοθεσίας του Γενικού Κανονισμού Προστασίας Δεδομένων στην λειτουργία του ΟΤΕ και πόσο έχει συμμορφωθεί στις νέες διαδικασίες ώστε να διασφαλίσει την ασφάλεια των προσωπικών δεδομένων του προσωπικού, των πελατών αλλά και των προμηθευτών. Με την εφαρμογή του ΓΚΠΚ μπορεί να επέμβει άμεσα και με διασφάλιση του απορρήτου σε οποιαδήποτε απαίτηση του πελάτη είτε αυτή είναι η τροποποίηση και η επεξεργασία προσωπικών δεδομένων είτε η διασφάλιση της τεχνολογικής του υποδομής.

Κεφάλαιο 5

Συμπεράσματα-Προτάσεις

5.1 Συμπεράσματα Έρευνας

Παρατηρούμε ότι η αλματώδης εξέλιξη στον τομέα της Τεχνολογίας και των Επικοινωνιών προάγει τη διευκόλυνση της εξυπηρέτησης και των συναλλαγών των πολιτών, δημιουργεί όμως ταυτόχρονα και «γκρίζες ζώνες», όσον αφορά την προστασία των ευαίσθητων προσωπικών δεδομένων τους. Έχει δημιουργηθεί λοιπόν σε ευρωπαϊκό επίπεδο ένα ισχυρό ρυθμιστικό και νομοθετικό πλαίσιο, έτσι ώστε να αντιμετωπιστούν οι οποιοσδήποτε προκλήσεις παρουσιάζονται στο πεδίο της Ασφάλειας και Προστασίας προσωπικών δεδομένων.

Στόχος της παρούσας διπλωματικής εργασίας ήταν η διερεύνηση της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και της Ασφάλειας Προσωπικών Δεδομένων σε τομείς της Ηλεκτρονικής Διακυβέρνησης, και πιο συγκεκριμένα στον τομέα των Τηλεπικοινωνιών. Δια μέσου της παρουσίασης των πιο σημαντικών εννοιών σχετικών με τα ανωτέρω θέματα, δίδεται στον αναγνώστη μια πιο πλήρης εικόνα όσον αφορά την τρέχουσα κατάσταση αλλά και τις προκλήσεις που καλούνται να αντιμετωπίσουν οι αντίστοιχοι φορείς.

Έτσι, μέσω της πρωτογενούς αλλά και δευτερογενούς έρευνας που πραγματοποιήθηκε παρατηρούμε ότι οι βασικές συνέπειες από την εφαρμογή του GDPR στον τομέα των Τηλεπικοινωνιών και συγκεκριμένα στον ΟΤΕ, αφορούν τόσο τις σχέσεις του με τους πολίτες, το προσωπικό και τους προμηθευτές όσο και τις τεχνολογικές βελτιώσεις και τις οργανωτικές αλλαγές που πρέπει να εφαρμοστούν.

Οι τροποποιήσεις που επέφερε ο GDPR στον τομέα των Τηλεπικοινωνιών και ιδιαίτερα στον ΟΤΕ αφορούν:

- ✓ Στην επεξεργασία δεδομένων: χρειάζεται το αντίστοιχο πληροφοριακό σύστημα διαχείρισης που αφορά στη δυνατότητα τροποποίησης και διόρθωσης των προσωπικών δεδομένων μετά από απαίτηση του υποκειμένου, στη συναίνεση, στη δυνατότητα φορητότητας των δεδομένων και στην ασφαλή διαγραφή.
- ✓ Στην τεχνολογική υποδομή: Κρυπτογράφηση ή ψευδωνυμοποίηση, κατάλογος περιοχών που περιλαμβάνουν προσωπικά δεδομένα, πληροφοριακό σύστημα επεξεργασίας και αποθήκευσης των metadata.

- ✓ Στη δομή και την οργάνωση: τροποποιήσεις στο χειρισμό των δεδομένων, ορισμός Υπεύθυνου Προστασίας προσωπικών Δεδομένων, καινούριες πολιτικές Ασφάλειας ή τροποποιήσεις και αναβαθμίσεις στις υφιστάμενες, αναθεώρηση του πρωτοκόλλου και του οργανικού κώδικα δεοντολογίας.

Με τη συμβολή του GDPR οι φορείς Τηλεπικοινωνιών και συγκεκριμένα ο ΟΤΕ ,έχουν τη δυνατότητα να ανταποκριθούν πιο γρήγορα και ευέλικτα στις παρακάτω απαιτήσεις των πολιτών:

- ✓ Το δικαίωμα της φορητότητα των δεδομένων
- ✓ Τη διεκπεραίωση μιας παραβίασης των προσωπικών δεδομένων των πολιτών. Η διεκπεραίωση μπορεί να περιλαμβάνει τον προσδιορισμό του μεγέθους και της φύσης των δεδομένων που διέρρευσαν , έγκαιρες ενέργειες για την αποτροπή της παραβίασης καθώς και άμεση ενημέρωση των Αρχών και των υποκειμένων των δεδομένων.

Συμπεραίνουμε λοιπόν, ότι ο ΟΤΕ ως κύριος φορέας Τηλεπικοινωνιών σε εθνικό επίπεδο, έχει συμμορφωθεί και προσαρμοστεί πλήρως με την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων κι αυτό αντικατοπτρίζει πλήρως την οργανωτική ωριμότητα καθώς και την υπεύθυνη στάση του απέναντι στην μακροημέρευση της Κοινωνίας της Πληροφορίας. Σε αυτό συνέβαλε πλήρως η απόλυτη και συνεχής στήριξη της εφαρμογής

του ΓΚΠΚ από τις Διοικητικές Αρχές του ΟΤΕ, ενισχύοντας τη διαδικασία μέσω του ανασχεδιασμού των Πολιτικών Ασφαλείας και τη συνεχή επιμόρφωση του ανθρώπινου δυναμικού πάνω σε θέματα που αφορούν την προστασία των Προσωπικών Δεδομένων των πολιτών

5.2 Περιορισμοί Έρευνας

Κατά την διάρκεια της έρευνας παρουσιάστηκαν κάποιες δυσκολίες στην διεξαγωγή της και αυτές είχαν να κάνουν με τον χρόνο και με τον περιορισμό του δείγματος των ερωτηματολογίων.

Η Υποδιεύθυνση την περίοδο που εστάλησαν τα ερωτηματολόγια, λόγω ενός εσωτερικού event, ήταν πολύ πιεσμένοι με μεγάλο φόρτο εργασίας και με την διαδικασία του event καθώς βραβεύτηκαν για την συνεισφορά τους και την πολύτιμη βοήθεια τους στο Όμιλο για την διασφάλιση των Προσωπικών Δεδομένων.

Επίσης μπορεί το δείγμα είναι λίγο περιορισμένο όμως στην συγκεκριμένη περίπτωση είναι πλήρως ικανοποιητικό καθώς οι συνάδελφοι είναι έμπειροι και πλήρως εκπαιδευμένοι και ενημερωμένοι στο αντικείμενο της εργασίας τους.

5.3 Προτάσεις - Εκπαίδευση προσωπικού

Για την ορθή λειτουργία του τμήματος θα πρέπει οι εργαζόμενοι να είναι, όπως είπαμε και πιο πάνω, πλήρως ενημερωμένοι με τις διατάξεις του νόμου και με τυχόν νέες προσθήκες, διορθώσεις της νομοθεσίας. Επιπλέον οι εργαζόμενοι του τμήματος είναι υπεύθυνοι στο να γίνεται έλεγχος στο σύνολο των υπηρεσιών του Ομίλου ώστε να διαπιστώσουν ότι τηρούνται οι διαδικασίες.

Για τον έλεγχο των διαδικασιών ο Όμιλος έχει ορίσει Υπεύθυνο Προστασίας Δεδομένων (DPO) ο ρόλος του οποίου είναι να κάνει εντατικούς ελέγχους στο σύνολο των διαδικασιών του Ομίλου. Σε αυτό το σημείο θα μπορούσαμε να προτείνουμε οι έλεγχοι αυτοί να είναι πιο εντατικοί και σχολαστικοί καθώς οι εισροή των δεδομένων είναι σε τεράστιο βαθμό και θα πρέπει για να διατηρήσει ακέραιο το προφίλ του ο Όμιλος θα πρέπει να εφαρμόζει την νομοθεσία στο ακέραιο.

Τέλος θα πρέπει να γίνει μία μεγαλύτερη προσπάθεια για την εκπαίδευση των υπολοίπων εργαζομένων καθώς επίσης και ενημέρωση για την σημαντικότητα της εφαρμογής του GDPR με κάποια e-learning ή ακόμα και με ημερίδες.

5.4 Μελλοντικές Προτάσεις

Καθώς ο Γενικός Κανονισμός Προστασίας Δεδομένων έχει μπει πρόσφατα σε ισχύ, ανοίγεται ένα ευρύ πεδίο μελέτης της εφαρμογής του. Από εδώ και στο εξής αξίζει να διερευνηθούν πλήρως τόσο τα πλεονεκτήματα της εφαρμογής του σε όλους τους τομείς της Ηλεκτρονικής Διακυβέρνησης καθώς και οι περιορισμοί που προκύπτουν αλλά και πιθανοί τρόποι ώστε να ξεπεραστούν αποτελεσματικά. Η εξέλιξη και η πρόοδος της Τεχνολογίας πρέπει να αποτελεί αναπόσπαστο εφόδιο στη διευκόλυνση της καθημερινότητας των πολιτών της Κοινωνίας της Πληροφορίας και το να ξεπεραστούν οι πιθανοί κίνδυνοι που προκύπτουν αποτελεί στόχο για κάθε σύγχρονη κοινωνία.

Παράρτημα Α

Γλωσσάρι Βασικών Εννοιών του GDPR

Υποκείμενο των δεδομένων

«Το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή η μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιοριστεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική».
Παραδείγματα ενός υποκειμένου δεδομένων μπορούν να είναι ένα πρόσωπο, ένας πελάτης, ένας δυνητικός πελάτης, ένας υπάλληλος, ένας αρμόδιος κτλ.

Άρθρο 2(α) Οδηγίας (ΕΚ) 95/46

Άρθρο 2(α) Κανονισμού (ΕΚ) 45/2001

Άρθρο 4 παρ. 1 Γενικού Κανονισμού Προστασίας Δεδομένων

Άρθρο 3 παρ. 1 Οδηγίας (ΕΕ) 2016/680

Άρθρο 2(γ) Ν. 2472/1997

Επιχείρηση

«Φυσικό ή νομικό πρόσωπο που ασκεί οικονομική δραστηριότητα, ανεξάρτητα από τη νομική του μορφή, περιλαμβανομένων των προσωπικών εταιρειών ή των ενώσεων που ασκούν τακτικά οικονομική δραστηριότητα».

Άρθρο 4 παρ. 18 Γενικού Κανονισμού Προστασίας Δεδομένων

Όμιλος επιχειρήσεων

«Μία ελέγχουσα επιχείρηση και οι ελεγχόμενες από αυτήν επιχειρήσεις».

Άρθρο 4 παρ. 19 Γενικού Κανονισμού Προστασίας Δεδομένων

Δεσμευτικοί εταιρικοί κανόνες

«Οι πολιτικές προστασίας δεδομένων προσωπικού χαρακτήρα τις οποίες ακολουθεί ένας υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία εγκατεστημένος στο έδαφος κράτους μέλους για διαβιβάσεις η δέσμη διαβιβάσεων δεδομένων προσωπικού χαρακτήρα σε υπεύθυνο επεξεργασίας ή εκτελούνται την επεξεργασία σε μία ή περισσότερες τρίτες χώρες εντός ομίλου επιχειρήσεων, ή ομίλου εταιρειών που ασκεί κοινή οικονομική δραστηριότητα».

Άρθρο 4 παρ. 20 Γενικού Κανονισμού Προστασίας Δεδομένων

Δεδομένα προσωπικού χαρακτήρα

«Κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή η μπορεί να εξακριβωθεί» Άρθρο 2(α) Οδηγίας (ΕΚ) 95/46

Άρθρο 2(α) Κανονισμού (ΕΚ) 45/2001

Άρθρο 4 παρ. 1 Γενικού Κανονισμού Προστασίας Δεδομένων

Άρθρο 3 παρ. 1 Οδηγίας (ΕΕ) 2016/680

Άρθρο 2(α) Ν. 2472/1997

Ευαίσθητα δεδομένα

«Τα δεδομένα που αφορούν στη φυλετική η εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων».

Άρθρο 2 (β)Ν. 2472 / 1997

Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα

«Η φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, οι θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή η συμμετοχή σε συνδικαλιστική οργάνωση, τα βιομετρικά και γενετικά δεδομένα όταν υποβάλλονται σε επεξεργασία με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένα που αφορούν την υγεία ή δεδομένα που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή το γενετήσιο προσανατολισμό». Άρθρο 9 παρ. 1 Γενικού Κανονισμού Προστασίας Δεδομένων

Άρθρο 10 παρ.1 Οδηγίας (ΕΕ) 2016/680

Αρχεία των δραστηριοτήτων επεξεργασίας

«Κάθε υπεύθυνος επεξεργασίας και, κατά περίπτωση, ο εκπρόσωπος του, τηρεί αρχείο των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνος». Άρθρο 35 Γενικού Κανονισμού Προστασίας Δεδομένων

Άρθρο 27 Οδηγίας (ΕΕ) 2016/680

Εκτίμηση αντίκτυπου σχετικά με την προστασία δεδομένων

«Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους».

Άρθρο 35 Γενικού Κανονισμού Προστασίας Δεδομένων

Άρθρο 27 Οδηγίας (ΕΕ) 2016/680

Υπεύθυνος επεξεργασίας

«Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα η από κοινού με άλλα καθορίζουν τους σκοπούς και τον τρόπο επεξεργασίας δεδομένων προσωπικού χαρακτήρα όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους».

Άρθρο 2(δ) Οδηγίας (ΕΚ) 95/46

Άρθρο 2(δ) Κανονισμού (ΕΚ) 45/2001

Άρθρο 4 παρ. 7 Γενικού Κανονισμού Προστασίας Δεδομένων

Άρθρο 3 παρ. 8 Οδηγίας (ΕΕ) 2016/680

Άρθρο 2(ζ) Ν. 2472/1997

Εκτελών την επεξεργασία

«Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας» Άρθρο 2(ε) Οδηγίας (ΕΚ) 95/46

Άρθρο 2(ε) Κανονισμού (ΕΚ) 45/2001

Άρθρο 4 παρ. 8 Γενικού Κανονισμού Προστασίας Δεδομένων

Άρθρο 3 παρ. 9 Οδηγίας (ΕΕ) 2016/680

Άρθρο 2(θ) Ν. 2472/1997

Τρίτος

«Οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπευθύνο επεξεργασίας, των εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα του προσωπικού χαρακτήρα»

Άρθρο 2(στ) Οδηγίας (ΕΚ) 95/46

Άρθρο 2(στ) Κανονισμού (ΕΚ) 45/2001

Άρθρο 4 παρ. 10 Γενικού Κανονισμού Προστασίας Δεδομένων

Άρθρο 2(θ) Ν. 2472/1997

Αρχείο δεδομένων προσωπικού χαρακτήρα ή σύστημα αρχειοθέτησης

«Κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική η γεωγραφική βάση» Άρθρο 2(γ) Οδηγίας (ΕΚ) 95/46

Άρθρο 2(γ) Κανονισμού (ΕΚ) 45/2001

Άρθρο 4 παρ. 6 Γενικού Κανονισμού Προστασίας Δεδομένων

Άρθρο 3 παρ. 6 Οδηγίας (ΕΕ) 2016/680

Άρθρο 2(ε) Ν. 2472/1997

Συγκατάθεση

«Κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και πλήρει επιγνώσει με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή σαφή θετική ενέργεια να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που τον αφορούν»

Άρθρο 2(η) Οδηγίας (ΕΚ) 95/46

Άρθρο 2(η) Κανονισμού (ΕΚ) 45/2001

Άρθρο 4 παρ. 11 Γενικού Κανονισμού Προστασίας Δεδομένων

Άρθρο 2(ια) Ν. 2472/1997

Κατάρτιση προφίλ

«Οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου»

Άρθρο 4 παρ. 4 Γενικού Κανονισμού Προστασίας Δεδομένων

Άρθρο 3 παρ. 4 Οδηγίας (ΕΕ) 2016/680

Ψευδωνυμοποίηση

«Η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο η ταυτοποιήσιμο φυσικό πρόσωπο».

Άρθρο 4 παρ. 5 Γενικού Κανονισμού Προστασίας Δεδομένων

Άρθρο 3 παρ. 5 Οδηγίας (ΕΕ) 2016/680

Παραβίαση δεδομένων προσωπικού χαρακτήρα

«Η παραβίαση της ασφάλειας που οδήγησε τυχαία η παράνομη καταστροφή, απώλεια, μεταβολή, άνευ αδείας κοινολόγηση η πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν υποβλήθηκαν κατ άλλο τρόπο σε επεξεργασία».

Άρθρο 4 παρ. 12 Γενικού Κανονισμού Προστασίας Δεδομένων

Άρθρο 3 παρ. 11 Οδηγίας (ΕΕ) 2016/680

Άρθρο 2 αρ. 8 της οδηγίας (ΕΚ)
2002 / 58

Παράρτημα Β

Νομοθεσία & Άλλες Διοικητικές Πράξεις

ΚΑΝΟΝΙΣΜΌΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΎ ΚΟΙΝΟΒΟΥΛΊΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΊΟΥ

της 27ης Απριλίου 2016

για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 16,

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Μετά από διαβίβαση του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής ,

Έχοντας υπόψη τη γνώμη της Επιτροπής των Περιφερειών ,

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία ,

Εκτιμώντας τα ακόλουθα:

- Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα θα πρέπει να προορίζεται να εξυπηρετεί τον άνθρωπο. Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα δεν είναι απόλυτο δικαίωμα· πρέπει να εκτιμάται σε σχέση με τη λειτουργία του στην κοινωνία και να σταθμίζεται με άλλα θεμελιώδη δικαιώματα, σύμφωνα με την αρχή της αναλογικότητας. Ο παρών κανονισμός σέβεται όλα τα θεμελιώδη δικαιώματα και τηρεί τις ελευθερίες και αρχές που αναγνωρίζονται στον Χάρτη όπως κατοχυρώνονται στις Συνθήκες, ιδίως τον σεβασμό της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και των

επικοινωνιών, την προστασία των δεδομένων προσωπικού χαρακτήρα, την ελευθερία σκέψης, συνείδησης και θρησκείας, την ελευθερία έκφρασης και πληροφόρησης, την επιχειρηματική ελευθερία, το δικαίωμα πραγματικής προσφυγής και αμερόληπτου δικαστηρίου και την πολιτιστική, θρησκευτική και γλωσσική πολυμορφία.

- Η προστασία που παρέχει ο παρών κανονισμός θα πρέπει να ισχύει για τα φυσικά πρόσωπα, ανεξαρτήτως ιθαγένειας ή τόπου διαμονής, σε σχέση με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα τους. Ο παρών κανονισμός δεν καλύπτει την επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν νομικά πρόσωπα και ιδίως επιχειρήσεις συσταθείσες ως νομικά πρόσωπα, περιλαμβανομένων της επωνυμίας, του τύπου και των στοιχείων επικοινωνίας του νομικού προσώπου.
- Για να διασφαλιστεί ότι τα φυσικά πρόσωπα δεν στερούνται την προστασία που δικαιούνται βάσει του παρόντος κανονισμού, η επεξεργασία των δεδομένων προσωπικού χαρακτήρα υποκειμένων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση θα πρέπει να διέπεται από τον παρόντα κανονισμό, εφόσον οι δραστηριότητες επεξεργασίας σχετίζονται με την παροχή αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων, ανεξάρτητα από το εάν συνδέονται με πληρωμή. Για να κριθεί εάν ένας τέτοιος υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία προσφέρει αγαθά ή υπηρεσίες σε υποκείμενα των δεδομένων που βρίσκονται στην Ένωση, θα πρέπει να εξακριβωθεί αν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία προδήλως αποσκοπεί να παράσχει υπηρεσίες στα υποκείμενα των δεδομένων σε ένα ή περισσότερα κράτη μέλη της Ένωσης. Ενώ η απλή προσβασιμότητα στην ιστοσελίδα του υπευθύνου επεξεργασίας, του εκτελούντος την επεξεργασία ή ενός μεσάζοντος στην Ένωση ή στη διεύθυνση ηλεκτρονικού ταχυδρομείου και σε άλλα στοιχεία επικοινωνίας ή η χρήση γλώσσας που χρησιμοποιείται συνήθως στην τρίτη χώρα όπου ο υπεύθυνος επεξεργασίας είναι εγκατεστημένος δεν αρκεί για να τεκμηριωθεί τέτοια πρόθεση, παράγοντες όπως η χρήση γλώσσας ή νομίσματος που χρησιμοποιούνται συνήθως σε ένα ή περισσότερα κράτη μέλη, με δυνατότητα παραγγελίας προϊόντων και υπηρεσιών σε αυτήν την άλλη γλώσσα, ή η αναφορά σε πελάτες ή χρήστες που βρίσκονται στην Ένωση μπορούν να καταστήσουν πρόδηλο ότι ο

υπεύθυνος επεξεργασίας προτίθεται να προσφέρει αγαθά ή υπηρεσίες σε υποκείμενα των δεδομένων στην Ένωση.

- Η επεξεργασία δεδομένων προσωπικού χαρακτήρα, στον βαθμό που είναι αυστηρά αναγκαία και ανάλογη για τους σκοπούς της διασφάλισης της ασφάλειας δικτύων και πληροφοριών, δηλαδή της ικανότητας ενός δικτύου ή ενός συστήματος πληροφοριών να ανθίσταται, σε ένα δεδομένο επίπεδο εμπιστοσύνης, σε τυχαία γεγονότα ή παράνομες ή κακόβουλες ενέργειες οι οποίες θέτουν σε κίνδυνο τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα αποθηκευμένων ή διαβιβαζόμενων δεδομένων προσωπικού χαρακτήρα, καθώς και της ασφάλειας των σχετικών υπηρεσιών που προσφέρουν τα εν λόγω δίκτυα και συστήματα ή που είναι προσπελάσιμες μέσω των εν λόγω δικτύων και συστημάτων, ή που προσφέρονται από δημόσιες αρχές, από ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT), από ομάδες παρέμβασης για συμβάντα που αφορούν την ασφάλεια των υπολογιστών (CSIRT), από παρόχους δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών και από παρόχους τεχνολογιών και υπηρεσιών ασφάλειας, αποτελεί έννομο συμφέρον του ενδιαφερόμενου υπευθύνου επεξεργασίας δεδομένων. Αυτό θα μπορούσε να περιλαμβάνει, λόγου χάρη, την αποτροπή ανεξουσιοδότητης πρόσβασης σε δίκτυα ηλεκτρονικών επικοινωνιών και διανομής κακόβουλων κωδικών και την παύση επιθέσεων «άρνησης υπηρεσίας» και ζημιών σε συστήματα πληροφορικής και ηλεκτρονικών επικοινωνιών.
- Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς θα πρέπει να υπόκειται σε κατάλληλες εγγυήσεις για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων σύμφωνα με τον παρόντα κανονισμό. Οι εν λόγω εγγυήσεις θα πρέπει να διασφαλίζουν ότι έχουν θεσπιστεί τα τεχνικά και οργανωτικά μέτρα που εγγυώνται, ειδικότερα, την αρχή της ελαχιστοποίησης των δεδομένων. Η περαιτέρω επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς πραγματοποιείται όταν ο υπεύθυνος της επεξεργασίας έχει εκτιμήσει κατά πόσο είναι εφικτό να εκπληρωθούν οι σκοποί αυτοί μέσω της επεξεργασίας δεδομένων τα οποία δεν επιτρέπουν ή δεν επιτρέπουν πλέον την ταυτοποίηση των

υποκειμένων των δεδομένων, υπό την προϋπόθεση ότι υπάρχουν κατάλληλες εγγυήσεις (όπως, για παράδειγμα, η ψευδωνυμοποίηση των δεδομένων). Τα κράτη μέλη θα πρέπει να προβλέπουν κατάλληλες διασφαλίσεις σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς. Θα πρέπει να επιτρέπεται στα κράτη μέλη να παρέχουν, υπό συγκεκριμένες προϋποθέσεις και με δέουσες εγγυήσεις για τα υποκείμενα των δεδομένων, προδιαγραφές και παρεκκλίσεις όσον αφορά τις απαιτήσεις πληροφόρησης και τα δικαιώματα διόρθωσης και διαγραφής, το δικαίωμα στη λήθη, το δικαίωμα περιορισμού της επεξεργασίας,το δικαίωμα στη φορητότητα των δεδομένων και το δικαίωμα αντίταξης κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς. Οι εν λόγω προϋποθέσεις και εγγυήσεις ενδέχεται να συνεπάγονται ειδικές διαδικασίες, ώστε τα υποκείμενα των δεδομένων να ασκούν τα δικαιώματα αυτά, εφόσον είναι σκόπιμο για τους σκοπούς που επιδιώκονται με τη συγκεκριμένη επεξεργασία, παράλληλα με τεχνικά και οργανωτικά μέτρα που αποσκοπούν στην ελαχιστοποίηση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα σύμφωνα με τις αρχές της αναλογικότητας και της αναγκαιότητας. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για επιστημονικούς σκοπούς θα πρέπει να συμμορφώνεται επίσης με άλλες σχετικές νομοθεσίες, όπως αυτή για τις κλινικές δοκιμές.

Άρθρο 12

Διαφανής ενημέρωση, ανακοίνωση και ρυθμίσεις για την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων

1. Ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία που αναφέρεται στα άρθρα 13 και 14 και κάθε ανακοίνωση στο πλαίσιο των άρθρων 15 έως 22 και του άρθρου 34 σχετικά με την επεξεργασία σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία

απευθυνόμενη ειδικά σε παιδιά. Οι πληροφορίες παρέχονται γραπτώς ή με άλλα μέσα, μεταξύ άλλων, εφόσον ενδείκνυται, ηλεκτρονικώς. Όταν ζητείται από το υποκείμενο των δεδομένων, οι πληροφορίες μπορούν να δίνονται προφορικά, υπό την προϋπόθεση ότι η ταυτότητα του υποκειμένου των δεδομένων είναι αποδεδειγμένη με άλλα μέσα.

2. Ο υπεύθυνος επεξεργασίας διευκολύνει την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων που προβλέπονται στα άρθρα 15 έως 22. Στις περιπτώσεις που προβλέπονται στο άρθρο 11 παράγραφος 2, ο υπεύθυνος επεξεργασίας δεν αρνείται να ενεργήσει κατόπιν αιτήσεως του υποκειμένου των δεδομένων για να ασκήσει τα δικαιώματά του βάσει των άρθρων 15 έως 22, εκτός αν ο υπεύθυνος επεξεργασίας αποδείξει ότι δεν είναι σε θέση να εξακριβώσει την ταυτότητα του υποκειμένου των δεδομένων.

3. Ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων πληροφορίες για την ενέργεια που πραγματοποιείται κατόπιν αιτήματος δυνάμει των άρθρων 15 έως 22 χωρίς καθυστέρηση και σε κάθε περίπτωση εντός μηνός από την παραλαβή του αιτήματος. Η εν λόγω προθεσμία μπορεί να παραταθεί κατά δύο ακόμη μήνες, εφόσον απαιτείται, λαμβανομένων υπόψη της πολυπλοκότητας του αιτήματος και του αριθμού των αιτημάτων. Ο υπεύθυνος επεξεργασίας ενημερώνει το υποκείμενο των δεδομένων για την εν λόγω παράταση εντός μηνός από την παραλαβή του αιτήματος, καθώς και για τους λόγους της καθυστέρησης. Εάν το υποκείμενο των δεδομένων υποβάλλει το αίτημα με ηλεκτρονικά μέσα, η ενημέρωση παρέχεται, εάν είναι δυνατόν, με ηλεκτρονικά μέσα, εκτός εάν το υποκείμενο των δεδομένων ζητήσει κάτι διαφορετικό.

4. Εάν ο υπεύθυνος επεξεργασίας δεν ενεργήσει επί του αιτήματος του υποκειμένου των δεδομένων, ο υπεύθυνος επεξεργασίας ενημερώνει το υποκείμενο των δεδομένων, χωρίς καθυστέρηση και το αργότερο εντός μηνός από την παραλαβή του αιτήματος, για τους λόγους για τους οποίους δεν ενήργησε και για τη δυνατότητα υποβολής καταγγελίας σε εποπτική αρχή και άσκησης δικαστικής προσφυγής.

5. Οι πληροφορίες που παρέχονται σύμφωνα με τα άρθρα 13 και 14 και κάθε ανακοίνωση καθώς και όλες οι ενέργειες που αναλαμβάνονται σύμφωνα με τα άρθρα 15 έως 22 και το άρθρο 34 παρέχονται δωρεάν. Εάν τα αιτήματα του υποκειμένου των δεδομένων είναι προδήλως αβάσιμα ή υπερβολικά, ιδίως λόγω του επαναλαμβανόμενου χαρακτήρα τους, ο υπεύθυνος επεξεργασίας μπορεί είτε:

α) να επιβάλει την καταβολή εύλογου τέλους, λαμβάνοντας υπόψη τα διοικητικά έξοδα για την παροχή της ενημέρωσης ή την ανακοίνωση ή την εκτέλεση της ζητούμενης ενέργειας, ή

β) να αρνηθεί να δώσει συνέχεια στο αίτημα.

Ο υπεύθυνος επεξεργασίας φέρει το βάρος της απόδειξης του προδήλως αβάσιμου ή του υπερβολικού χαρακτήρα του αιτήματος.

6. Με την επιφύλαξη του άρθρου 11, όταν ο υπεύθυνος επεξεργασίας έχει εύλογες αμφιβολίες σχετικά με την ταυτότητα του φυσικού προσώπου που υποβάλλει το αίτημα που αναφέρεται στα άρθρα 15 έως 21, ο υπεύθυνος επεξεργασίας μπορεί να ζητήσει την παροχή πρόσθετων πληροφοριών αναγκαίων για την επιβεβαίωση της ταυτότητας του υποκειμένου των δεδομένων.

7. Οι πληροφορίες που πρέπει να παρέχονται στα υποκείμενα των δεδομένων σύμφωνα με τα άρθρα 13 και 14 μπορούν να παρέχονται σε συνδυασμό με τυποποιημένα εικονίδια προκειμένου να δίνεται με ευδιάκριτο, κατανοητό και ευανάγνωστο τρόπο μια ουσιαστική επισκόπηση της σκοπούμενης επεξεργασίας. Εάν τα εικονίδια διατίθενται ηλεκτρονικά, είναι μηχανικώς αναγνώσιμα.

8. Η Επιτροπή εξουσιοδοτείται να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 92 για τον καθορισμό των πληροφοριών που πρέπει να παρουσιάζονται με τα εικονίδια και των διαδικασιών για την παροχή τυποποιημένων εικονιδίων.

Άρθρο 13

Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων

1. Όταν δεδομένα προσωπικού χαρακτήρα που αφορούν υποκείμενο των δεδομένων συλλέγονται από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας, κατά τη λήψη των δεδομένων προσωπικού χαρακτήρα, παρέχει στο υποκείμενο των δεδομένων όλες τις ακόλουθες πληροφορίες:

α) την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας,

β) τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, κατά περίπτωση,

γ) τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία,

δ) εάν η επεξεργασία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο στ), τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο,

ε) τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν,

στ) κατά περίπτωση, την πρόθεση του υπευθύνου επεξεργασίας να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό και την ύπαρξη ή την απουσία απόφασης επάρκειας της Επιτροπής ή, όταν πρόκειται για τις διαβιβάσεις που αναφέρονται στο άρθρο 46 ή 47 ή στο άρθρο 49 παράγραφος 1 δεύτερο εδάφιο, αναφορά στις ενδεδειγμένες ή κατάλληλες εγγυήσεις και τα μέσα για να αποκτηθεί αντίγραφό τους ή στο πού διατέθηκαν.

2. Εκτός από τις πληροφορίες που αναφέρονται στην παράγραφο 1, ο υπεύθυνος επεξεργασίας, κατά τη λήψη των δεδομένων προσωπικού χαρακτήρα, παρέχει στο υποκείμενο των δεδομένων τις εξής επιπλέον πληροφορίες που είναι αναγκαίες για την εξασφάλιση θεμιτής και διαφανούς επεξεργασίας:

α) το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα,

β) την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορούν το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην επεξεργασία, καθώς και δικαιώματος στη φορητότητα των δεδομένων,

γ) όταν η επεξεργασία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο α) ή στο άρθρο 9 παράγραφος 2 στοιχείο α), την ύπαρξη του δικαιώματος να ανακαλέσει τη συγκατάθεσή του οποτεδήποτε, χωρίς να θιγεί η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της,

δ) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή,

ε) κατά πόσο η παροχή δεδομένων προσωπικού χαρακτήρα αποτελεί νομική ή συμβατική υποχρέωση ή απαίτηση για τη σύναψη σύμβασης, καθώς και κατά πόσο το υποκείμενο των δεδομένων υποχρεούται να παρέχει τα δεδομένα προσωπικού χαρακτήρα και ποιες ενδεχόμενες συνέπειες θα είχε η μη παροχή των δεδομένων αυτών,

στ) την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που αναφέρεται στο άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που

ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

3. Όταν ο υπεύθυνος επεξεργασίας προτίθεται να επεξεργαστεί περαιτέρω τα δεδομένα προσωπικού χαρακτήρα για άλλο σκοπό από εκείνο για τον οποίο τα δεδομένα προσωπικού χαρακτήρα συλλέχθηκαν, ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων, πριν από την εν λόγω περαιτέρω επεξεργασία, πληροφορίες για τον σκοπό αυτόν και άλλες τυχόν αναγκαίες πληροφορίες, όπως αναφέρεται στην παράγραφο 2.

4. Οι παράγραφοι 1, 2 και 3 δεν εφαρμόζονται, όταν και εφόσον το υποκείμενο των δεδομένων έχει ήδη τις πληροφορίες,

Άρθρο 14

Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων

1. Όταν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων τις ακόλουθες πληροφορίες:

α) την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας,

β) τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, κατά περίπτωση,

γ) τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία,

δ) τις σχετικές κατηγορίες δεδομένων προσωπικού χαρακτήρα,

ε) τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, ενδεχομένως,

στ) κατά περίπτωση, ότι ο υπεύθυνος επεξεργασίας προτίθεται να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε αποδέκτη σε τρίτη χώρα ή διεθνή οργανισμό και την ύπαρξη ή την απουσία απόφασης επάρκειας της Επιτροπής ή, όταν πρόκειται για τις διαβιβάσεις που αναφέρονται στο άρθρο 46 ή 47 ή στο άρθρο 49 παράγραφος 1 δεύτερο

εδάφιο, αναφορά στις ενδεδειγμένες ή κατάλληλες εγγυήσεις και τα μέσα για να αποκτηθεί αντίγραφό τους ή στο πού διατέθηκαν.

2. Εκτός από τις πληροφορίες που αναφέρονται στην παράγραφο 1, ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων τις εξής πληροφορίες που είναι αναγκαίες για τη διασφάλιση θεμιτής και διαφανούς επεξεργασίας όσον αφορά το υποκείμενο των δεδομένων:

α) το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω χρονικό διάστημα,

β) εάν η επεξεργασία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο στ), τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο,

γ) την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορά το υποκείμενο των δεδομένων και δικαιώματος αντίταξης στην επεξεργασία, καθώς και δικαιώματος στη φορητότητα των δεδομένων,

δ) όταν η επεξεργασία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο α) ή στο άρθρο 9 παράγραφος 2 στοιχείο α), την ύπαρξη του δικαιώματος να ανακαλέσει τη συγκατάθεσή του οποτεδήποτε, χωρίς να θιγεί η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της,

ε) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή,

στ) την πηγή από την οποία προέρχονται τα δεδομένα προσωπικού χαρακτήρα και, ανάλογα με την περίπτωση, εάν τα δεδομένα προήλθαν από πηγές στις οποίες έχει πρόσβαση το κοινό,

ζ) την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που προβλέπεται στο άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

3. Ο υπεύθυνος επεξεργασίας παρέχει τις πληροφορίες που αναφέρονται στις παραγράφους 1 και 2:

α) εντός εύλογης προθεσμίας από τη συλλογή των δεδομένων προσωπικού χαρακτήρα, αλλά το αργότερο εντός ενός μηνός, λαμβάνοντας υπόψη τις ειδικές

συνθήκες υπό τις οποίες τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία,

β) εάν τα δεδομένα προσωπικού χαρακτήρα πρόκειται να χρησιμοποιηθούν για επικοινωνία με το υποκείμενο των δεδομένων, το αργότερο κατά την πρώτη επικοινωνία με το εν λόγω υποκείμενο των δεδομένων, ή

γ) εάν προβλέπεται γνωστοποίηση σε άλλον αποδέκτη, το αργότερο όταν τα δεδομένα προσωπικού χαρακτήρα γνωστοποιούνται για πρώτη φορά.

4. Όταν ο υπεύθυνος επεξεργασίας προτίθεται να επεξεργαστεί περαιτέρω τα δεδομένα προσωπικού χαρακτήρα για σκοπό άλλο από εκείνον για τον οποίο τα δεδομένα προσωπικού χαρακτήρα συλλέχθηκαν, ο υπεύθυνος επεξεργασίας θα πρέπει να παρέχει στο υποκείμενο των δεδομένων, πριν από την εν λόγω περαιτέρω επεξεργασία, πληροφορίες για τον σκοπό αυτόν και άλλες τυχόν αναγκαίες πληροφορίες, όπως αναφέρεται στην παράγραφο 2.

5. Οι παράγραφοι 1 έως 4 δεν εφαρμόζονται εάν και εφόσον:

α) το υποκείμενο των δεδομένων διαθέτει ήδη τις πληροφορίες,

β) η παροχή τέτοιων πληροφοριών αποδεικνύεται αδύνατη ή θα συνεπαγόταν δυσανάλογη προσπάθεια, ιδίως όσον αφορά επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, υπό τους όρους και τις εγγυήσεις που αναφέρονται στο άρθρο 89 παράγραφος 1 ή εφόσον η υποχρέωση που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου είναι πιθανόν να καταστήσει αδύνατη ή να βλάψει σε μεγάλο βαθμό την επίτευξη των σκοπών της εν λόγω επεξεργασίας. Στις περιπτώσεις αυτές, ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για την προστασία των δικαιωμάτων και ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων, μεταξύ άλλων καθιστώντας τις πληροφορίες διαθέσιμες στο κοινό,

γ) η απόκτηση ή η κοινολόγηση προβλέπεται ρητώς από το δίκαιο της Ένωσης ή του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας και το οποίο παρέχει τα κατάλληλα μέτρα για την προστασία των έννομων συμφερόντων του υποκειμένου των δεδομένων ή

δ) εάν τα δεδομένα προσωπικού χαρακτήρα πρέπει να παραμείνουν εμπιστευτικά δυνάμει υποχρέωσης επαγγελματικού απορρήτου που ρυθμίζεται από το δίκαιο της Ένωσης ή κράτους μέλους, συμπεριλαμβανομένης της εκ του νόμου υποχρέωσης τήρησης απορρήτου.

Διόρθωση και διαγραφή

Άρθρο 16

Δικαίωμα διόρθωσης

Το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης.

Άρθρο 17

Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)

1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένας από τους ακόλουθους λόγους:

α) τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία,

β) το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο α) ή το άρθρο 9 παράγραφος 2 στοιχείο α) και δεν υπάρχει άλλη νομική βάση για την επεξεργασία,

γ) το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 1 και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία ή το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 2,

δ) τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα,

ε) τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν, ώστε να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους, στην οποία υπόκειται ο υπεύθυνος επεξεργασίας,

στ) τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών που αναφέρονται στο άρθρο 8 παράγραφος 1.

2. Όταν ο υπεύθυνος επεξεργασίας έχει δημοσιοποιήσει τα δεδομένα προσωπικού χαρακτήρα και υποχρεούται σύμφωνα με την παράγραφο 1 να διαγράψει τα δεδομένα προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία και το κόστος εφαρμογής, λαμβάνει εύλογα μέτρα, συμπεριλαμβανομένων των τεχνικών μέτρων, για να ενημερώσει τους υπευθύνους επεξεργασίας που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, ότι το υποκείμενο των δεδομένων ζήτησε τη διαγραφή από αυτούς τους υπευθύνους επεξεργασίας τυχόν συνδέσμων με τα δεδομένα αυτά ή αντιγράφων ή αναπαραγωγών των εν λόγω δεδομένων προσωπικού χαρακτήρα.

3. Οι παράγραφοι 1 και 2 δεν εφαρμόζονται στον βαθμό που η επεξεργασία είναι απαραίτητη:

α) για την άσκηση του δικαιώματος ελευθερίας της έκφρασης και του δικαιώματος στην ενημέρωση,

β) για την τήρηση νομικής υποχρέωσης που επιβάλλει την επεξεργασία βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους στο οποίο υπάγεται ο υπεύθυνος επεξεργασίας ή για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας,

γ) για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας σύμφωνα με το άρθρο 9 παράγραφος 2 στοιχεία η) και θ), καθώς και το άρθρο 9 παράγραφος 3,

δ) για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1, εφόσον το δικαίωμα που αναφέρεται στην παράγραφο 1 είναι πιθανόν να καταστήσει αδύνατη ή να εμποδίσει σε μεγάλο βαθμό την επίτευξη σκοπών της εν λόγω επεξεργασίας, ή

ε) για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Άρθρο 18

Δικαίωμα περιορισμού της επεξεργασίας

1. Το υποκείμενο των δεδομένων δικαιούται να εξασφαλίζει από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας, όταν ισχύει ένα από τα ακόλουθα:

α) η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητείται από το υποκείμενο των δεδομένων, για χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να επαληθεύσει την ακρίβεια των δεδομένων προσωπικού χαρακτήρα,

β) η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους,

γ) ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων,

δ) το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 1, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερισχύουν έναντι των λόγων του υποκειμένου των δεδομένων.

2. Όταν η επεξεργασία έχει περιοριστεί σύμφωνα με την παράγραφο 1, τα εν λόγω δεδομένα προσωπικού χαρακτήρα, εκτός της αποθήκευσης, υφίστανται επεξεργασία μόνο με τη συγκατάθεση του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή για την προστασία των δικαιωμάτων άλλου φυσικού ή νομικού προσώπου ή για λόγους σημαντικού δημόσιου συμφέροντος της Ένωσης ή κράτους μέλους.

3. Το υποκείμενο των δεδομένων το οποίο έχει εξασφαλίσει τον περιορισμό της επεξεργασίας σύμφωνα με την παράγραφο 1 ενημερώνεται από τον υπεύθυνο επεξεργασίας πριν από την άρση του περιορισμού επεξεργασίας.

Άρθρο 19

Υποχρέωση γνωστοποίησης όσον αφορά τη διόρθωση ή τη διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας

Ο υπεύθυνος επεξεργασίας ανακοινώνει κάθε διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας των δεδομένων που διενεργείται σύμφωνα με το άρθρο 16, το άρθρο 17 παράγραφος 1 και το άρθρο 18 σε κάθε αποδέκτη στον οποίο γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, εκτός εάν αυτό αποδεικνύεται ανέφικτο ή εάν συνεπάγεται δυσανάλογη προσπάθεια. Ο υπεύθυνος επεξεργασίας ενημερώνει το υποκείμενο των δεδομένων σχετικά με τους εν λόγω αποδέκτες, εφόσον αυτό ζητηθεί από το υποκείμενο των δεδομένων.

Άρθρο 20

Δικαίωμα στη φορητότητα των δεδομένων

1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα, όταν:

α) η επεξεργασία βασίζεται σε συγκατάθεση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο α) ή το άρθρο 9 παράγραφος 2 στοιχείο α) ή σε σύμβαση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο β) και

β) η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα.

2. Κατά την άσκηση του δικαιώματος στη φορητότητα των δεδομένων σύμφωνα με την παράγραφο 1, το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητά την απευθείας διαβίβαση των δεδομένων προσωπικού χαρακτήρα από έναν υπεύθυνο επεξεργασίας σε άλλον, σε περίπτωση που αυτό είναι τεχνικά εφικτό.

3. Το δικαίωμα που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου ασκείται με την επιφύλαξη του άρθρου 17. Το εν λόγω δικαίωμα δεν ισχύει για την επεξεργασία που είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο

συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.

4. Το δικαίωμα που αναφέρεται στην παράγραφο 1 δεν επηρεάζει δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων.

ΠΑΡΑΡΤΗΜΑ Γ

Ερωτηματολόγιο

• Ποιος είναι ο ρόλος σας στην εταιρεία με τι ασχολείστε (συνοπτικά)

• Πόσα χρόνια εργάζεστε στο ΟΤΕ

• Πόσα χρόνια έχετε στην συγκεκριμένη θέση

• Παρακαλούμε προσδιορίστε τις μεθόδους που χρησιμοποιείτε για τη συλλογή των δεδομένων προσωπικού χαρακτήρα (επιγραμματικά).

• Ποια είναι τα πλεονεκτήματα για την εταιρεία από την εφαρμογή του GDPR.

• Ποιες είναι οι κατηγορίες των προσωπικών δεδομένων που επεξεργάζονται από τον ΟΤΕ;

• Υπάρχει έγγραφη πολιτική ασφαλείας της επιχείρησης σας για την προστασία των δεδομένων προσωπικού χαρακτήρα; Τι αναφέρει;

• Η επιχείρησή σας τηρεί συγκεκριμένη διαδικασία όσον αφορά την ασφαλή διαγραφή ή την ηθελημένη καταστροφή προσωπικών δεδομένων; Αν ναι ποια είναι;

• Σε συνέχεια της παραπάνω ερώτησης οι εργαζόμενοι ερωτήθηκαν για τα Τεχνικά και Οργανωτικά μέτρα που λαμβάνει η εταιρεία

• Σας έχει γίνει εκπαίδευση για την προστασία προσωπικών δεδομένων; Αν ναι κάθε πότε γίνεται ;

• Υπάρχει υπεύθυνος Επεξεργασίας (Controller) και Υπεύθυνος Προστασίας Δεδομένων(DPO) και ποιος είναι ο ρόλος τους;

• Με ποιους συνεργάτες σας έχετε υπογράψει συμβάσεις εμπιστευτικότητας και εχεμύθειας π.χ. Συμφωνητικό Επεξεργασίας Δεδομένων και σε τι αναφέρεται αυτό;

• Τι είναι το Συμφωνητικό Επεξεργασίας Δεδομένων(Data Processing Agreement) που υπογράφετε με τους εξωτερικούς συνεργάτες και τους προμηθευτές ;

• Παρακαλώ περιγράψτε συνοπτικά τα βήματα ασφαλείας που ακολουθούνται από τους εργαζόμενους σε περίπτωση που αποκτούν πρόσβαση σε προσωπικά δεδομένα.

Βιβλιογραφία

Zhiyuan Fang (2002) E-Government in Digital Era: Concept, Practice, and Development http://www.journal.au.edu/ijcim/2002/may02/article1.pdf

Meghan E. Cook(2000) What Citizens Want From E-Government http://www.ctg.albany.edu/publications/reports/what_citizens_want/what_citizens_want.pdf

Kim M. Thompson(2003) E-government around the world: Lessons, challenges, and future directions http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6W4G-4B6SK9R-5&_user=83476&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000059629&_version=1&_urlVersion=0&_userid=83476&md5=5db231b7e5fcf43a0a19339aeaf1f582

Paul T. Jaeger(2003) The endless wire: E-government as global phenomenon http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6W4G-4B6SK9R-1&_user=83476&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000059629&_version=1&_urlVersion=0&_userid=83476&md5=d9f73ae58d1b17f7ff45f4ce37583328

Yu-Che Chen, Kurt Thurmaier (2007) Advancing E-Government: Financing Challenges and Opportunities.

http://www.blackwell-synergy.com/doi/pdf/10.1111/j.15406210.2008.00889.x?cookieSet=1

Lourdes Torres,Vicente Pina, and Basilio Acerete(2006) E-Governance developments in European Union Cities: Reshaping Government's Relationship with Citizens.

http://www.blackwell-synergy.com/doi/pdf/10.1111/j.1468-0491.2006.00315.x

E-GOV AWARDS IN EYROPE

http://ec.europa.eu/information_society/activities/egovernment/docs/lisbon_2007/lisbon_exhibition_catalogue_2007.pdf

Παρατηρητήριο

http://www.observatory.gr/files/meletes/eGov

Ιστοσελίδες

https://www.dpa.gr/portal/page?_pageid=33,213319&_dad=portal&_schema=PORTAL
https://mynet.ote.gr/useful-information/%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%B5%CE%B9%CE%B1-%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CF%89%CE%BD-%CE%BA%CE%B1%CE%B9-%CF%80%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%B9%CE%B1-%CF%80%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CF%89%CE%BD-%CE%B4%CE%B5%CE%B4%CE%BF/general-data-protection-regulation-(gdpr)

https://mynet.ote.gr/getattachment/Useful-Information/Ασφαλεια-πληροφοριων-και-προστασια-προσωπικων-δεδο/Ενημερωσεις-Προστασιας-Δεδομενων-(Privacy-Noti-(1)/Ενημερωση-για-την-Προστασια-Προσωπικων-Δεδομενων-τ/Ενημερωση-για-την-επεξεργασια-προσωπικων-δεδομενων-στις-Εταιρειες-του-Ομιλου-OTE.pdf
https://www.dreamweaver.gr/gdpr-%CE%BD%CE%BF%CE%BC%CE%BF%CE%B8%CE%B5%CF%83%CE%AF%CE%B1.php