Εφαρμόζοντας τον γενικό κανονισμό προστασίας προσωπικών δεδομένων στο σχολικό εργαστήριο πληροφορικής

Ελευθέριος Ε. Δερμιτζάκης

Επιστημονικός Συνεργάτης, Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών, Πολυτεχνείο Κρήτης, Χανιά 73100, Ελλάδα, Καθηγητής Πληροφορικής (ΠΕ86) ΔΕ Χανίων.
Email:dermitz@dpem.tuc.gr

Περίληψη

Στο παρόν άρθρο προτείνεται ένα πλαίσιο ασφαλείας προσωπικών δεδομένων του σχολικού εργαστηρίου πληροφορικής βασιζόμενο στο ISO 27001 (ISO/IEC 27001:2013), εναρμονισμένο στη λογική της συμμόρφωσης με τον γενικό κανονισμό προστασίας δεδομένων (ΓΚΠΔ). Στόχος του πλαισίου είναι η προστασία των προσωπικών δεδομένων τόσο των μαθητών όσο και των καθηγητών μέσα από μία σειρά ενεργειών και πολιτικών ασφαλείας που πρέπει να εφαρμόζονται στο σχολικό εργαστήριο πληροφορικής.

Λέξεις κλειδιά: Γενικός κανονισμός προστασίας δεδομένων(ΓΚΠΔ), Ασφάλεια πληροφοριών, ISO27001.

1. Εισαγωγή

Η παρούσα εργασία επιχειρεί να διαμορφώσει ένα πλαίσιο ασφάλειας των προσωπικών δεδομένων των μαθητών και εκπαιδευτικών στο σχολικό εργαστήριο πληροφορικής εναρμονισμένο με τον ΓΚΠΔ. Αν και υπάρχουν οδηγίες, που κάθε χρόνο επικαιροποιούνται, από το Πανελλήνιο Σχολικό Δίκτυο(ΠΣΔ) που αφορούν ζητήματα ασφάλειας προσωπικών δεδομένων, ωστόσο δεν έχει μέχρι τώρα διαμορφωθεί ή προταθεί ένα σαφές πλαίσιο ως μοντέλο συμμόρφωσης ούτε αυτό εμφανίζεται στη βιβλιογραφία.

Ο νέος κανονισμός EU 2016/679 (ΓΚΠΔ,2016) του ευρωπαϊκού κοινοβουλίου ορίζει με σαφήνεια το δικαίωμα κάθε φυσικού προσώπου στην προστασία των προσωπικών του δεδομένων. Παράλληλα θέτει τους κανόνες σε ότι αφορά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα διαμορφώνοντας έτσι έναν χώρο ασφάλειας και ελευθερίας για την ασφαλή διακίνηση και διαχείριση των προσωπικών δεδομένων εντός και εκτός Ευρωπαϊκής Ένωσης όπως περιγράφεται στην αιτιολογική έκθεση 1 &2 του ΓΚΠΔ.

Επιπλέον, τα άρθρα 6, 12 έως 22 και 29 του ΓΚΠΔ απαιτούν την ασφάλεια του πληροφοριακού συστήματος εξ' ορισμού, ορίζουν κανόνες για τη νομιμότητα της επεξεργασίας και τα δικαιώματα των φυσικών προσώπων. Ουσιαστικά ο κανονισμός δημιουργεί ένα νομικό πλαίσιο για τη διαχείριση των προσωπικών δεδομένων,

ISBN: 978-960-578-084-5

περιγράφοντας τα εργαλεία που πρέπει κάποιος να χρησιμοποιήσει για τη συμμόρφωση. Ένα εξ αυτών είναι ένα πρότυπο διαχείρισης της ασφάλειας ενός πληροφοριακού συστήματος όπως το ISO 270001:2013 (ISO/IEC 27001:2013,2013)

Το ISO 27001 επιτυγχάνει τον στόχο του με την εφαρμογή ενός καλά σχεδιασμένου συνόλου ελέγχων, πολιτικών, διαδικασιών και λήψη τεχνικών μέτρων. Σημαντικό είναι επίσης ότι οι έλεγχοι αυτοί θα πρέπει όχι μόνο να σχεδιαστούν και να υλοποιηθούν αλλά στη συνέχεια να μετρηθεί η εφαρμογή τους και η απόδοσή τους (Calder, A. and Watkins, 2008).
Το περιβάλλον ενός σχολικού εργαστηρίου πληροφορικής αποτελεί για τους μαθητές μια πρώτη επαφή με ένα πληροφοριακό σύστημα μικρής κλίμακας με ιδιαίτερα χαρακτηριστικά. Για παράδειγμα, οι μαθητές όπως και οι εκπαιδευτικοί κάνουν χρήση προσωπικών δεδομένων, είτε για να ταυτοποιηθούν (όνομα χρήστη, κωδικοί κλπ) σε εκπαιδευτικές πλατφόρμες, είτε για να ανταλλάξουν δεδομένα στο πλαίσιο της εκπαιδευτικής διαδικασίας (αποστολή και λήψη ηλεκτρονικού ταχυδρομείου, φωτογραφίες κλπ). Ωστόσο δεν τίθεται θέμα συγκατάθεσης των μαθητών για την χρήση των προσωπικών δεδομένων τους από τους εκπαιδευτικούς, αφού χρησιμοποιούνται μόνο αυτά που παρέχονται από το myschool. Επιπλέον, η δυνατότητα χρήσης μεταφερόμενων αποθηκευτικών μέσων, είτε η χρήση της τεχνολογίας cloud computing, μπορούν να αποτελέσουν εύκολη πηγή διαμοιρασμού προσωπικών δεδομένων (φωτογραφίες, κείμενα συνομιλιών, ευαίσθητα προσωπικά δεδομένα και λοιπά). Αν και τυπικά δεν επιτρέπεται η χρήση πηγών εκτός ΠΣΔ ωστόσο άτυπα μπορεί να συμβεί.

2. Το Διεθνές Πρότυπο ISO/IEC 27000:2013

Το Διεθνές Πρότυπο ISO/IEC 27000:2013, αποτελεί ένα διεθνές πρότυπο στην ασφάλεια ενός πληροφοριακού συστήματος. Το πρότυπο αυτό, δίνει τη δυνατότητα με ένα αντικειμενικό τρόπο, να αναγνωρίσουμε τις τεχνικές ευπάθειες καθώς και την επάρκεια ή μη ενός πληροφοριακού συστήματος σε θέματα ασφάλειας. Κάνοντας χρήση του συγκεκριμένου προτύπου η εταιρεία ή ο οργανισμός αποκτά και τεκμηριώνει τη γνώση που χρειάζεται να έχει, σε ότι αφορά την ασφάλεια του πληροφοριακού του συστήματος. Το πρότυπο περιλαμβάνει εκατό δεκατρία σημεία ελέγχου (ISO 27001 controls) τα οποία ελέγχουν αναλυτικά ένα πληροφοριακό σύστημα. Οι έλεγχοι αυτοί περιλαμβάνουν τις παρακάτω ενότητες:

ISO 27001 -2013 Κατηγορίες Ελέγχου

1. A.5 Πολιτικές ασφάλειας πληροφοριών
2. A.6 Οργάνωση της ασφάλειας των πληροφοριών
3. A.7 Ασφάλεια των ανθρώπινων πόρων
4. A.8 Διαχείριση περιουσιακών στοιχείων

ISBN: 978-960-578-084-5

5. Α.9 Έλεγχος πρόσβασης
6. Α.10 Κρυπτογραφία
7. Α.11 Φυσική και περιβαλλοντική ασφάλεια
8. Α.12 Ασφάλεια επιχειρήσεων
9. Α.13 Ασφάλεια επικοινωνιών
10. Α.14 Απόκτηση, ανάπτυξη και συντήρηση του συστήματος
11. Α.15 Σχέσεις προμηθευτών
12. Α.16 Διαχείριση περιστατικών ασφάλειας πληροφοριών
13. Α.17 Ασφάλεια πληροφοριών όσον αφορά τη διαχείριση της συνέχισης των δραστηριοτήτων
14. Α.18 Συμμόρφωση

Κάθε βασική κατηγορία, επιμερίζεται σε υποκατηγορίες, εξειδικεύοντας περισσότερο στον τομέα της ασφάλειας της πληροφορίας που ελέγχει, βάζοντας ένα στόχο ο οποίος πρέπει να επιτευχθεί μέσα από τους ελέγχους. Η περιγραφή του κάθε ελέγχου έχει συγκεκριμένη δομή η οποία αποτελείται από (α) τον καθορισμό μέσα σε μια ειδική δήλωση, ώστε να ικανοποιείται ο στόχος, (β) οδηγίες οι οποίες παρέχουν λεπτομερέστατη πληροφορία ώστε να υποστηρίζεται η εφαρμογή του, και να πληρούνται οι απαιτήσεις που έχουν τεθεί και (γ) συμπληρωματική πληροφορία που θα πρέπει να ληφθεί υπόψη, όπως νομικά ζητήματα και αναφορές σε άλλα πρότυπα (J. Stuart Broderick, 2006).

3. Πλαίσιο συμμόρφωσης ενός σχολικού εργαστηρίου πληροφορικής με τον γενικό κανονισμό

Από τις κατηγορίες των δεικτών που αναφέρθηκαν παραπάνω για το ISO 27001 θα εστιάσουμε σε συγκεκριμένες κατηγορίες οι οποίες σε συνδυασμό με τις βασικές αρχές του γενικού κανονισμού προστασίας, μπορούν να αποτελέσουν ένα πλαίσιο συμμόρφωσης του σχολικού εργαστηρίου πληροφορικής με τον γενικό κανονισμό προστασίας δεδομένων. Το πλαίσιο συμμόρφωσης θα πρέπει να περιλαμβάνει δύο άξονες. Από τη μία πρέπει να εντοπίζει ζητήματα ασφαλείας του εργαστηρίου πληροφορικής τα οποία θα αναδειχθούν μέσα από τους ελέγχους του ISO 27001. Από την άλλη θα πρέπει να διευθετηθούν ζητήματα που αφορούν τη διαχείριση προσωπικών δεδομένων (μαθητών και καθηγητών).
Το πλαίσιο συμμόρφωσης διακρίνει δύο άξονες ελέγχου όπως έχει ήδη αναφερθεί.

ISBN: 978-960-578-084-5

3.1. Άξονας Ι

Περιλαμβάνει επιλεγμένους δείκτες από το ISO 27001 οι οποίοι ελέγχουν και αναγνωρίζουν τεχνικές ευπάθειες και ζητήματα ασφαλείας του σχολικού εργαστηρίου.
Στον παρακάτω πίνακα (πίνακας 1) φαίνονται οι επιλεγμένοι δείκτες από το ISO 2700:2013 οι οποίοι προτείνονται ως σημεία ελέγχου του σχολικού εργαστηρίου πληροφορικής Η επιπλέον μελέτη του πρωτότυπου κειμένου του ISO/IEC 27001:2013 θα βοηθούσε στη εφαρμογή του.

Πίνακας 1. *Προτεινόμενα πεδία ελέγχου του άξονα Ι*

Κωδικός Δείκτη Ελέγχου	Περιγραφή Ενεργειών
A.5.1.1	Πρέπει να οριστεί ένα σύνολο πολιτικών και κανόνων που αφορούν γενικά την ασφάλεια και τη χρήση του εργαστηρίου πληροφορικής. Οι κανόνες αυτοί θα πρέπει να είναι γνωστοί σε όσους χρησιμοποιούν το εργαστήριο.
A.5.1.2	Εάν υπάρξουν αλλαγές στη χρήση του εργαστηρίου θα πρέπει να επικαιροποιούνται οι κανόνες οι οποίοι θα πρέπει να γνωστοποιούνται ως αλλαγές.
A.6.1.1	Θα πρέπει να είναι απολύτως ξεκάθαρο ποιες είναι οι υποχρεώσεις ενός καθηγητή που χρησιμοποιεί το εργαστήριο πληροφορικής.
A.6.1.4	Ο υπεύθυνος εργαστηρίου θα πρέπει να είναι σε επικοινωνία με τους υπεύθυνους του κεπληνετ για ζητήματα που αφορούν την ασφάλεια και την διαχείριση των προσωπικών δεδομένων.
A.6.2.2	Σε περίπτωση τηλεργασίας ή γενικότερα συνεργασίας αυτής της μορφής θα πρέπει να εξασφαλίζεται η προστασία των πληροφοριών που μεταφέρονται, επεξεργάζονται ή αποθηκεύονται σε χώρους τηλεργασίας.
A.7.2.2	Όλοι όσοι κάνουν χρήση του εργαστηρίου πληροφορικής θα πρέπει να λαμβάνουν κατάλληλη εκπαίδευση και κατάρτιση ευαισθητοποίησης σε θέματα ασφάλειας πληροφοριών.
A.7.2.3	Θα πρέπει να έχει γνωστοποιηθεί εξαρχής ποια πειθαρχική (ενδεχομένως) διαδικασία προβλέπεται και ποια μέτρα λαμβάνονται σε περίπτωση που υπάρξει παραβίαση της ασφάλειας των πληροφοριών.
A.8.1.1	Τα περιουσιακά στοιχεία που σχετίζονται με τις πληροφορίες και την επεξεργασία προσδιορίζονται και καταρτίζεται και τηρείται κατάλογος αυτών των περιουσιακών στοιχείων
A.8.1.4	Όλοι οι εργαζόμενοι και οι εξωτερικοί χρήστες θα επιστρέψουν όλα τα οργανωτικά περιουσιακά στοιχεία που βρίσκονται στην κατοχή τους κατά τη λήξη της απασχόλησης, της σύμβασης ή της συμφωνίας.
A.8.3.1	Εφαρμόζονται διαδικασίες για τη διαχείριση των αφαιρούμενων αποθηκευτικών μέσων σύμφωνα με το σύστημα που υιοθετεί ο οργανισμός.
A.8.3.2	Τα μέσα πρέπει να απορρίπτονται με ασφάλεια όταν δεν χρειάζονται πλέον, χρησιμοποιώντας επίσημες διαδικασίες.
A.8.3.3	Τα μέσα που περιέχουν πληροφορίες προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, κακή χρήση ή διαφθορά κατά τη μεταφορά.

ISBN: 978-960-578-084-5

A.9.1.2	Οι χρήστες πρέπει να έχουν πρόσβαση μόνο στις υπηρεσίες δικτύου και δικτύου που έχουν εξουσιοδοτηθεί ειδικά να χρησιμοποιούν.
A.9.2.1	Απαιτείται επίσημη διαδικασία καταχώρισης και διαγραφής από τον χρήστη, προκειμένου να καταστεί δυνατή η ανάθεση δικαιωμάτων πρόσβασης. Η διαδικασία αυτή μπορεί να συνεπικουρείται από τα στοιχεία του myschool.
A.9.2.3	Η κατανομή και η χρήση προνομιακών δικαιωμάτων πρόσβασης περιορίζεται και ελέγχεται.
A.9.2.6	Τα δικαιώματα πρόσβασης καθηγητών και μαθητών σε εγκαταστάσεις πληροφόρησης και επεξεργασίας πληροφοριών αφαιρούνται κατά τη λήξη της απασχόλησης, της σύμβασης ή της λήξης του σχολικού έτους.
A.9.3.1	Θα πρέπει να γίνει ξεκάθαρο προς τους χρήστες του εργαστηρίου ότι αυτοί έχουν την ευθύνη για τους κωδικούς πρόσβαση τους.
A.9.4.4	Η χρήση βοηθητικών προγραμμάτων που ενδέχεται να είναι ικανά να παραβλέψουν τους ελέγχους συστημάτων και εφαρμογών πρέπει να περιορίζεται και να ελέγχεται αυστηρά η πιθανή εγκατάστασή τους
A.11.1.2	Οι ασφαλείς περιοχές προστατεύονται με τους κατάλληλους ελέγχους εισόδου ώστε να εξασφαλίζεται ότι επιτρέπεται η πρόσβαση μόνο εξουσιοδοτημένου προσωπικού.
A.11.2.1	Ο εξοπλισμός πρέπει να τοποθετείται και να προστατεύεται για τη μείωση των κινδύνων από περιβαλλοντικές απειλές και κινδύνους και ευκαιρίες για μη εξουσιοδοτημένη πρόσβαση
A.11.2.3	Οι καλωδιώσεις ενέργειας και των τηλεπικοινωνιών που μεταφέρουν δεδομένα ή υποστηρίζουν τις υπηρεσίες πληροφοριών πρέπει να προστατεύονται από την παρακολούθηση, την παρεμβολή ή τη ζημία.
A.11.2.4	Ο εξοπλισμός πρέπει να διατηρείται σωστά για να εξασφαλίζεται η συνεχής διαθεσιμότητα και ακεραιότητά του.
A.11.2.5	Ο εξοπλισμός, η πληροφορία ή το λογισμικό δεν πρέπει να καταργούνται χωρίς προηγούμενη άδεια.
A.11.2.9	Πρέπει να υιοθετηθεί μια σαφής πολιτική γραφείου για χαρτιά και αφαιρούμενα μέσα αποθήκευσης και μια πολιτική «καθαρής» οθόνης για τις εγκαταστάσεις επεξεργασίας πληροφοριών.
A.12.6.1	Ο υπεύθυνος του εργαστηρίου θα πρέπει να τηρεί αρχείο σε σχέση με τις τεχνικές ευπάθειες των συστημάτων πληροφοριών που ανιχνεύονται και να τις αξιολογεί λαμβάνοντας τα κατάλληλα μέτρα.
A.13.2.1	Πρέπει να υπάρχουν γνωστοποιημένοι κανόνες που αφορούν τη μεταφορά πληροφοριών είτε εντός του εργαστηρίου είτε εκτός.
A.13.2.3	Οι πληροφορίες που αφορούν τα ηλεκτρονικά μηνύματα πρέπει να προστατεύονται κατάλληλα.
A.16.1.1	Πρέπει να θεσπιστούν διαδικασίες διαχείρισης περιστατικών ασφαλείας, για να εξασφαλιστεί η ταχεία, αποτελεσματική και τακτική αντιμετώπιση τους.
A.16.1.2	Τα γεγονότα για την ασφάλεια των πληροφοριών πρέπει να ανακοινώνονται μέσω κατάλληλων διαύλων διαχείρισης το συντομότερο δυνατό (Για παράδειγμα στο κεπληνετ).
A.16.1.3	Όσοι κάνουν χρήση του εργαστηρίου πληροφορικής υποχρεούνται να σημειώνουν και να αναφέρουν τυχόν παρατηρούμενες ή ύποπτες αδυναμίες

ISBN: 978-960-578-084-5

	ασφάλειας πληροφοριών σε συστήματα ή υπηρεσίες.
A.18.1.1	Θα πρέπει να γνωστοποιείται σε όλους τους χρήστες του εργαστηρίου με ένα εύκολα κατανοητό τρόπο, η ισχύουσα νομοθεσία που αφορά την προστασία των προσωπικών δεδομένων καθώς και την ασφάλεια όλο του πληροφοριακού συστήματος.
A.18.1.2	Θα πρέπει να γνωστοποιείται σε όλους τους χρήστες του εργαστηρίου η νομοθεσία που αφορά ζητήματα πνευματικής ιδιοκτησίας.
A.18.1.3	Ο υπεύθυνος του εργαστηρίου θα πρέπει να ενημερώνει όλους τους χρήστες σχετικά με τους τρόπους που μπορούν να προστατεύσουν τα αρχεία τους.

3.2. Άξονας ΙΙ

Σε αυτόν τον άξονα οι έλεγχοι εξειδικεύουν σε ζητήματα διαχείρισης προσωπικών δεδομένων σύμφωνα με τον γενικό κανονισμό .
Σε αυτό τον άξονα λοιπόν, προτείνονται οι παρακάτω έλεγχοι (πίνακας 2).

Πίνακας 2. *Προτεινόμενα πεδία ελέγχου του άξονα ΙΙ*

Όνομα Ενέργειας	Περιγραφή
Ε1. Ενημέρωση	Ενημερώστε το ανθρώπινο δυναμικό του σχολικού εργαστηρίου για τα δικαιώματα των υποκειμένων των δεδομένων, υπογραμμίζοντας τις σημαντικές επιπτώσεις σε περίπτωση παραβιάσεις των δικαιωμάτων.
Ε2. Καταγραφή	Καταγράψτε ενδελεχώς τις κατηγορίες (ροές δεδομένων) των προσωπικών δεδομένων που ενδεχομένως χρησιμοποιούνται από μαθητές και καθηγητές καθώς και τις πιθανές επεξεργασίες στις οποίες μπορεί να υποβάλλονται.
Ε3. Ετοιμότητα	Αξιολογήστε τους πιθανούς κινδύνους για τα προσωπικά δεδομένα που χρησιμοποιούνται στο σχολικό εργαστήριο πληροφορικής και διαμορφώσετε μία στρατηγική αντιμετώπισης των πιθανών κινδύνων με τεχνικά και οργανωτικά μέτρα.
Ε4. Παραβίαση δεδομένων	Υιοθετήστε μεθόδους για την ανίχνευση, την καταγραφή και τη διερεύνηση περιστατικών παραβιάσεων σε προσωπικά δεδομένα εντός του σχολικού εργαστηρίου πληροφορικής.
Ε5. Αναθεώρηση πολιτικών προστασίας	Επικαιροποιήστε τις διαδικασίες που ενδεχομένως διαθέτετε στο σχολικό εργαστήριο σε σχέση με την ασφάλεια και την προστασία των προσωπικών δεδομένων, πάντα στο πνεύμα του κανονισμού προστασίας προσωπικών δεδομένων.
Ε6. Εκτίμηση Επιπτώσεων	Θα πρέπει να είστε σε θέση να εκτιμήσετε τις πιθανότητες επέλευσης κινδύνων και τις συνέπειες στα προσωπικά δεδομένα μαθητών και καθηγητών.

ISBN: 978-960-578-084-5

Για τη συμμόρφωση με το προτεινόμενο πλαίσιο προτείνεται η παρακάτω σειρά ενεργειών.

1. Άξονας Ι (Α.5.1.1 έως και Α.18.1.3) σύμφωνα με τη περιγραφή των συνοπτικών ενεργειών που παρατίθεται. Αναλυτικές οδηγίες για κάθε πεδίο ελέγχου υπάρχουν στα κείμενα που τεκμηριώνουν το ISO27001 (ISO/IEC 27001:2013,2013).
2. Άξονας ΙΙ (Ε1 έως και Ε6). Αναλυτικές οδηγίες υπάρχουν στον ΓΚΠΔ (ΓΚΠΔ,2016) και συγκεκριμένα στο τμήμα αιτιολογικών εκθέσεων (1 έως και 173)

4. Επίλογος

Αυτό που τονίζεται μέσα από το γενικό κανονισμό (ΓΚΠΔ, 2016) είναι ότι τα προσωπικά δεδομένα κάθε φυσικού προσώπου αποτελούν ένα κομμάτι από την ψηφιακή του περιουσία τα οποία και θα πρέπει να προστατεύει. Ο γενικός κανονισμός έρχεται και οριοθετεί τους κανόνες και τις αρχές για τους πολίτες της Ευρωπαϊκής Ένωσης σε σχέση με τα προσωπικά τους δεδομένα. Αν αναλογιστούμε τον όγκο των πληροφοριών που χειρίζονται τα κοινωνικά δίκτυα καθώς και οι υπηρεσίες διαδικτύου αντιλαμβανόμαστε την απόλυτη ανάγκη του κανονισμού.

Το άρθρο καταλήγει στα παρακάτω συμπεράσματα. Το πλαίσιο που προτείνεται για τη συμμόρφωση του σχολικού εργαστηρίου πληροφορικής με τον γενικό κανονισμό προστασίας δεδομένων, με τη βοήθεια του ISO 27001, αποτελεί μία βάση για το πώς θα πρέπει να αντιλαμβάνονται τόσο οι εκπαιδευτικοί όσο και οι μαθητές τη σπουδαιότητα των προσωπικών τους δεδομένων. Η εφαρμογή του πλαισίου θα αποτελέσει έναν καλό μηχανισμό διαχείρισης της ασφαλείας του σχολικού εργαστηρίου. Οι προτεινόμενες ενέργειες του Άξονα Ι παρέχουν την ασφάλεια μέσα από ένα δοκιμασμένο και διεθνές πρότυπο, το ISO27001, ενώ οι προτεινόμενες ενέργειες του Άξονα ΙΙ εξασφαλίζουν την κατά το δυνατόν σύγκλιση στις απαιτήσεις του ΓΚΠΔ.

Το όφελος από την εφαρμογή του προτεινόμενου πλαισίου είναι διπλό. Αφενός διευθετεί ζητήματα ασφάλειας που ο εκπαιδευτικός μπορεί να αντιμετωπίσει μέσα στο σχολικό εργαστήριο καθώς και ζητήματα που αφορούν τον ΓΚΠΔ, αφετέρου αποτελεί μια πλατφόρμα εκπαίδευσης σε ζητήματα και έννοιες του ΓΚΠΔ (προσωπικά δεδομένα, ευαίσθητα προσωπικά δεδομένα, επεξεργασίας, συγκατάθεση κλπ). Τέλος να σημειωθεί ότι ο ΓΚΠΔ κάνει αναφορά στο θέμα της εκπαίδευσης και ευαισθητοποίησης στις έννοιές του (ΓΚΠΔ, αιτιολογική σκέψη 132).

Μία επέκταση αυτού του πλαισίου θα ήταν η πλήρης συμμόρφωση ενός εργαστηρίου πληροφορικής με το ISO 27001 έτσι ώστε να διασφαλιστεί πλήρως και να πιστοποιηθεί ο εργαστηριακός χώρος. Τέλος, το προτεινόμενο πλαίσιο, θα μπορούσε να χρησιμοποιηθεί ως εκπαιδευτικό υλικό έτσι ώστε να εισαγάγει τους μαθητές και

ISBN: 978-960-578-084-5

τους καθηγητές στον τρόπο με τον οποίον διαχειριζόμαστε την ασφάλεια ενός πληροφοριακού συστήματος.

Αναφορές

Calder, A. and Watkins, S. (2008). IT Governance: A Manager's Guide to Security and ISO27001/ISO27002. London and Philadelphia: Kogan Page LTD.

ISO/IEC 27001:2013. (2013). Information technology — Security techniques — Code of practice for information security management.

Stuart Broderick. (2006). "ISMS, security standards and security regulations," Information Security Technical Report, Volume 11, Issue 1, pp. 26-31.

ΓΚΠΔ. (2016). Γενικός Κανονισμός Προστασίας Δεδομένων) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και για την κατάργηση της οδηγίας 95/46/ΕΚ.

Abstract

In this article a new framework for the security of an information system based on ISO 27001:2013 and General Data Protection Regulation (GDPR) is defined for school's computer labs. A school computer lab is essentially an environment for managing and processing small-scale personal data. Although there are instructions and general guidelines for the whole school network, additional actions should be taken at the school laboratory level to ensure that the personal data of students and teachers are protected from violations.

Keywords: General Data Protection Regulation (GDPR), Information Security, ISO2700.

ISBN: 978-960-578-084-5