ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 07-05-2019
Αριθ. Πρωτ.: Γ/ΕΞ/3254/07-05-2019

Α Π Ο Φ Α Σ Η ΑΡ. 10 / 2019

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνήλθε, μετά από πρόσκληση του Προέδρου της, σε τακτική συνεδρίαση στην έδρα της την 24/4/2018, σε συνέχεια των από 16/3/2017, 20/6/2017 και 21/9/2017 συνεδριάσεων, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν ο Πρόεδρος της Αρχής, Κωνσταντίνος Μενουδάκος και τα τακτικά μέλη της Αρχής Κωνσταντίνος Χριστοδούλου, Αντώνιος Συμβώνης, ως εισηγητής, Σπυρίδων Βλαχόπουλος, επίσης ως εισηγητής, Κωνσταντίνος Λαμπρινουδάκης, Χαράλαμπος Ανθόπουλος καθώς το αναπληρωματικό μέλος Εμμανουήλ Δημογεροντάκης σε αναπλήρωση του τακτικού μέλους Ελένης Μαρτσούκου, η οποία, αν και εκλήθηκε νομίμως εγγράφως, δεν προσήλθε λόγω κωλύματος. Στη συνεδρίαση, χωρίς δικαίωμα ψήφου, παρέστησαν, επίσης, με εντολή του Προέδρου, οι Μαρία Αλικάκου και Ευφροσύνη Σιουγλέ, ειδικοί επιστήμονες - ελεγκτές, ως βοηθοί εισηγητές, οι οποίες αποχώρησαν μετά τη συζήτηση και πριν από τη διάσκεψη και τη λήψη αποφάσεως, και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του Τμήματος Διοικητικών Υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη τα παρακάτω:

Υποβλήθηκε στην Αρχή η με αριθμ. πρωτ. Γ/ΕΙΣ/7646/23.11.2016 καταγγελία του Συνδέσμου Ιδιωτικών Σχολείων (εφεξής ΣΙΣ) αναφορικά με επιβαλλόμενη από το

Υπουργείο Παιδείας, Έρευνας και Θρησκευμάτων (εφεξής ΥΠΕΘ) υποχρέωση καταχώρησης «απλών» δεδομένων και δεδομένων ειδικών κατηγοριών των μαθητών, γονέων/κηδεμόνων και εκπαιδευτικών των ιδιωτικών σχολείων στην ενιαία κεντρική βάση δεδομένων του ΥΠΕΘ με την ονομασία ««mySchool» (εφεξής «mySchool»).

Συγκεκριμένα, με το με αριθμ. πρωτ. Φ8/145/97610/Δ2/14.6.2016 έγγραφο του Γ.Γ. του ΥΠΕΘ, ο ΣΙΣ ενημερώθηκε ότι από το σχολικό έτος 2016-2017 όλα τα ιδιωτικά σχολεία Α' βάθμιας και Β' βάθμιας Εκπαίδευσης όφειλαν να καταχωρούν στην ως άνω βάση «mySchool» στοιχεία αναφορικά με το μαθητικό δυναμικό, τη σχολική μονάδα και το μητρώο εκπαιδευτικού προσωπικού, έτσι ώστε να ολοκληρωθεί η ψηφιακή απεικόνιση των στοιχείων λειτουργίας όλων των ιδιωτικών σχολικών μονάδων. Στις 22.9.2016, το ΥΠΕΘ με το με αριθμ. πρωτ. 154892/Ε1.22.09.2016 έγγραφό του επανήλθε στο ως άνω ζήτημα και, μεταξύ άλλων, όπως αναφέρεται στην υπό κρίση καταγγελία, επιβλήθηκε στα ιδιωτικά σχολεία η υποχρέωση να καταχωρούν στο «mySchool» το εβδομαδιαίο πρόγραμμα διδασκαλίας, τα στοιχεία των εκπαιδευτικών και των μαθητών κάθε τάξης και τμήματος κατ' αντιστοιχία με τα δημόσια σχολεία. Αναφορικά με τις πρόσθετες προαιρετικές σχολικές δράσεις, διευκρινίζεται στο ως άνω έγγραφο ότι για αυτές ακολουθείται η υφιστάμενη διαδικασία υποχρεωτικής ενημέρωσης της οικείας διεύθυνσης εκπαίδευσης. Στη συνέχεια, στις 07.10.2016, σύμφωνα με την υπό κρίση καταγγελία, όλα τα ιδιωτικά σχολεία έλαβαν από την Προϊσταμένη του Τμήματος Β΄ Ιδιωτικής Πρωτοβάθμιας Εκπαίδευσης του ΥΠΕΘ ηλεκτρονικό μήνυμα, με το οποίο κλήθηκαν να καταχωρίσουν τα στοιχεία λειτουργίας τους για το σχολικό έτος 2016-2017 σε μία ηλεκτρονική φόρμα ελεύθερου λογισμικού (Google Forms), στο κάτω μέρος της οποίας υπήρχε η επισήμανση να μην συμπληρωθεί ο κωδικός.

Στη συνέχεια ο ΣΙΣ με το με αριθμ. πρωτ. 260/24.10.2016 έγγραφό του προς την Προϊσταμένη του Τμήματος Ιδιωτικής Εκπαίδευσης του ΥΠΕΘ ζήτησε να ενημερωθεί, εάν το ΥΠΕΘ έχει συμμορφωθεί προς τις συστάσεις που είχε απευθύνει η ΑΠΔΠΧ με την απόφαση 139/2014, καθώς και για τους τρόπους επικοινωνίας του ΥΠΕΘ με τα σχολεία προκειμένου να μπορούν τα ιδιωτικά σχολεία να ενημερώνουν με ασφάλεια το ΥΠΕΘ σύμφωνα με την νομοθεσία που διέπει τις ασφαλείς ηλεκτρονικές συναλλαγές. Σε απάντηση του ως άνω εγγράφου αναφορικά με την νομιμότητα της υπό κρίση επεξεργασίας, το ΥΠΕΘ ενημέρωσε τον ΣΙΣ ότι αυτή

ερείδεται στο π.δ. 114/2014 (Οργανόγραμμα ΥΠΕΘ) και το με αριθ. πρωτ. Φ8/145/97610/Δ2/14.6.2016 έγγραφο του ΥΠΕΘ (βλ. ανωτέρω).

Ο ΣΙΣ, θεωρώντας ότι η ως άνω απάντηση του ΥΠΕΘ περί νομιμότητας της υπό κρίση επεξεργασίας δεν ευσταθεί, καθώς, κατά τους ισχυρισμούς του, «*δεν βρίσκει το παραμικρό έρεισμα στον νόμο και παράλληλα εγκυμονεί μεγάλους κινδύνους ως προς την ασφάλεια των δεδομένων*» και «*το ΥΠΠΕΘ δεν έχει συμμορφωθεί στις συστάσεις που του απηύθυνε η Αρχή με την υπ' αριθμ. 139/2014 απόφασή της*», προσέφυγε με την υπό κρίση καταγγελία στην Αρχή.

Στο πλαίσιο εξέτασης της εν λόγω καταγγελίας, η Αρχή έστειλε το με αρ. πρωτ. Γ/ΕΞ/7646-1/01.12.2016 έγγραφο, με το οποίο γνωστοποίησε τόσο στο ΥΠΕΘ, ως υπεύθυνο επεξεργασίας, όσο και στο Ινστιτούτο Τεχνολογίας Υπολογιστών και Εκδόσεων «Διόφαντος» (εφεξής ΙΤΥΕ-Διόφαντος) ως εκτελούντα την επεξεργασία, την ως άνω καταγγελία και τους κάλεσε να υποβάλουν εγγράφως τις απόψεις τους και να διευκρινίσουν, ιδίως, α) τις διατάξεις, στις οποίες προβλέπεται η υποχρέωση καταχώρισης προσωπικών δεδομένων των μαθητών/γονέων-κηδεμόνων/εκπαιδευτικών των ιδιωτικών σχολείων στο σύστημα «mySchool», β) ζητήματα που αφορούν στην ασφάλεια της ως άνω επεξεργασίας, περιλαμβανομένου του ζητήματος ασφάλειας του πιστοποιητικού SSL του διαδικτυακού τόπου sso.sch.gr, της πρόσβασης των ιδιωτικών σχολείων στο ως άνω σύστημα εκτός IP διευθύνσεων του Πανελλήνιου Σχολικού Δικτύου (ΠΣΔ), καθώς και της εφαρμογής των συστάσεων β, γ, δ, στ, η, θ του σημείου 6 της απόφασης 139/2014 σε συνδυασμό με το εγχειρίδιο χρήσης πύλης «mySchool», που είναι αναρτημένο στην κεντρική σελίδα του εν λόγω συστήματος με ημερομηνία 01.9.2014.

Στη συνέχεια το ΥΠΕΘ κοινοποίησε στην Αρχή το με αριθμ. πρωτ. Γ/ΕΙΣ/8365/19.12.2016 έγγραφο, με το οποίο καλούσε το ΙΤΥΕ-Διόφαντος να απαντήσει στο β) ερώτημα του ως άνω εγγράφου της Αρχής. Με το με αριθμ. πρωτ. Γ/ΕΙΣ/8494/23.12.2016 ηλεκτρονικό μήνυμα της Γραμματείας Ηλεκτρονικής Διεύθυνσης, διαβιβάστηκε το με αριθμ. πρωτ. 219178/Α3/21.12.2016 έγγραφο του Τμήματος Α' – Ψηφιακού Σχεδιασμού και Ανάπτυξης Εφαρμογών Α/θμιας και Β/θμιας Εκπαίδευσης του ΥΠΕΘ, στο οποίο αναφερόταν ότι η εν λόγω διεύθυνση «*δεν έχει καμία εμπλοκή στη σχεδίαση, την ανάπτυξη και τη λειτουργία του Πληροφοριακού συστήματος «mySchool»*.

Ακολούθως, και δεδομένου ότι η Αρχή δεν έλαβε απάντηση στο ως άνω έγγραφό της, απέστειλε εκ νέου το με αριθμ. πρωτ. Γ/ΕΞ/1060/10.2.2017 έγγραφο, με το οποίο επεσήμανε τόσο προς το ΥΠΕΘ, όσο και προς το ΙΤΥΕ-Διόφαντος, ότι σε περίπτωση που δεν ελάμβανε απάντηση θα προχωρούσε στην άσκηση των εκ του νόμου αρμοδιοτήτων της.

Σε απάντηση του τελευταίου ως άνω εγγράφου της Αρχής, το ΙΤΥΕ-Διόφαντος απέστειλε το με αριθμ. πρωτ. Γ/ΕΙΣ/1074/10.2.2017 ηλεκτρονικό μήνυμα, με το οποίο διαβίβασε στην Αρχή έγγραφό του προς το ΥΠΕΘ, το οποίο περιείχε απαντήσεις στο αρχικό με αριθμ. πρωτ. Γ/ΕΙΣ/7646/23.11.2016 έγγραφο της Αρχής και το οποίο, σύμφωνα με το ΙΤΥΕ-Διόφαντος, το ΥΠΕΘ όφειλε να έχει ενσωματώσει στη δική του απάντηση προς την Αρχή.

Κατόπιν τούτων, και κυρίως για τον λόγο ότι η Αρχή δεν έλαβε σε εύλογο χρονικό διάστημα κάποια απάντηση από το ΥΠΕΘ στα ως άνω έγγραφά της, κάλεσε το ΥΠΕΘ, ως υπεύθυνο επεξεργασίας, το ΙΤΥΕ-Διόφαντος, ως εκτελούντα την επεξεργασία καθώς και τον καταγγέλλοντα ΣΙΣ, να παραστούν στη συνεδρίαση της Ολομέλειας της Αρχής την Πέμπτη 16-3-2017, για τη συζήτηση της υπό κρίση καταγγελίας του ΣΙΣ (αντίστοιχοι αριθμ. πρωτ. κλήσεων Γ/ΕΞ/1721/02.3.2017, Γ/ΕΞ/1722/02.3.2017, Γ/ΕΞ/1725/02.3.2017).

Στη συνέχεια, το Τμήμα Β΄ Ιδιωτικής Εκπαίδευσης Δευτεροβάθμιας και Πρωτοβάθμιας Εκπαίδευσης του ΥΠΕΘ απέστειλε στην Αρχή το με αριθμ. πρωτ. 40496/ΓΔ4/09.3.2017 (αριθμ. πρωτ. της Αρχής Γ/ΕΙΣ/1964/10.3.2017) απαντητικό έγγραφο αναφερόμενο στο πρώτο διευκρινιστικό έγγραφο της Αρχής, χωρίς να κάνει μνεία στο δεύτερο και τελευταίο έγγραφο της Αρχής. Με το ως άνω έγγραφο, το ΥΠΕΘ έδωσε τις ακόλουθες διευκρινίσεις: α) τα ιδιωτικά σχολεία δεν μπορούν να αντιμετωπίζονται ως επιχειρήσεις που λειτουργούν με όρους ελεύθερης οικονομίας, αλλά υπόκεινται στην εποπτεία του ΥΠΕΘ σύμφωνα με το άρθρο 16 του Συντάγματος και τον Ν. 682/1977 που αναφέρεται στην ιδιωτική εκπαίδευση, β) οι διατάξεις του Ν. 1566/1985, σύμφωνα με το άρθρο 62 παρ. 7 αυτού, εφαρμόζονται αναλογικά και στα ιδιωτικά σχολεία προκειμένου να υπάρχει εναρμόνιση μεταξύ των δύο μορφών εκπαίδευσης (δημόσιας και ιδιωτικής), γ) από τις υπάρχουσες διατάξεις δεν προβλέπεται εξαίρεση καταχώρησης των στοιχείων των μαθητών και εκπαιδευτικών ιδιωτικών σχολείων Α΄ βάθμιας και Β΄ βάθμιας εκπαίδευσης. Στο έγγραφο αυτό ενσωματώθηκε η απάντηση του ΙΤΥΕ-Διόφαντος

(Γ/ΕΙΣ/1074/10.2.2017) σχετικά με τα ζητήματα που αφορούν την ασφάλεια της επεξεργασίας μέσω του συστήματος «mySchool».

Στην από 16-3-2017 συνεδρίαση της Ολομέλειας της Αρχής παρέστησαν νομίμως, εξέθεσαν τις απόψεις τους και απάντησαν σε ερωτήσεις των μελών της Αρχής οι εκπρόσωποι του ΥΠΕΘ Α, Προϊσταμένη Γενικής Διεύθυνσης Σπουδών, η Β, Γενική Διευθύντρια Προσωπικού Πρωτοβάθμιας και Δευτεροβάθμιας Εκπαίδευσης και η Γ, Προϊσταμένη Τμήματος Ιδιωτικών Σχολείων Πρωτοβάθμιας Εκπαίδευσης, οι εκπρόσωποι του ΣΙΣ, Δ, μέλος του διοικητικού συμβουλίου, ο Ε, σύμβουλος του ΣΙΣ και συνεργάτης σε θέματα πληροφορικής και ο Γρηγόριος Λαζαράκος, πληρεξούσιος δικηγόρος, καθώς και οι εκπρόσωποι του ΙΤΥΕ-Διόφαντος ΣΤ, τεχνικός, υπεύθυνος του συστήματος «mySchool» και ο Ζ, προϊστάμενος τμήματος Τ1 της Διεύθυνσης Εκπαιδευτικής Τεχνολογίας. Επιπλέον, το ΥΠΕΘ και ο ΣΙΣ κατέθεσαν τα υπ' αριθμ. πρωτ. Γ/ΕΙΣ/2664/29-3-2017 και Γ/ΕΙΣ/2665/29-3-2017 υπομνήματα, αντίστοιχα.

Στη συνέχεια, η Αρχή, με το από 27/4/2017 ηλεκτρονικό μήνυμα, προσκάλεσε το ΙΤΥΕ-Διόφαντος σε συνάντηση στην έδρα της με σκοπό την παρουσίαση της λειτουργίας του συστήματος «mySchool» στις βοηθούς εισηγήτριες. Το ΙΤΥΕ-Διόφαντος αποδέχθηκε την πρόσκληση αυτή (αριθμ. πρωτ. Γ/ΕΙΣ/3504/28-04-2017) και στη συνάντηση, η οποία πραγματοποιήθηκε στις 3-5-2017, έγινε παρουσίαση του συστήματος «mySchool» σε δοκιμαστικό περιβάλλον από τους εκπροσώπους του ΙΤΥΕ-Διόφαντος ΣΤ και Ζ, οι οποίοι παρείχαν διευκρινίσεις στις ερωτήσεις των βοηθών εισηγητριών που υποβλήθηκαν κατά την παρουσίαση. Περαιτέρω διευκρινίσεις σχετικά με τα μέτρα ασφάλειας του συστήματος «mySchool» προσκομίστηκαν στην Αρχή από το ΙΤΥΕ-Διόφαντος με το από 02/5/2017 ηλεκτρονικό μήνυμα (αριθ. πρωτ. Γ/ΕΙΣ/3511/02-05-2017). Επίσης, με το από 04-5-2017 ηλεκτρονικό μήνυμα ζητήθηκε από το ΙΤΥΕ-Διόφαντος να στείλει στην Αρχή τις «οθόνες» και τα δεδομένα που καταχωρούνται στο σύστημα «mySchool» για τις πανελλήνιες εξετάσεις πριν και μετά την αλλαγή του τρόπου διεξαγωγής τους, καθώς και τις «οθόνες» που αφορούν τα στοιχεία των εκπαιδευτικών των ιδιωτικών σχολείων. Το ΙΤΥΕ-Διόφαντος προσκόμισε τα παραπάνω στοιχεία με το από 04-5-2017 ηλεκτρονικό μήνυμα (αριθμ. πρωτ. Γ/ΕΙΣ/3637/05-5-2017).

Η Αρχή συνεδρίασε στις 20/6/2017 για να συζητήσει την εν λόγω υπόθεση και έκρινε αναγκαίο να προσκομισθούν επιπλέον στοιχεία αναφορικά με τη συλλογή

δεδομένων μαθητών-γονέων/κηδεμόνων και εκπαιδευτικών των ιδιωτικών σχολείων. Κατόπιν τούτου, η Αρχή, ζήτησε από το ΙΤΥΕ-Διόφαντος, με το από 20/6/2017 ηλεκτρονικό μήνυμα, να προσκομίσει κατάσταση με το είδος όλων των δεδομένων που τηρούνται στο σύστημα «mySchool» και αφορούν μαθητές-γονείς/κηδεμόνες και εκπαιδευτικούς. Το ΙΤΥΕ-Διόφαντος προσκόμισε τα ζητηθέντα στοιχεία στην Αρχή με το από 21/6/2017 ηλεκτρονικό μήνυμα. Στη συνέχεια, η Αρχή έστειλε το με αριθμ. πρωτ. Γ/ΕΞ/4865/23-6-2017 έγγραφο, με το οποίο ζήτησε από το ΥΠΕΘ και τον ΣΙΣ να προσκομίσουν συμπληρωμένες δύο καταστάσεις (excel αρχείο με δύο φύλλα), οι οποίες περιλάμβαναν το είδος των δεδομένων (στήλη Α), η μια των μαθητών-γονέων/κηδεμόνων (στο πρώτο φύλλο του excel αρχείου) και η άλλη των εκπαιδευτικών (στο δεύτερο φύλλο του excel αρχείο). Για καθένα εκ των δεδομένων των μαθητών-γονέων/κηδεμόνων και των εκπαιδευτικών ζητήθηκε η συμπλήρωση τεσσάρων στηλών (Β-Ε). Ειδικότερα, στα πεδία της στήλης Β ζητήθηκε να συμπληρωθεί «ΝΑΙ», αν το αντίστοιχο δεδομένο της στήλης Α διαβιβάζονταν στο ΥΠΕΘ από τα ιδιωτικά σχολεία πριν το σύστημα «mySchool» και «ΟΧΙ» στην αντίθετη περίπτωση. Στα πεδία της στήλης Γ ζητήθηκε να συμπληρωθεί «ΝΑΙ», αν είχε ζητήθηκε από το ΥΠΕΘ να καταχωρείται στο σύστημα «mySchool» από τα ιδιωτικά σχολεία το αντίστοιχο δεδομένο της στήλης Α και «ΟΧΙ» στην αντίθετη περίπτωση. Στα πεδία της στήλης Δ ζητήθηκε να συμπληρωθεί ποια δεδομένα θεωρούσαν αφενός το ΥΠΕΘ και αφετέρου ο ΣΙΣ, απαραίτητα, κατά την κρίση τους, για την άσκηση της εποπτικής αρμοδιότητας του ΥΠΕΘ, όπως προβλέπεται στην κείμενη νομοθεσία (ιδίως ν.682/1977, ν.4452/2017, π.δ. 114/2014), σε σχέση και με την απόδοση ενιαίου αριθμού μαθητή και τη διεξαγωγή των πανελλήνιων εξετάσεων. Στα πεδία της στήλης Ε ζητήθηκε να αιτιολογήσουν, κατά την κρίση τους, ποια δεδομένα θεωρούν ότι δεν είναι απαραίτητα για την εποπτική αρμοδιότητα του ΥΠΕΘ, όπως προβλέπεται στην κείμενη νομοθεσία, σε σχέση και με την απόδοση ενιαίου αριθμού μαθητή και τη διεξαγωγή των πανελλήνιων εξετάσεων. Το ΥΠΕΘ απάντησε στην Αρχή με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/5232/10-07-2017 έγγραφο και ο ΣΙΣ με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/5212/07-07-2017 έγγραφο.

Εν συνεχεία, η Αρχή έστειλε το υπ' αριθμ. πρωτ. Γ/ΕΞ/5399/14-07-2017 έγγραφο, με το οποίο ζήτησε από το ΥΠΕΘ να τεκμηριώσει ειδικώς, με επίκληση τυχόν υφιστάμενων σχετικών διατάξεων της κείμενης νομοθεσίας, την αναγκαιότητα της καταχώρισης στο σύστημα «mySchool» (καθώς και την αναγκαιότητα της

πρόσβασης από τον οικείο Διευθυντή Εκπαίδευσης) για καθένα από τα προσωπικά δεδομένα μαθητών και εκπαιδευτικών (όπως παρατίθενται στην αντίστοιχη στήλη Α του excel αρχείου), τα οποία κρίνει ότι είναι πρόσφορα και αναγκαία για τον επιδιωκόμενο σκοπό της εποπτικής αρμοδιότητας των ιδιωτικών σχολείων, όπως κάθε φορά αυτός εξειδικεύεται (πχ. για την επικύρωση τίτλων σπουδών των ιδιωτικών σχολείων, για τον έλεγχο της παιδαγωγικής καταλληλόλητας του ωρολόγιου προγράμματος, για τη διεξαγωγή των πανελλήνιων εξετάσεων, τον έλεγχο του διδακτικού ωραρίου απασχόλησης, κλπ) και, γενικότερα, για την άσκηση των αρμοδιοτήτων του οικείου Διευθυντή Εκπαίδευσης. Το ΥΠΕΘ απάντησε στην Αρχή με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/5845/01-08-2017 έγγραφο.

Στη συνέχεια, παρατίθενται αναλυτικότερα τα ζητήματα σχετικά με τα μέτρα ασφάλειας του συστήματος «mySchool» βάσει των ως άνω εγγράφων των ΥΠΕΘ, ΙΤΥΕ-Διόφαντος και ΣΙΣ.

Στην υπό κρίση καταγγελία, ο ΣΙΣ ανέφερε ότι το ΥΠΕΘ δεν έχει συμμορφωθεί με τις συστάσεις υπό στοιχεία 6α και 6ζ που του απηύθυνε η Αρχή με την υπ' αριθμ. πρωτ. 139/2014 Απόφασή της αναφορικά με τα μέτρα ασφάλειας του συστήματος «mySchool».

Συγκεκριμένα, ο ΣΙΣ έθεσε το ζήτημα της μη συμμόρφωσης με τη σύσταση 6α της ως άνω απόφασης, σύμφωνα με την οποία το ΥΠΕΘ οφείλει *«(…) α) Να προβεί σε κρυπτογράφηση, σύμφωνα με τα διεθνώς αποδεκτά πρότυπα, κατ' ελάχιστον, των δεδομένων ταυτοποίησης των μαθητών και των γονέων-κηδεμόνων τους (καθώς και των δεδομένων ταυτοποίησης όλων των κατηγοριών υποκειμένων) που τηρούνται στη βάση δεδομένων του εν λόγω συστήματος (…)»*. Ο ΣΙΣ ισχυρίστηκε ότι δεν γνωρίζει, αν έχει ολοκληρωθεί η εν λόγω κρυπτογράφηση και έθεσε το ζήτημα της ασφάλειας του πιστοποιητικού TLS που χρησιμοποιείται για την κρυπτογράφηση των μεταδιδόμενων δεδομένων μεταξύ του ηλεκτρονικού υπολογιστή/φυλλομετρητή του χρήστη και του κεντρικού διακομιστή του συστήματος «mySchool». Σύμφωνα με τα καταγγελλόμενα, το πιστοποιητικό TLS του εν λόγω συστήματος είναι χαμηλής ασφάλειας, συγκρινόμενο με τα αντίστοιχα πιστοποιητικά της εφαρμογής ενός ιδιωτικού φορέα με υψηλό επίπεδο ασφάλειας (όπως ενδεικτικά η σχετική εφαρμογή μιας Τράπεζας). Ο ΣΙΣ προσκόμισε ενδεικτικά δύο αντίγραφα επισκοπήσεων ασφαλείας (security overviews), όπως παράγονται από τον φυλλομετρητή ιστού Chrome, εκ των οποίων η μια αφορά τον κεντρικό διαδικτυακό τόπο του συστήματος

«mySchool» και η άλλη τον διαδικτυακό τόπο της τράπεζας Eurobank ΑΕ. Στην προσκομισθείσα επισκόπηση ασφάλειας του τραπεζικού διαδικτυακού τόπου αναφέρονταν ο χαρακτηρισμός «ισχυρή κρυπτογράφηση» («strong cipher»), ενώ στην αντίστοιχη του διαδικτυακού τόπου του συστήματος «mySchool» αναφέρονταν «παλαιότερη υπηρεσία σύνδεσης» («obsolete connection service») και «παλαιότερη κρυπτογράφηση» («obsolete cipher»). Επίσης, ο ΣΙΣ ανέφερε ότι το taxisnet, σύμφωνα με πληροφορίες του τύπου, έχει αποφασίσει να υλοποιήσει αναβάθμιση των πρωτοκόλλων επικοινωνίας, με αποτέλεσμα να μην υποστηρίζονται πλέον λειτουργικά συστήματα, όπως τα Windows XP τα οποία ακόμα χρησιμοποιούν οι υπηρεσίες –κεντρικές και αποκεντρωμένες– του ΥΠΕΘ, (αλλά δεν υποστηρίζονται με νέες ενημερώσεις, γεγονός που τα καθιστά απροστάτευτα και επισφαλή).

Επιπλέον, σύμφωνα με την υπό κρίση καταγγελία, παρότι η Αρχή με την υπό στοιχεία 6ζ σύσταση της Απόφασης 139/2014 ζήτησε από το ΥΠΕΘ *«(…) ζ) Να μεριμνήσει ώστε το σύστημα να αποκλείει την πρόσβαση των χρηστών που προέρχονται από IP διευθύνσεις εκτός του Πανελλήνιου Σχολικού Δικτύου δεδομένου ότι η εφαρμογή επιτρέπει την πρόσβαση μόνο στους χρήστες που είναι πιστοποιημένοι από την Κεντρική Υπηρεσία Πιστοποίησης του Πανελλήνιου Σχολικού Δικτύου και το ΥΠΑΙΘ δεν τεκμηριώνει καθόλου για ποιο λόγο επιτρέπεται η πρόσβαση από όλες τις ελληνικές IP διευθύνσεις, γεγονός που αυξάνει τον κίνδυνο διαδικτυακών επιθέσεων. (…)»*, σε κανένα ιδιωτικό σχολείο δεν έχει εγκατασταθεί, από την αρμόδια αρχή, διεύθυνση IP του ΠΣΔ, με αποτέλεσμα να μην τηρείται η ως άνω σύσταση της Αρχής.

Το ΥΠΕΘ, ως υπεύθυνος επεξεργασίας και το ΙΤΥΕ-Διόφαντος, ως εκτελών την επεξεργασία, ενημέρωσαν την Αρχή σχετικά με τα ζητήματα που έθεσε ο ΣΙΣ για τα μέτρα ασφάλειας του συστήματος «mySchool», ως εξής:

Στην Απόφαση 139/2014 της Αρχής, δεν αναδείχτηκαν «κενά ασφαλείας» της κεντρικής βάσης δεδομένων του συστήματος «mySchool». Η Αρχή από το θεσμικό της ρόλο προέβη σε συστάσεις, κυρίως, αναφορικά με την ενίσχυση της ασφαλούς χρήσης της εφαρμογής, ώστε μόνο εξουσιοδοτημένοι χρήστες να έχουν πρόσβαση στο ονοματεπώνυμο, μητρώο, τάξη και στοιχεία γονέων/κηδεμόνων των μαθητών, και την επιβεβαίωση της μη πρόσβασης χρηστών εκτός σχολείου στα στοιχεία αυτά, ενώ επιπλέον έγιναν συστάσεις για την υιοθέτηση διαδικασιών ελεγχόμενης πρόσβασης.

Ως προς το ζήτημα της ασφάλειας του πιστοποιητικού TLS το ΥΠΕΘ ανέφερε ότι η πρόσβαση στο σύστημα «mySchool» γίνεται με την αυθεντικοποίηση του χρήστη μέσω της διεπαφής εισαγωγής του κωδικού στο κεντρικό σύστημα πιστοποίησης/εξουσιοδότησης (https://sso.sch.gr) και στο σύστημα αλλαγής του κωδικού πρόσβασης (https://register.sch.gr/password). Σχετικά με τη Διαχείριση και Ασφάλεια Λογαριασμών στο διαδικτυακό τόπο https://sso.sch.gr διατίθενται οδηγίες ασφαλούς χρήσης (https://sso.sch.gr/safetyInfo.jsp). Με συχνότητα τουλάχιστον δύο φορές το χρόνο, υπάρχει ενημέρωση των χρηστών από την υπηρεσία «Single Sign On» - SSO του ΠΣΔ σε σχέση με τον κωδικό πρόσβασης και την ασφάλειά του.

Το πιστοποιητικό TLS του διαδικτυακού τόπου https://sso.sch.gr είναι RSA 2048 bits (signature algorithm SHA256withRSA) και έχει εκδοθεί από την TERENA Certificate Authority. Κάποιες εφαρμογές απαιτείται να εξυπηρετούν και παλαιότερους φυλλομετρητές, οι οποίοι είναι ενσωματωμένοι σε παλαιά λειτουργικά συστήματα και για αυτό το λόγο υποστηρίζονται τα αντίστοιχα chiphers ή παλαιότερα πρωτόκολλα. Σε αυτό οφείλεται ο χαρακτηρισμός περί «obsolete cipher» στις επιλογές ασφαλείας (security options) του φυλλομετρητή Chrome, ενώ αν υπήρχε πρόβλημα θα παρουσιάζονταν μήνυμα ελλιπούς ή μειωμένης ασφάλειας.

Τα αντίστοιχα πιστοποιητικά TLS των διαδικτυακών τόπων τραπεζικών οργανισμών όπως www.nbg.gr, www.alpha.gr/e-banking/en και www.winbank.gr/sites/idiwtes/el/Pages/default.aspx είναι RSA 2048 bits (signature algorithm SHA256withRSA) όμοια με του sso.sch.gr. Επιπλέον, το TLS certificate του συστήματος «mySchool» μετά την αυθεντικοποίηση του χρήστη είναι και αυτό RSA 2048 bits (signature algorithm SHA256withRSA) και κατηγοριοποιείται ως Α', από γνωστούς ιστότοπους αποτίμησης επιπέδων ασφάλειας εξυπηρετητών διαδικτυακών εφαρμογών. Τα χαρακτηρισμένα από τις τελευταίες εκδόσεις του chrome των πιστοποιητικών TLS ως obsolete ciphers σε καμία περίπτωση δεν σημαίνει πως είναι ασθενή ή δημιουργούν θέματα ελλιπούς ασφάλειας. Απλά έχουν υλοποιηθεί νεότερες μέθοδοι δημιουργίας cipher (χαρακτηρίζονται «modern»).

Το ΥΠΕΘ και το ΙΤΥΕ-Διόφαντος προσκόμισαν με το με αριθμ. πρωτ. Γ/ΕΙΣ/1964/10-3-2017 έγγραφο αντίγραφα των επισκοπήσεων ασφαλείας διαδικτυακών τόπων e-banking τραπεζικών οργανισμών (π.χ. https://ibankretail.nbg.gr (Εθνική), www.alpha.gr/e-banking (Alpha), https://www.winbank.gr/sites/idiwtes/el/Pages/default.aspx (Πειραιώς)), καθώς και

της ΓΓΠΣ (https://login.gsis.gr/mylogin/pages/login.jsp), από τις οποίες φαίνεται ότι οι εν λόγω διαδικτυακοί τόποι είχαν τον ίδιο χαρακτηρισμό από τον φυλλομετρητή chrome (με αυτόν του συστήματος «mySchool») για χρήση «obsolete ciphers».

Ενόψει των ανωτέρω, σύμφωνα με το ΥΠΕΘ και το ΙΤΥΕ-Διόφαντος, ο ισχυρισμός που αναφέρεται στην καταγγελία του ΣΙΣ περί ελλιπούς ασφάλειας του συστήματος «mySchool» δεν ανταποκρίνεται στην πραγματικότητα.

Ως προς το ζήτημα της πρόσβασης στο σύστημα «mySchool» εκτός IP διευθύνσεων του ΠΣΔ, το ΥΠΕΘ και το ΙΤΥΕ-Διόφαντος ανέφεραν τα ακόλουθα:

Η πρόσβαση αποκλειστικά εντός ΠΣΔ δεν μπορεί να είναι ρεαλιστική επιλογή για το σύστημα «mySchool». Το σύνολο των χρηστών αξιοποιεί το εργαλείο, συχνά και σε μη εργάσιμες ώρες. Επιπλέον, οι χρήστες της Κεντρικής Υπηρεσίας του ΥΠΕΘ, οι χρήστες του Ινστιτούτου Εκπαιδευτικής Πολιτικής (ΙΕΠ), καθώς και όλα τα ιδιωτικά σχολεία δεν έχουν πρόσβαση στο ΠΣΔ.

Η υποδομή του συστήματος παραμένει ασφαλής σε κακόβουλες επιθέσεις με τη βοήθεια πιστοποιητικών, συστημάτων παρακολούθησης και αποτροπής επιθέσεων καθώς και συστημάτων τείχους προστασίας (firewall), η δε πρόσβαση σε αυτό επιτρέπεται μόνο σε ελληνικές IP διευθύνσεις.

Πρόσβαση στο σύστημα «mySchool» διαθέτουν όλες οι μονάδες της τυπικής Α΄βάθμιας και Β΄βάθμιας εκπαίδευσης και όλες οι διοικητικές δομές της εκπαίδευσης. Επιπλέον, έχουν αποδοθεί και ατομικοί λογαριασμοί πρόσβασης σε χρήστες της κεντρικής υπηρεσίας του ΥΠΕΘ, καθώς και στο Ινστιτούτο Εκπαιδευτικής Πολιτικής. Πρόσβαση θα αποκτήσουν και οι σχολές μη τυπικής εκπαίδευσης του ΥΠΕΘ για την αξιοποίηση του συστήματος ως μηχανογραφικού εργαλείου καθημερινής λειτουργίας. Ακόμα, αξιοποιώντας το ρόλο του υπεύθυνου τμήματος πρόσβαση έχουν και περίπου 30.000 εκπαιδευτικοί με τους ατομικούς λογαριασμούς, όπως αυτοί εκδόθηκαν και συντηρούνται από το ΠΣΔ. Οι χρήστες του συστήματος «mySchool» διαθέτουν λογαριασμό στο ΠΣΔ, το οποίο έχει την διαχείριση των λογαριασμών αυτών. Οι κωδικοί για την πρόσβαση των χρηστών στο σύστημα κρυπτογραφούνται από το ΠΣΔ.

Η χρήση του συστήματος «mySchool» από τα ιδιωτικά σχολεία, κατά την εξέταση της υπό κρίση υπόθεσης, αναλύεται ως εξής:

Τύπος	Ποσοστό χρήσης συστήματος (μαθητές)	Ποσοστό χρήσης συστήματος (εκπαιδευτικοί)
Ιδιωτικό Γυμνάσιο	80.5%	61%
Ιδιωτικό Γυμνάσιο με Τάξεις Λυκείου	100.0%	100%
Ιδιωτικό Δημοτικό Σχολείο	80.8%	54%
Ιδιωτικό Εσπερινό Λύκειο	100.0%	100%
Ιδιωτικό Ημερήσιο ΕΠΑΛ	100.0%	100%
Ιδιωτικό Λύκειο	98.9%	74%
Ιδιωτικό Νηπιαγωγείο	68.6%	47%

Επίσης, το σύστημα «mySchool» ενσωματώνει τις μηχανογραφικές λειτουργίες για την υποστήριξη των πανελλήνιων εξετάσεων σε επίπεδο σχολικών μονάδων και ΥΠΕΘ. Ακόμα λαμβάνει στοιχεία από το σύστημα ΟΠΣΕΔ του Εθνικού Δημοτολογίου (ΥΠΕΣ) με βάση την ΚΥΑ 1493/2016 ως αποτέλεσμα της κατάργησης της έντυπης προσκόμισης των πιστοποιητικών γέννησης των μαθητών. Επίσης, παρέχει τα στατιστικά στοιχεία που ζητούνται από την ΕΛΣΤΑΤ για κάθε σχολικό έτος.

Η χρήση του συστήματος «mySchool» γίνεται και εκτός τυπικού ωραρίου, καθώς οι δυνατότητες που δίνει το σύστημα για τη μηχανογραφική υποστήριξη των δομών είναι τέτοιες που καθιστούν την αποδοχή και την αξιοποίησή του καθολική. Συχνά δεν καθίσταται εφικτό, το διοικητικό έργο να ολοκληρωθεί εντός του τυπικού ωραρίου των εκπαιδευτικών. Επιπλέον, παράγοντας που δεν επιτρέπει τη διαπεραίωση όλων των μηχανογραφικών εργασιών κατά τη διάρκεια του τυπικού ωραρίου αποτελεί το γεγονός πως δεν υπάρχουν οι απαραίτητοι σταθμοί εργασίας στο γραφείο των καθηγητών (π.χ. για κάθε έναν υπεύθυνο τμήματος) και σε πολλές περιπτώσεις ούτε καν ένας υπολογιστής. Ενόψει αυτού, σε κάθε ενημερωτική συνάντηση εκπαιδευτικών, στην οποία παρευρέθηκε το ΙΤΥΕ-Διόφαντος, το αίτημα πρόσβασης στο σύστημα εκτός ωραρίου εργασίας ήταν καθολικό. Τα αιτήματα προέκυψαν κατά τις ημερίδες παρουσίασης του συστήματος το 2014 σε όλες τις Περιφέρειες της χώρας παρουσία όλων των διευθυντών σχολικών μονάδων, ενώ καταγράφονται και σε ηλεκτρονικά δελτία της ίδιας περιόδου. Οι λόγοι συνοψίζονται στην μερική ανεπάρκεια της υποδομής του ΠΣΔ σε μερικές περιπτώσεις να

ανταποκριθεί στην αποτελεσματική κάλυψη δικτυακών αναγκών των σχολικών μονάδων.

Με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/2665/29-3-2017 υπόμνημά του, το οποίο κατέθεσε στην Αρχή σε συνέχεια της από 16-3-2017 κλήσης σε ακρόαση, ο ΣΙΣ έθεσε, επιπλέον των ζητημάτων που προαναφέρθηκαν, τα κάτωθι ζητήματα σχετικά με την ασφάλεια του συστήματος «mySchool». Ειδικότερα:

1) Σχετικά με την αυθεντικοποίηση των χρηστών αναφέρονται τα εξής, συνοπτικώς παρατιθέμενα:

Το επίπεδο αυθεντικοποίησης του συστήματος «mySchool» δεν είναι τόσο ισχυρό όσο απαιτεί το επίπεδο εμπιστοσύνης αυτού. Οι ηλεκτρονικές υπηρεσίες του συστήματος επεξεργάζονται «απλά» δεδομένα και δεδομένα ειδικών κατηγοριών και, κατά συνέπεια, εντάσσονται στο ανώτατο επίπεδο εμπιστοσύνης, στο επίπεδο 3.

Η αυθεντικοποίηση του συστήματος «mySchool» είναι μικρής ή μέτριας βεβαιότητας για την ορθότητα της ψηφιακής ταυτότητας του χρήστη. Το σύστημα χρησιμοποιεί για την αυθεντικοποίηση συνθηματικό (password), γεγονός που το κατατάσσει στο επίπεδο αυθεντικοποίησης 1 (μικρή ή μέτρια βεβαιότητα για την ορθότητα της ψηφιακής ταυτότητας ενός χρήστη). Τα διεθνή πρότυπα ασφαλείας ορίζουν ότι για τα συστήματα, τα οποία επεξεργάζονται «απλά» και δεδομένα ειδικών κατηγοριών και στα οποία μόνο εξουσιοδοτημένα πρόσωπα έχουν τη δυνατότητα πρόσβασης στις προσφερόμενες υπηρεσίες, απαιτείται υψηλή βεβαιότητα για την ορθότητα της ψηφιακής ταυτότητας του χρήστη. Αυτό σημαίνει ότι ο μηχανισμός αυθεντικοποίησης θα έπρεπε να αξιοποιεί τεχνολογία δύο παραγόντων (two-factor authentication) και συγκεκριμένα ψηφιακών πιστοποιητικών ή αξιοποίηση διακριτικών χαλαρής ή σκληρής αποθήκευσης αντί της χρήσης αυθεντικοποίησης με ένα απλό συνθηματικό που επιλέχθηκε για το σύστημα «mySchool».

Το γεγονός ότι καταχωρείται στο σύστημα «mySchool» πολύ μεγάλος αριθμός προσωπικών δεδομένων και ότι επιτρέπεται η πρόσβαση πολλών χιλιάδων δημοσίων υπαλλήλων, οι οποίοι βρίσκονται γεωγραφικά διάσπαρτοι και έχουν πρόσβαση ακόμα και από internet cafe ή το σπίτι τους, η δε πρόσβαση αυτή επιτρέπεται από ενδεχομένως ευάλωτους σε επίθεση τερματικούς σταθμούς, καθιστά απολύτως απαραίτητο να υπάρχει και δεύτερος βαθμός ασφαλείας (2nd factor authentication).

Επίσης, γίνεται αναφορά στη σύσταση 6β της απόφασης 139/2014 της ΑΠΔΠΧ, σύμφωνα με την οποία το ΥΠΕΘ οφείλει *«(…) να μεριμνήσει, ώστε να περιληφθεί στο σύστημα δυνατότητα δημιουργίας ατομικών λογαριασμών χρηστών που να αποδίδονται σε κατάλληλα εξουσιοδοτημένους εκπαιδευτικούς της κάθε σχολικής μονάδας και υπαλλήλους της κάθε διοικητικής δομής όπως διεύθυνση ή περιφερειακή διεύθυνση, ώστε να αποφευχθεί τυχόν κοινή χρήση του μοναδικού λογαριασμού που αποδίδεται στον διευθυντή της σχολικής μονάδας ή της διοικητικής δομής για την διεκπεραίωση όλων των εργασιών που απαιτούνται στο πλαίσιο του συστήματος «mySchool» (…)»*. Για την σύσταση αυτή αναφέρεται από τον ΣΙΣ ότι είναι γνωστό σε όλη την εκπαιδευτική κοινότητα ότι το «mySchool» χρησιμοποιείται από τουλάχιστον τρεις (3) υπαλλήλους κάθε Διεύθυνσης Εκπαίδευσης ή κάθε Περιφερειακής Διεύθυνσης, εκτός από τον υπεύθυνο Διευθυντή. Το αποτέλεσμα είναι ότι όλοι οι ανωτέρω υπάλληλοι μπορεί να μοιράζονται το username και το password του Διευθυντή έχοντας, μάλιστα, τη δυνατότητα πρόσβασης από το σπίτι τους και από πιθανόν μολυσμένους Η/Υ.

Επιπλέον, αναφέρεται ότι η διεπαφή εισόδου στο «mySchool» είναι ευάλωτη σε επιθέσεις, διότι δεν εφαρμόζεται CAPTCHA κατά την εισαγωγή των κωδικών, επιτρέπεται η αντιγραφή-επικόλληση (copy-paste) των κωδικών στα αντίστοιχα πεδία, επιτρέπεται η αποθήκευση του συνθηματικού από τον φυλλομετρητή, ενώ δίνεται απλά ως συμβουλή στους χρήστες «*Αποφεύγετε την αποθήκευση του συνθηματικού σας από τον φυλλομετρητή και προτιμήστε να τον πληκτρολογείτε εκ νέου κάθε φορά*» και δεν εφαρμόζεται κρυπτογράφηση στους κωδικούς.

2) Σχετικά με την Πολιτική Ασφαλείας του συστήματος «mySchool» αναφέρονται τα κάτωθι, συνοπτικώς παρατιθέμενα:

Το σύστημα «mySchool» δεν είναι κατάλληλα σχεδιασμένο για την αποτροπή απειλών κατά τη διαδικασία εγγραφής χρήστη, διότι α) η δημιουργία νέου λογαριασμού είναι ευάλωτη σε απειλές και δεν είναι ασφαλής, δεδομένου ότι δεν επαληθεύει την ταυτότητα του χρήστη (σελίδα 26 της Πολιτικής Ασφαλείας), β) η ανάκτηση των στοιχείων πρόσβασης λογαριασμού δεν είναι ασφαλής (σελίδα 30 της Πολιτικής Ασφαλείας), γ) η διαδικασία κατάργησης πρόσβασης χρήστη είναι λάθος σχεδιασμένη και ενέχει πολλούς κινδύνους ασφαλείας (σελίδα 31 της Πολιτικής Ασφαλείας).

Επίσης, το σύστημα «mySchool» δείχνει να είναι ευάλωτο σε πλήθος επιθέσεων, καθώς αυτές δεν έχουν προβλεφθεί από την Πολιτική Ασφαλείας. Η Πολιτική Ασφαλείας δεν αντιστοιχεί στο επίπεδο που απαιτεί το σύστημα «mySchool», δεν δείχνει να αναθεωρείται τακτικά, δεν είναι γνωστή στους χρήστες, δεν πραγματοποιούνται έλεγχοι της τήρησής της, δεν έχει προβλεφθεί διαδικασία διαχείρισης κινδύνου και δεν προβλέπονται περιοδικοί έλεγχοι τρωτότητας και παρείσδυσης και έχει βασικές ελλείψεις στο περιεχόμενο.

3) Σχετικά με επιπλέον ζητήματα για την 6ζ σύσταση της Απόφασης 139/2014 της ΑΠΔΠΧ αναφέρονται τα κάτωθι, συνοπτικώς παρατιθέμενα:

Η χρήση Η/Υ εκτός κλειστού δικτύου (ΠΣΔ) και, μάλιστα, από χώρους εκτός της υπηρεσιακής έδρας εγκυμονεί πολλούς κινδύνους για την υποκλοπή κωδικών και δεδομένων, ιδιαιτέρως σε ένα σύστημα που δεν προστατεύεται από ισχυρή αυθεντικοποίηση. Ενδεικτικά, αναφέρεται ότι το σύστημα δεν προστατεύεται από «ιούς», «δούρειους ίππους» και «σκουλήκια» (virus, trojan horses, worms) στους τοπικούς υπολογιστές από τους οποίους γίνεται η πρόσβαση και τους οποίους μπορεί να χρησιμοποιεί όλη η οικογένεια. Μπορεί να υπάρχει πρόσβαση και από internet cafe ή Η/Υ κάποιου φίλου, στον οποίο ο χρήστης παραλείπει να κάνει αποσύνδεση ή του οποίου το δίκτυο παρακολουθείται, από ελεύθερο wifi, από κινητά τηλέφωνο και ταμπλέτες ή από Η/Υ με παλιά λειτουργικά συστήματα windows XP, vista, τα οποία δεν υποστηρίζονται με νέες εκδόσεις ασφαλείας από την Microsoft. Τα αναφερόμενα από το ΙΤΥΕ-Διόφαντο μέτρα ασφαλείας, σύμφωνα με τον ΣΙΣ, δεν μπορούν να καλύψουν την υποκλοπή των αναγνωριστικών και συνθηματικών των παραπάνω περιπτώσεων με αποτέλεσμα ο κακόβουλος χρήστης να αποκτήσει πρόσβαση στα στοιχεία μαθητών και εκπαιδευτικών.

Όσον αφορά τη χρήση του συστήματος «mySchool» σε μη εργάσιμες ώρες και εκτός του τυπικού ωραρίου, ο ΣΙΣ ανέφερε ότι η ανωτέρω πρακτική αντιβαίνει στην εργατική νομοθεσία, καθώς συνεπάγεται ευθεία παραβίαση των νομοθετικών διατάξεων που έχουν θεσπιστεί για την προάσπιση των δικαιωμάτων των εργαζομένων και, κυρίως, τον αποκλεισμό φαινομένων εκμετάλλευσης του εργατικού δυναμικού. Επίσης, ανέφερε ότι είναι αυτονόητο ότι τα ιδιωτικά σχολεία δεν επιθυμούν να υιοθετήσουν παραβατική συμπεριφορά σε βάρος των εκπαιδευτικών και των μισθωτών των σχολείων, που έχουν προσληφθεί να παρέχουν τις υπηρεσίες με δεδομένο τρόπο και σε ορισμένο χρόνο και τόπο.

4) Σχετικά με άλλα μέτρα ασφάλειας του συστήματος «mySchool» αναφέρονται τα εξής, συνοπτικώς παρατιθέμενα:

Οι χρήστες του συστήματος δεν είναι εκπαιδευμένοι σε θέματα ασφάλειας. Οι ημερίδες και τα ηλεκτρονικά μηνύματα που αποστέλλονται δύο φορές το χρόνο στους χρήστες της υπηρεσίας SSO του ΠΣΔ σε σχέση με τον κωδικό πρόσβασης και την ασφάλεια του, αποτελούν τυπική και όχι ουσιαστική διαδικασία εκπαίδευσης των χρηστών. Οι χρήστες είναι εύκολο, λόγω ελλιπούς εκπαίδευσης, να πέσουν θύματα απάτης ("phishing") για την υποκλοπή των κωδικών.

Το σύστημα «mySchool» παρουσιάζει προβλήματα διαθεσιμότητας, διότι από τις 23.30 της 16-3-2017 και μέχρι το πρωί της επόμενης μέρας δεν λειτουργούσε.

Δεν παρέχεται δυνατότητα μαζικής εισαγωγής των δεδομένων από τα πληροφοριακά συστήματα των ιδιωτικών σχολείων στο σύστημα «mySchool» με αρχεία τύπου xml, παρότι, σύμφωνα με τον ΣΙΣ, κατά την ακροαματική διαδικασία ενώπιον της Αρχής αναφέρθηκε ότι υπάρχει η δυνατότητα αυτή. Ο ΣΙΣ απέστειλε στην Αρχή, προς απόδειξη, όπως αναφέρει, του ισχυρισμού του, το από 16.3.2017 μήνυμα ηλεκτρονικού ταχυδρομείου με επισυναπτόμενα screenshots και το εγχειρίδιο χρήσης του συστήματος «mySchool», σύμφωνα με τα οποία η μαζική εισαγωγή των στοιχείων των μαθητών γίνεται από excel αρχείο.

Σύμφωνα με τον ΣΙΣ, ερωτηματικά ως προς την ασφάλεια του συστήματος δημιουργεί η δυνατότητα αναζήτησης και εύρεσης όλων των στοιχείων ιδιωτικού εκπαιδευτικού, συμπεριλαμβανομένου και του ΑΚΜΑ αυτού, με μόνη την καταχώριση του ΑΦΜ του εκπαιδευτικού στο σύστημα αυτό. Τούτο προβλέπεται στο εγχειρίδιο χρήσης του «mySchool» και στα screenshots που εμπεριέχονται σε αυτό. Προς αντίκρουση ισχυρισμού ότι ο ΑΜΚΑ υπάρχει ως εικόνα στο εγχειρίδιο αλλά δεν λειτουργεί, ο εκπρόσωπος του ΣΙΣ απέστειλε στην Αρχή το από 16.3.2017 μήνυμα ηλεκτρονικού ταχυδρομείου με επισυναπτόμενα screenshots της εφαρμογής και με στοιχεία συγκεκριμένου εκπαιδευτικού, σύμφωνα με τα οποία εμφανίζεται και ο ΑΜΚΑ του.

Επίσης, σύμφωνα με τον ΣΙΣ, ερωτηματικά ως προς την ασφάλεια και προστασία των προσωπικών δεδομένων δημιουργεί η διασύνδεση της βάσης δεδομένων του συστήματος «mySchool» με τη βάση του Εθνικού Δημοτολογίου και, κυρίως, το γεγονός ότι οι χρήστες του συστήματος «mySchool» μπορούν να αναζητήσουν τα στοιχεία μαθητή στη βάση του Εθνικού Δημοτολογίου. Επιπλέον, ο

ΣΙΣ ανέφερε ότι ενημερώθηκε ότι τους κωδικούς της βάσης δεδομένων και της κρυπτογράφησης του συστήματος ««mySchool» έχει μόνο ένα πρόσωπο.

Περαιτέρω, στο ως άνω υπόμνημά του, ο ΣΙΣ υποστηρίζει ότι η Αρχή πρέπει να ζητήσει από τον υπεύθυνο επεξεργασίας να προβεί στην εκπόνηση μελέτης εκτίμησης αντικτύπου για την προστασία των προσωπικών δεδομένων του συστήματος «mySchool» κατά τα οριζόμενα στο άρθρο 35 του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΕΕ) 2016/679.

Η Αρχή, μετά από εξέταση όλων των στοιχείων του φακέλου, καθώς και των όσων αναφέρθηκαν κατά την ακροαματική διαδικασία, αφού άκουσε τους εισηγητές και τις βοηθούς εισηγήτριες, οι οποίες στη συνέχεια αποχώρησαν πριν από τη διάσκεψη και τη λήψη απόφασης, και κατόπιν διεξοδικής συζήτησης,

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Η ιδιωτική εκπαίδευση υπάγεται στην εποπτεία του Κράτους κατά το Σύνταγμα, στο άρθρο 16 παρ. 2 και 8 οποίου ορίζεται ότι «[…] 2. Η παιδεία αποτελεί βασική αποστολή του Κράτους και έχει σκοπό την ηθική, πνευματική, επαγγελματική και φυσική αγωγή των Ελλήνων, την ανάπτυξη της εθνικής και θρησκευτικής συνείδησης και τη διάπλασή τους σε ελεύθερους και υπεύθυνους πολίτες.[…]. 8. Νόμος ορίζει τις προϋποθέσεις και τους όρους χορήγησης άδειας για την ίδρυση και λειτουργία εκπαιδευτηρίων που δεν ανήκουν το Κράτος, τα σχετικά με την εποπτεία που ασκείται πάνω σε αυτά, καθώς και την υπηρεσιακή κατάσταση του διδακτικού προσωπικού τους.».
2. Το άρθρο 4 παρ. 1 του εφαρμοστέου στην εξεταζόμενη υπόθεση Ν.2472/1997 (Α΄ 50) ορίζει ότι «Τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει: α) Να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών. β) Να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της

επεξεργασίας. γ) Να είναι ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση. δ) […]».

3. Το άρθρο 10 παρ. 3 του Ν.2472/1997 ορίζει ότι «ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας.[…].» Η υποχρέωση αυτή βαρύνει αναλόγως και κάθε εκτελούντα την επεξεργασία, σύμφωνα με την παρ. 4 του ιδίου άρθρου.

4. Το άρθρο 1 του Ν. 682/1977 «Περί Ιδιωτικών Σχολείων Γενικής Εκπαιδεύσεως και Οικοτροφείων» (Α΄ 244), όπως ισχύει, ορίζει ότι «Ιδιωτικά σχολεία γενικής εκπαιδεύσεως, κατά την έννοιαν του παρόντος νόμου, είναι τα αντίστοιχα προς τα δημόσια σχολεία γενικής δημοτικής ή μέσης Εκπαιδεύσεως τα μη ανήκοντα εις το Κράτος, αλλά ιδρυόμενα και συντηρούμενα υπό φυσικών ή νομικών προσώπων, κατά τα ειδικώτερον εις τον παρόντα νόμον οριζόμενα.». Περαιτέρω, στο άρθρο 2 παρ. 1 και 5 ορίζεται ότι «1. Τα Ιδιωτικά σχολεία γενικής εκπαιδεύσεως υπάγονται εις την αρμοδιότητα του Υπουργείου Εθνικής Παιδείας και Θρησκευμάτων, ασκούντος την επ' αυτών εποπτείαν δια των περιφερειακών εποπτικών οργάνων. […] 5. Για την πειθαρχική ευθύνη και την εν γένει διαδικασία και κάθε άλλο σχετικό θέμα που αφορά την πειθαρχική δίωξη και ποινές για τους εκπαιδευτικούς των ιδιωτικών σχολείων γενικής εκπαίδευσης εφαρμόζονται αναλογικά οι διατάξεις του ν. 3528/2007.»[1].

5. Το άρθρο 62 παρ. 7 του Ν. 1566/1985 «Δομή και λειτουργία της πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης και άλλες διατάξεις» (Α΄ 167) προβλέπει ότι «Με την επιφύλαξη της παραγράφου 4 του άρθρου 52, οι διατάξεις αυτού του νόμου εφαρμόζονται ανάλογα στις ιδιωτικές σχολικές μονάδες της πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης και στο εκπαιδευτικό προσωπικό τους, εκτός από τις διατάξεις των περιπτώσεων Α΄, Β΄ και Γ΄ του άρθρου 11.»[2].

[1] Η παράγραφος 5 προστέθηκε με το άρθρο 41 του Ν. 4301/2014.

[2] Το άρθρο 52 καταργήθηκε με το άρθρο 3 της Υ. Α. ΣΤ.5/26 (Εσωτ. Οικ. Εθν. Παιδ.) της 4/5.10.88, Β΄732. Επιπλέον, κατά το άρθρο 110 παρ.1β Ν.4547/2018,ΦΕΚ Α 102/12.6.2018: "Με την επιφύλαξη του άρθρου 20 και ιδίως των παρ. 8, 9 και 12 έως και 15 του άρθρου αυτού, καταργείται κάθε διάταξη

6. Με το άρθρο 2 παρ. 2 περ. θ΄ του π.δ. 114/2014 «Οργανισμός Υπουργείου Παιδείας και Θρησκευμάτων», (Α΄ 181), όπως αυτό συμπληρώθηκε με τον πρόσφατο Ν. 4452/2017 (βλ. παρακάτω) ορίζεται «Αυτοτελής Διεύθυνση Ιδιωτικής Εκπαίδευσης». Με το άρθρο 40 του ίδιου ως άνω π.δ., όπως αυτό προστέθηκε από τον Ν.4452/2017, ορίζονται τα εξής: «1. Επιχειρησιακός στόχος της Αυτοτελούς Διεύθυνσης Ιδιωτικής Εκπαίδευσης είναι η εποπτεία των ιδιωτικών σχολείων πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης, η διασφάλιση της ποιότητας της παρεχόμενης εκπαίδευσης σε αυτά, ο χειρισμός θεμάτων του προσωπικού και των ιδιοκτητών αυτών, καθώς και η εποπτεία της λειτουργίας των ξένων σχολείων, των φροντιστηρίων και των κέντρων ξένων γλωσσών. 2. Η Αυτοτελής Διεύθυνση Ιδιωτικής Εκπαίδευσης υπάγεται απευθείας στον Γενικό Γραμματέα του Υπουργείου Παιδείας, Έρευνας και Θρησκευμάτων. 3. Η Αυτοτελής Διεύθυνση Ιδιωτικής Εκπαίδευσης συγκροτείται από τις ακόλουθες οργανικές μονάδες: α) Τμήμα Α΄ ιδιωτικών σχολείων πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης […]. 4. Το Τμήμα Α΄ ιδιωτικών σχολείων πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης είναι αρμόδιο για: α) την εποπτεία όλων των ιδιωτικών σχολείων πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης, β) τη χορήγηση, τροποποίηση, επικαιροποίηση, μεταβίβαση και ανάκληση της άδειας των ιδιωτικών σχολείων πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης, γ) κάθε θέμα σχετικό με την οργάνωση και λειτουργία των ιδιωτικών σχολείων πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης, και δ) το χειρισμό κάθε άλλου συναφούς θέματος. 5. Το Τμήμα Β΄ προσωπικού ιδιωτικών σχολείων πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης είναι αρμόδιο για: α) την εγγραφή στην Επετηρίδα, καθώς και την εποπτεία επί των θεμάτων υπηρεσιακής κατάστασης των ιδιωτικών εκπαιδευτικών πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης σύμφωνα με τις κείμενες διατάξεις, β) τις πειθαρχικές υποθέσεις των ιδιωτικών εκπαιδευτικών, καθώς και των ιδιοκτητών και νομίμων εκπροσώπων των ιδιωτικών σχολείων πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης, και γ) το χειρισμό κάθε άλλου συναφούς θέματος. […].».

7. Το άρθρο 41 παρ. 2 του Ν. 4301/2014 «Οργάνωση της νομικής μορφής των θρησκευτικών κοινοτήτων και των ενώσεων τους στην Ελλάδα και άλλες

που βρίσκεται σε αντίθεση προς τις διατάξεις του παρόντος και, ιδίως, οι εξής: α) […], β) τα Κεφάλαια Α έως και Γ` του άρθρου 11 […].

διατάξεις αρμοδιότητας Γενικής Γραμματείας Θρησκευμάτων και άλλες διατάξεις» (Α΄ 223) ορίζει ότι «[…] 2. Προστίθεται παράγραφος 5 στο άρθρο 2 του ν. 682/1977 ως ακολούθως: Για την πειθαρχική ευθύνη και την εν γένει διαδικασία και κάθε άλλο σχετικό θέμα που αφορά την πειθαρχική δίωξη και ποινές για τους εκπαιδευτικούς των ιδιωτικών σχολείων γενικής εκπαίδευσης εφαρμόζονται αναλογικά οι διατάξεις του ν. 3528/2007.».

8. Το άρθρο 41 παρ. 1 του Ν. 4351/2015 «Βοσκήσιμες γαίες Ελλάδας και άλλες διατάξεις» (Α΄ 164) προβλέπει αναφορικά με τους απολυτήριους τίτλους των ιδιωτικών σχολείων ότι «1. Η αληθής έννοια της διάταξης του δεύτερου εδαφίου της παρ. 5 του άρθρου 16 του ν. 3149/2003 (Α΄ 141) είναι ότι οι εκδιδόμενοι τίτλοι απόλυσης των μαθητών των ιδιωτικών σχολείων θεωρούνται από τον διευθυντή της οικείας διεύθυνσης δευτεροβάθμιας εκπαίδευσης, εκτός από τους απολυτήριους τίτλους απόλυσης των μαθητών που απονέμονται από τα αναγνωρισμένα ως ισότιμα προς τα δημόσια ιδιωτικά σχολεία πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης.».

9. Το άρθρο 7 παρ. 1 α΄ του Ν. 4452/2017 «Ρύθμιση θεμάτων του Κρατικού Πιστοποιητικού Γλωσσομάθειας, της Εθνικής Βιβλιοθήκης της Ελλάδας και άλλες διατάξεις» (Α΄ 17), όπως ισχύει, προβλέπει ότι «1. α) Καθιερώνεται Ενιαίος Αριθμός Εκπαίδευσης, ο οποίος εκδίδεται βάσει του Αριθμού Μητρώου Κοινωνικής Ασφάλισης, είναι αμετάβλητος για κάθε φυσικό πρόσωπο και διατηρείται και μετά την περάτωση των σπουδών. Ο Ενιαίος Αριθμός Εκπαίδευσης αποδίδεται με την κατά το πρώτον είσοδο του προσώπου σε οποιαδήποτε βαθμίδα εκπαίδευσης της ημεδαπής, δημόσιας ή ιδιωτικής. Ο Ενιαίος Αριθμός Εκπαίδευσης αντιστοιχεί σε σχετική εξατομικευμένη εγγραφή του οικείου πληροφοριακού συστήματος του Υπουργείου Παιδείας, Έρευνας και Θρησκευμάτων. β) […].»[3].

10. Στην υπ' αριθμ. ΚΥΑ 1493 (ΦΕΚ Β 298/12-02-2016) προβλέπεται διασύνδεση του Πληροφοριακού Συστήματος «mySchool» του Ινστιτούτου Τεχνολογίας Υπολογιστών και Εκδόσεων, (ΙΤΥΕ) «Διόφαντος», αρμοδιότητας ΥΠΕΘ, με την κεντρική βάση δεδομένων του Ολοκληρωμένου Πληροφοριακού Συστήματος Εθνικού Δημοτολογίου. Συγκεκριμένα, στις παρ. 1 και 2 του άρθρου μόνου της ως άνω ΚΥΑ προβλέπεται η πρόσβαση του ΙΤΥΕ-Διόφαντος, ως διαπιστευμένου

[3] Η παράγραφος 1 αντικαταστάθηκε ως άνω με το άρθρο 18 του Ν.4521/2018 (Α΄ 38).

φορέα, στην κεντρική βάση δεδομένων του ΟΠΣΕΔ Εθνικού Δημοτολογίου για την άσκηση αρμοδιοτήτων του ΥΠΕΘ, καθώς και η πρόσβαση του συστήματος «mySchool» στην ως άνω βάση αποκλειστικά για τη διεκπεραίωση των σχετικών εργασιών με την εγγραφή και παρακολούθηση των μαθητών σε Νηπιαγωγεία - Δημοτικά - Γυμνάσια - Λύκεια. Επίσης, στην παρ.3 του άρθρου μόνου της ως άνω ΚΥΑ ορίζεται ότι «(…) Οι απαραίτητες πληροφορίες για τη διεκπεραίωση των σχετικών εργασιών εγγραφής και παρακολούθησης των μαθητών στο Νηπιαγωγεία - Δημοτικά - Γυμνάσια - Λύκεια θα μεταφέρονται ψηφιακά από το ΟΠΣΕΔ στο Πληροφοριακό Σύστημα «my school» του ΙΤΥΕ «Διόφαντος» για το Υπουργείο Παιδείας, Έρευνας και Θρησκευμάτων (…)»). Επιπλέον, στην παρ. 4 ορίζεται ότι η διοίκηση του ΙΤΥΕ «Διόφαντος» πρέπει να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα ασφάλειας. Περαιτέρω, σύμφωνα με την παρ. 7, οι υπηρεσίες «που υπάγονται στις αρμοδιότητες του ΥΠΕΘ (αποκλειστικά: Νηπιαγωγεία - Δημοτικά - Γυμνάσια - Λύκεια)» και έχουν πρόσβαση στο «mySchool» αναζητούν τις απαιτούμενες πληροφορίες για τη διεκπεραίωση των διαδικασιών αρμοδιότητάς τους, μέσω του «mySchool», από το ΟΠΣΕΔ του Εθνικού δημοτολογίου και δεν επιτρέπεται να ζητούν από τους πολίτες να προβαίνουν στην προσκομιδή δικαιολογητικών στα οποία περιλαμβάνονται οι πληροφορίες που παρέχονται από το ΟΠΣΕΔ.

11. Ζητήματα ασφάλειας κατά την άσκηση αρμοδιοτήτων από τους φορείς του δημόσιου τομέα με χρήση ΤΠΕ, κατά την επικοινωνία και συναλλαγή μεταξύ των φορέων του δημοσίου τομέα με χρήση ΤΠΕ, ή μεταξύ των φορέων του δημοσίου τομέα και φυσικών ή νομικών προσώπων ιδιωτικού δικαίου, καθώς και ως προς την πρόσβαση φυσικών προσώπων ή νομικών προσώπων ιδιωτικού δικαίου σε δημόσια έγγραφα και τη διάθεσή τους για περαιτέρω χρήση με χρήση ΤΠΕ ρυθμίζονται στο ν. 3979/2011 (Α΄ 138) περί ηλεκτρονικής διακυβέρνησης (βλ. ιδίως άρθρο 2, άρθρο 3,- άρθρο 17 παρ. 1 και 3, άρθρο 21 παρ. 2, άρθρο 22 παρ. 1, άρθρο 32 παρ. 4).
12. Κατ' εξουσιοδότηση των άρθρων 27 του ν.3731/2008 (Α΄ 263) και 17 παρ. 3 και 21 παρ. 2 του ν.3979/2011 εκδόθηκε η υπ' αρ. ΥΑΠ/Φ.40.4/1/989 απόφαση του Υφυπουργού Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης, (ΦΕΚ Β΄ 1301/12.04.2012) με τίτλο «Κύρωση Πλαισίου Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης» (εφεξής ΠΠΥΗΔ). Ειδικότερα, στο ΠΠΥΗΔ

καθορίζονται οι κανόνες και τα πρότυπα για την εγγραφή, ταυτοποίηση και ηλεκτρονική αναγνώριση πολιτών σε ηλεκτρονικές υπηρεσίες του δημοσίου τομέα και συγκεκριμένα στο Παράρτημα ΙΙΙ αυτού (Πλαίσιο Ψηφιακής Αυθεντικοποίησης).

a. Σύμφωνα με το ΠΠΥΗΔ, οι προϋποθέσεις αυθεντικοποίησης των χρηστών καθορίζονται από το επίπεδο εμπιστοσύνης, στο οποίο εντάσσονται οι παρεχόμενες ηλεκτρονικές υπηρεσίες. Τα επίπεδα εμπιστοσύνης κατηγοριοποιούνται ανάλογα με το είδος των δεδομένων που αξιοποιούν (προσωπικά, ευαίσθητα και οικονομικά), αλλά και τις πιθανές επιπτώσεις που μπορεί να προκληθούν σε περίπτωση μη ορθής λειτουργίας ή διαχείρισής τους. Ειδικότερα, στο επίπεδο εμπιστοσύνης 2 εντάσσονται υπηρεσίες που απαιτούν ανταλλαγή προσωπικών δεδομένων, τα οποία δεν είναι ευαίσθητα, όπως για παράδειγμα, στοιχεία που αφορούν την οικογενειακή κατάσταση του χρήστη, ημερομηνία γέννησης, φύλο κτλ., ενώ στο επίπεδο εμπιστοσύνης 3 εντάσσονται είτε υπηρεσίες που απαιτούν ανταλλαγή ευαίσθητων δεδομένων, είτε υπηρεσίες ηλεκτρονικής ολοκλήρωσης επιπέδου 4, όπου ο χρήστης πραγματοποιεί και τις οικονομικές συναλλαγές που απαιτούνται με ηλεκτρονικό τρόπο.
b. Επίσης, σύμφωνα με το ΠΠΥΗΔ, οι μηχανισμοί αυθεντικοποίησης που προτείνονται για το επίπεδο αυθεντικοποίησης 1 συμπεριλαμβάνουν συνθηματικά, συνθηματικά μιας χρήσης (τα οποία αποτελούν μια μορφή ελέγχου δύο παραγόντων – two-factor authentication) ή συνδυασμό αυτών. Οι μηχανισμοί αυθεντικοποίησης που προτείνονται για το επίπεδο αυθεντικοποίησης 2 αξιοποιούν ψηφιακά πιστοποιητικά, προτείνεται δε και η αξιοποίηση διακριτικών χαλαρής ή σκληρής αποθήκευσης.
c. Στους κανόνες που έχουν τυποποιηθεί στο τέλος του παραρτήματος ΙΙΙ του ΠΠΥΗΔ ορίζεται ότι οι υπηρεσίες που έχουν ενταχθεί στο επίπεδο εμπιστοσύνης 2 πρέπει να υιοθετήσουν επίπεδο αυθεντικοποίησης τουλάχιστον 1 (Κ.Υ. 9) και οι υπηρεσίες που έχουν ενταχθεί στο επίπεδο εμπιστοσύνης 3 πρέπει να υιοθετήσουν επίπεδο αυθεντικοποίησης τουλάχιστον 1, ενώ συνιστάται επίπεδο αυθεντικοποίησης 2 (Κ.Υ. 10). Οι υπηρεσίες που έχουν υιοθετήσει το επίπεδο αυθεντικοποίησης 1 πρέπει να αξιοποιήσουν ως μηχανισμό αυθεντικοποίησης κατ' ελάχιστο τα

συνθηματικά (Κ.Υ. 11).

13. Στην υπό κρίση επεξεργασία, σκοπός της καταχώρισης των δεδομένων μαθητών/γονέων-κηδεμόνων και εκπαιδευτικών των ιδιωτικών σχολείων στο σύστημα «mySchool» είναι η διευκόλυνση, αλλά και η βελτίωση της άσκησης διαβαθμισμένης και ιεραρχικής εποπτικής αρμοδιότητας του ΥΠΕΘ μέσω των κατά τόπο και καθ' ύλην αρμοδίων οργάνων της διοίκησης της Α΄βάθμιας και Β΄βάθμιας ιδιωτικής εκπαίδευσης, όπως αυτή προβλέπεται στην κείμενη νομοθεσία.

Κατά την εξέταση της υπόθεσης διαπιστώθηκε ότι ισχύουν τα εξής:

Α) Αναφορικά με τους εκπαιδευτικούς:

Από τις ανωτέρω διατάξεις και γενικότερα από την κείμενη νομοθεσία συνάγεται ότι οι αρμόδιες υπηρεσίες του ΥΠΕΘ έχουν την εποπτεία της οργάνωσης των ιδιωτικών σχολείων σχετικά με το εκπαιδευτικό προσωπικό που εργάζεται σε αυτά. Εξάλλου, τα ιδιωτικά σχολεία διαβιβάζουν ήδη στο ΥΠΕΘ βάσει της κείμενης νομοθεσίας όλες τις κατηγορίες προσωπικών δεδομένων εκπαιδευτικών που τηρούνται στο σύστημα ««mySchool»[4] για τα δημόσια σχολεία, εκτός από εκείνα που σχετίζονται αποκλειστικά με την εργασία σε δημόσιο σχολείο, όπως π.χ. αναδρομικός διορισμός, αυτοδίκαιη αποχώρηση, πρόθεση παραίτησης κοκ.

Κατά συνέπεια, τα δεδομένα των εκπαιδευτικών των ιδιωτικών σχολείων που δεν είναι αναγκαία για τον ως άνω σκοπό και κατ' επέκταση για την υπό κρίση καταχώριση στο σύστημα, σε αντίθεση με ό,τι ισχύει για τους εκπαιδευτικούς των δημόσιων σχολείων, είναι τα εξής: 1. Περιοχή Μετάθεσης/Οργανικής Θέσης, 2. Έλαβε Μετάθεση, 3. Υπερ-5ετής Απόσπαση σε σχολείο του εξωτερικού, 4. Πενταετής θητεία σε Πρότυπα Πειραματικά Σχολεία (Π.Π.Σ.) και 5. Λήξη θητείας σε Π.Π.Σ.. Οι κατηγορίες αυτές προσωπικών δεδομένων δεν απαιτείται, κατά τις διατάξεις της κείμενης νομοθεσίας, να καταχωρούνται στο σύστημα για τους

[4] Τα 44 είδη προσωπικών δεδομέων που περιέχονται στο σύστημα ««mySchool» » είναι τα εξής: Επώνυμο, Όνομα, Όνομα πατέρα, Όνομα μητέρας, Αριθμός Μητρώου, Α.Φ.Μ, ΑΜΚΑ Φύλο, Ημερομηνία γέννησης, Ιδιότητα εργαζόμενου, Σχέση εργασίας, Βαθμός, Υποχρεωτικό Διδακτικό Ωράριο, ΦΕΚ Διορισμού = Αριθμός, Ημ/νια, Σειρά δημοσίευσης, Αναδρομικός Διορισμός (ΝΑΙ Ή ΟΧΙ), Ειδικότητες - Κύρια Ειδικότητα, Βαθμίδα Εκπαίδευσης, Κατάσταση εργαζομένου, ΜΚ, Ημερομηνία 1ης Ανάληψης Υπηρεσίας, Θέση προσωπικού φακέλου, Οργανική/Προσωρινή τοποθέτηση, Περιοχή Μετάθεσης Οργανικής, Εποπτεύων Φορέας, Αυτοδίκαιη Αποχώρηση (checkbox), Πρόθεση Παραίτησης (checkbox), Έλαβε Μετάθεση (checkbox), Υπερ-5ετής Απόσπαση σε σχολείο εξωτερικού (checkbox), Πενταετής θητεία σε Πρότυπα Πειραματικά Σχολεία (Π.Π.Σ). (checkbox), Λήξη Θητείας σε Π.Π.Σ , Διεύθυνση, Περιοχή, Τ.Κ., Δημοτική ενότητα, Σταθερό, Κινητό, Άλλα, Ηλεκτρονικές διευθύνσεις, Σημειώσεις, Άδειες, Απουσίες, Αναθέσεις εκπαιδευτικού στην μονάδα, Λεπτομέρειες ωραρίου εργασίας του εργαζόμενου, Τοποθετήσεις σε άλλες μονάδες.

εκπαιδευτικούς των ιδιωτικών σχολείων. Εξάλλου, δεν κρίνονται απαραίτητα για την άσκηση της εποπτείας του ΥΠΕΘ τα εξής στοιχεία: 1. Διεύθυνση, 2. Περιοχή, 3. Τ.Κ., 4. Δημοτική ενότητα, 5. Σταθερό τηλέφωνο, 6. άλλα τηλέφωνα και, συνεπώς, η καταχώρισή τους στο σύστημα έρχεται σε αντίθεση με την αρχή της αναλογικότητας..

Τα υπόλοιπα δεδομένα που τηρούνται ήδη στο σύστημα «mySchool» για τους εκπαιδευτικούς των δημοσίων σχολείων πρέπει, με βάση τις προαναφερόμενες διατάξεις, να τηρούνται και για τους εκπαιδευτικούς των ιδιωτικών σχολείων ώστε η εποπτεία του ΥΠΕΘ να είναι αποτελεσματική. Ωστόσο, δυνατότητα πρόσβασης σε αυτά πρέπει να έχουν συγκεκριμένοι χρήστες του συστήματος και ο διευθυντής της σχολικής μονάδας, ο καθ' ύλην αρμόδιος διευθυντής εκπαίδευσης, ο περιφερειακός διευθυντής εκπαίδευσης στο πλαίσιο των αρμοδιοτήτων του, καθώς και η κεντρική υπηρεσία του ΥΠΕΘ. Η τελευταία αυτή υπηρεσία πρέπει να έχει πρόσβαση μόνο στα στοιχεία που είναι απαραίτητα για την έκδοση διοικητικών πράξεων σχετιζομένων με την υπηρεσιακή κατάσταση των εκπαιδευτικών.

Κατά τη γνώμη του μέλους της Αρχής Κ. Χριστοδούλου, η αρχή της αναγκαιότητας επιβάλλει η εξέταση από την Αρχή της νομιμότητας για την καταχώρηση στο ως άνω σύστημα να μην περιοριστεί στο ζήτημα ποια δεδομένα επιτρεπτώς γνωστοποιούνται και διαβιβάζονται στο ΥΠΕΘ, αλλά να περιλάβει και το μέσο της επεξεργασίας. Δηλαδή, να εξεταστεί αν η πρόσβαση στα δεδομένα αυτά από τους αρμόδιους φορείς του ΥΠΕΘ δεν πρέπει να γίνεται μέσω του συστήματος «mySchool», αλλά με άλλους, ασφαλείς τρόπους, υπό την εποπτεία του οικείου Δ/ντη Εκπαίδευσης.

Β) Αναφορικά με τους μαθητές:

Σε αντίθεση με όσα ισχύουν για τους εκπαιδευτικούς, τα ιδιωτικά σχολεία διαβίβαζαν για τους μαθητές στο ΥΠΕΘ μόνο στατιστικής φύσεως στοιχεία που αφορούν στον αριθμό των τμημάτων ανά τάξη και τμήμα, καθώς και στο σύνολο του αριθμού των μαθητών κάθε ιδιωτικού σχολείου. Σκοπός αυτής της διαβίβασης είναι, μεταξύ άλλων, ο σχεδιασμός της εκπαιδευτικής πολιτικής από το ΥΠΕΘ.

Κατά την εξέταση της υπό κρίση υπόθεσης, διαπιστώθηκε ότι ειδικότερα για τις πανελλήνιες εξετάσεις και, ιδίως, για τη συμμετοχή των μαθητών σε αυτές, από την έναρξη λειτουργίας του συστήματος και μέχρι σήμερα καταχωρούνται από τα

ιδιωτικά σχολεία στο σύστημα 13 από τα 90 είδη προσωπικών δεδομένων μαθητών δημοσίων σχολείων που περιέχονται στο σύστημα[5].

Περαιτέρω, έχει θεσπιστεί ενιαίος αριθμός μαθητή με σκοπό τη μονοσήμαντη ταυτοποίησή του προκειμένου να παρακολουθείται η πορεία του στα σχολικά έτη φοίτησης, ανεξάρτητα από τις μονάδες ή τις γεωγραφικές περιφέρειες, στις οποίες φοιτά. Κατά τους ισχυρισμούς του ΣΙΣ ο σκοπός της ταυτοποίησης του μαθητή ικανοποιείται πλήρως με την καταχώριση 3 έως και 4 κατηγοριών προσωπικών δεδομένων μαθητών: 1. Όνομα μαθητή 2. Επώνυμο μαθητή 3. Όνομα πατρός και 4. Ημερομηνία γέννησης. Αντιθέτως, το ΥΠΕΘ ισχυρίζεται ότι και τα 90 δεδομένα που περιέχονται στο σύστημα είναι αναγκαία για την εποπτική του αρμοδιότητα και για τον ως άνω αναφερόμενο σκοπό της θέσπισης του ενιαίου αριθμού μαθητή. Εξάλλου, μετά την έναρξη λειτουργίας του συστήματος καταχωρούνται σε επίπεδο σχολικής μονάδας (ιδιωτικό σχολείο) στο σύστημα, ενώ πρόσβαση σε αυτά έχει αποκλειστικά ο διευθυντής του σχολείου. Η κεντρική υπηρεσία του ΥΠΕΘ έχει πρόσβαση μόνο σε στατιστικά στοιχεία.

Σύμφωνα με την αρχή της αναλογικότητας, όπως αυτή ορίζεται στο ανωτέρω άρθρο 4 του ν.2472/1997, το ΥΠΕΘ πρέπει να επεξεργάζεται μόνο όσα δεδομένα είναι απολύτως απαραίτητα για την πραγματοποίηση του επιδιωκόμενου σκοπού της επεξεργασίας, δηλαδή της εξασφάλισης της διαφάνειας και της αξιοπιστίας όλων των εκ του νόμου προβλεπόμενων διαδικασιών μέσω του ενιαίου και άμεσου ελέγχου από την Κεντρική Διοίκηση, αλλά και της αρτιότερης και ενιαίας εποπτείας του ΥΠΕΘ στο σύνολο των σχολικών μονάδων. Ως εκ τούτου είναι επιτρεπτή η επεξεργασία μόνο εκείνων των προσωπικών δεδομένων μαθητών ιδιωτικών σχολείων, η συλλογή και τήρηση των οποίων προβλέπεται ειδικώς από το ισχύον νομοθετικό καθεστώς ή είναι αναγκαία για την άσκηση των αρμοδιοτήτων εποπτείας των οικείων υπηρεσιών του ΥΠΕΘ. Επιπλέον, από την ως άνω αναφερόμενη διάταξη του άρθρου 4 παρ. 1 ν. 4351/2015 συνάγεται με σαφή τρόπο η βούληση του νομοθέτη να έχει την εποπτεία και τον έλεγχο της έκδοσης των τίτλων σπουδών όλων των τύπων των ιδιωτικών σχολείων από τον προϊστάμενο της οικείας Διεύθυνσης Πρωτοβάθμιας εκπαίδευσης. Είναι, επομένως, αναγκαία η καταχώρισης των προσωπικών στοιχείων των μαθητών

[5] Πρόκειται για τα εξής δεδομένα μαθητών: 1. Όνομα 2. Επώνυμο 3. Όνομα πατρός 4. Όνομα μητρός 5. Ημερομηνία γέννησης 6. Αριθμός δημοτολογίου 7.Δήμος εγγραφής 8. Γένος μητέρας 9. Διεύθυνση μαθητή 10. Ταχυδρομικός κώδικας 11. Τηλέφωνο 12. Σχολείο προέλευσης 13. Αριθμός ειδικού μητρώου σχολείου προέλευσης.

προκειμένου να καταστεί εφικτή η ταυτοποίηση των προσωπικών στοιχείων των μαθητών κατά τη θεώρηση των τίτλων απόλυσής τους από τον αρμόδιο Διευθυντή Εκπαίδευσης.

Κατά τα ανωτέρω εκτεθέντα, στο σύστημα «mySchool» νομίμως καταχωρούνται τα στοιχεία των μαθητών των ιδιωτικών σχολείων με δυνατότητα πρόσβασης στα στοιχεία αυτά από το καθ' ύλην και κατά τόπο αρμόδιο όργανο του ΥΠΕΘ για την άσκηση της εποπτικής του αρμοδιότητας, όσον αφορά: α) την απόδοση του ενιαίου αριθμού μαθητή, β) τη διεξαγωγή των πανελληνίων εξετάσεων, καθώς και γ) τη θεώρηση των απολυτηρίων τίτλων σπουδών. Οίκοθεν νοείται ότι τα ανωτέρω αφορούν στην καταχώριση και πρόσβαση στο σύστημα και δεν εμποδίζουν την άσκηση της εποπτικής αρμοδιότητας του ΥΠΕΘ, καθώς και την αναζήτηση στοιχείων μαθητών.

Κατά την γνώμη, ωστόσο, του μέλους της Αρχής Κ. Χριστοδούλου, εκτός των στοιχείων που προβλέπονται ρητώς στην κείμενη νομοθεσία, δεν υπάρχει κάποια άλλη νομοθετική πρόβλεψη, με την οποία να καθίσταται αναγκαία και υποχρεωτική η καταχώρηση των υπολοίπων δεδομένων που περιέχονται στο σύστημα. Η τεκμηρίωση δε από το ΥΠΕΘ της αναγκαιότητας της υπό κρίση καταχώρισης των δεδομένων των μαθητών των ιδιωτικών σχολείων στο σύστημα είναι γενική και αόριστη, παρά τη σχετική προβαλλόμενη άποψή του ότι η εν λόγω καταχώριση συνδέεται άρρηκτα με την εποπτική αρμοδιότητά του.

Γ) Αναφορικά με τα μέτρα ασφάλειας:

Η Αρχή έχει ήδη επισημάνει, με την Απόφαση 139/2014, ότι καθίσταται επιβεβλημένη η διατήρηση υψηλού επιπέδου ασφαλείας διότι στη βάση δεδομένων του συστήματος «mySchool», η οποία είναι προσβάσιμη μέσω του διαδικτύου, καταχωρίζεται μεγάλος όγκος των προσωπικών δεδομένων των μαθητών/γονέων-κηδεμόνων και των εκπαιδευτικών της χώρας.

Γ1) Όσον αφορά την υλοποίηση της 6α σύστασης της Απόφασης 139/2014 της Αρχής και το ζήτημα της ασφάλειας του πιστοποιητικού TLS:

Η σύσταση 6α της Απόφασης 139/2014, η οποία αφορά την κρυπτογράφηση των δεδομένων του συστήματος «mySchool» (κατ' ελάχιστον των στοιχείων ταυτοποίησης των υποκειμένων) σε επίπεδο βάσης δεδομένων, έχει, σύμφωνα με τη σχετική απάντηση του ΥΠΕΘ και του ΙΤΥΕ-Διόφαντος, υλοποιηθεί ήδη.

Όσον αφορά το πρωτόκολλο TLS, επισημαίνεται ότι χρησιμοποιείται για τη διασφάλιση της εμπιστευτικότητας των μεταδιδόμενων δεδομένων μεταξύ δύο επικοινωνούντων κόμβων μέσω της κρυπτογράφησης των δεδομένων αυτών (βλ. Απόφαση 121/2014 της Αρχής, διαθέσιμη στο διαδικτυακό της τόπο). Το πρωτόκολλο αυτό παρέχεται στις εκδόσεις 1.0, 1.1, 1.2 και 1.3 και αποτελεί διάδοχο του πρωτοκόλλου SSL (το οποίο παρέχεται στις εκδόσεις 1.0, 2.0 και 3.0). Η κάθε έκδοση του πρωτοκόλλου TLS διορθώνει/μετριάζει ευπάθειες των προηγούμενων εκδόσεων. Συνιστάται να αποφεύγεται η χρήση της έκδοσης TLS 1.0 επειδή οι ευπάθειες του πρωτοκόλλου SSL 3.0 μπορεί να τύχουν εκμετάλλευσης και στην περίπτωση της χρήσης του πρωτοκόλλου TLS 1.0, το οποίο υποστηρίζει την έκδοση SSL 3.0[6]. Περαιτέρω, η ύπαρξη γνωστών επιθέσεων (όπως padding oracle attack, BEAST attack, Lucky Thirteen attack) θέτει συγκεκριμένες απαιτήσεις σχετικά με τη χρήση συμμετρικών αλγορίθμων κρυπτογράφησης στο πρωτόκολλο TLS[7].

Σύμφωνα με τη σχετική απάντηση του ΥΠΕΘ και του ΙΤΥΕ-Διόφαντος, τόσο ο κεντρικός διαδικτυακός τόπος του συστήματος «mySchool» (https://app.myschool.sch.gr), όσο και ο διαδικτυακός τόπος της κεντρικής υπηρεσίας πιστοποίησης του ΠΣΔ (https://sso.sch.gr) διαθέτουν εγκατεστημένο το πρωτόκολλο TLS 1.2. Προκειμένου να εξυπηρετούνται και παλαιότεροι φυλλομετρητές, οι οποίοι είναι ενσωματωμένοι σε παλαιότερα, επίσης, λειτουργικά συστήματα που μπορεί να υπάρχουν ακόμα σε κάποια σχολεία, υποστηρίζονται και τα αντίστοιχα «ciphers» (κρυπτογραφικοί αλγόριθμοι) ή παλαιότερα πρωτόκολλα (TLS 1.0).

---

[6] Πβλ. α) B. Moller, T. Duong, and K. Kotowicz., 2014, "This poodle bites: Exploiting the SSL 3.0 fallback. https://www.openssl.org/~bodo/ssl-poodle.pdf" και β) NIST Special Publication 800-52 Revision 1.

[7] Εάν χρησιμοποιούνται block ciphers θα πρέπει να αποφεύγεται ο τρόπος της CBC κρυπτογράφησης λόγω των επιθέσεων padding oracle attack, BEAST attack και Lucky Thirteen Attack (πρβ. α) B. Canvel, A. Hiltgen, S. Vaudenay, and M. Vuagnoux. Password inerception in a SSL/TLS channel. In Advances in Cryptology - CRYPTO 2003: 23rd Annual International Cryptology Conference, Lecture Notes in Computer Science, vol. 2729, pages 583-599. Springer Berlin Heidelberg, August 2003, β) T. Duong and J. Rizzo. Here come the xor ninjas. In Ekoparty Security Conference, 2011 και γ) N. J. AlFardan and K. G. Paterson. Lucky thirteen: Breaking the TLS and DTLS record protocols. In IEEE Symposium on Security and Privacy, pages 526-540, May 2013).
Επίσης, πρέπει να αποφεύγεται ο αλγόριθμος RC4, διότι αν χρησιμοποιηθεί μπορούν να πραγματοποιηθούν άλλες επιθέσεις, λόγω εγγενών αδυναμιών του RC4.
(πβλ. α) N. J. AlFardan, D. J. Bernstein, K. G. Paterson, B. Poettering, and J. C. N. Schuldt. On the security of RC4 in TLS. In Proceedings of the 22d USENIX Conference on Security, S, pages 305{320. USENIX Association, August 2013 β) K. G. Paterson, B. Poettering, and J. C. N. Schuldt. Big Bias Hunting in Amazonia: Large-Scale Computation and Exploitation of RC4 Biases (Invited Paper), pages 398{419. Lecture Notes in Computer Science, vol. 8873. Springer Berlin Heidelberg, December 2014).

Από σχετική επισκόπηση, κατά την εξέταση της υπό κρίση υπόθεσης, φαίνεται ότι, τόσο οι παραπάνω διαδικτυακοί τόποι, όσο και οι διαδικτυακοί τόποι https://myschool.sch.gr/ (αρχικός διαδικτυακός τόπος που οδηγεί στον διαδικτυακό τόπο της κεντρικής υπηρεσίας πιστοποίησης χωρίς να φαίνεται ότι πραγματοποιείται μέσω αυτού επεξεργασία προσωπικών δεδομένων), https://register.sch.gr/password/change_password/ (διαδικτυακός τόπος αλλαγής κωδικού πρόσβασης του ΠΣΔ) και https://register.sch.gr/password/reset_password/ (διαδικτυακός τόπος ανάκτησης κωδικού πρόσβασης του ΠΣΔ), διαθέτουν πιστοποιητικό TLS 1.2. Επιπλέον, οι επισκοπήσεις ασφαλείας του φυλλομετρητή Chrome αναφέρουν για όλους τους παραπάνω διαδικτυακούς τόπους τους χαρακτηρισμούς «strong cipher» («ισχυρή κρυπτογράφηση») και «strong key exchange» («ισχυρή ανταλλαγή κλειδιών»).

Σύσταση 1η: Το ΥΠΕΘ και το ΙΤΥΕ-Διόφαντος, κατά το μέρος που του αναλογεί, οφείλουν να μεριμνήσουν, ώστε να μην υπάρχει δυνατότητα υποστήριξης των προηγούμενων εκδόσεων του πρωτοκόλλου TLS 1.2 ήτοι 1.0 και 1.1 σε οποιονδήποτε από τους διαδικτυακούς τόπους, οι οποίοι υποστηρίζουν τη λειτουργία του συστήματος «mySchool», καθώς και να μην χρησιμοποιούνται οι κρυπτογραφικοί αλγόριθμοι που έχουν ήδη αποκλεισθεί στην έκδοση 1.3 του πρωτοκόλλου TLS. Το ΥΠΕΘ οφείλει να μεριμνήσει για την κατάλληλη προσαρμογή των υπολογιστών των σχολικών μονάδων και των διοικητικών δομών που χρησιμοποιούνται για τη σύνδεση στο σύστημα «mySchool» .

Γ2) Όσον αφορά την υλοποίηση της 6ζ σύστασης της Απόφασης 139/2014 της Αρχής:

Το ΥΠΕΘ και το ΙΤΥΕ-Διόφαντος διευκρίνισαν με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/7689/08-12-2014 έγγραφο (το οποίο εστάλη στην Αρχή σε συνέχεια της Απόφασης 139/2014), το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/8320/16-12-2016 έγγραφο (το οποίο εστάλη κατόπιν του υπ' αριθμ. πρωτ. Γ/ΕΞ/7648/23-11-2016 εγγράφου της Αρχής, στο πλαίσιο εξέτασης της συμμόρφωσης με την Απόφαση 139/2014) και το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/1964/10-3-2017 υπόμνημα (που αφορά στην υπό κρίση καταγγελία) ότι ο περιορισμός στην πρόσβαση (ήτοι πρόσβαση στο «mySchool» μόνο από IP διευθύνσεις του ΠΣΔ) που θέτει η υλοποίηση της σύστασης 6ζ της Απόφασης 139/2014 δεν αποτελεί ρεαλιστική επιλογή για το σύστημα «mySchool»

για τους λόγους που εκτίθενται στα έγγραφα αυτά και παρατίθενται στο ιστορικό της παρούσας.

Επισημαίνεται ότι συστήματα ηλεκτρονικής διακυβέρνησης, όπως ενδεικτικά το Σύστημα της Ηλεκτρονικής Συνταγογράφησης και το σύστημα taxisnet, στα οποία τυγχάνει επεξεργασίας τεράστιος όγκος προσωπικών δεδομένων (στο μεν πρώτο δεδομένα ειδικών κατηγοριών που αφορούν στην υγεία στο δε δεύτερο δεδομένα που προστατεύονται από το φορολογικό απόρρητο και χρησιμοποιούνται για την παροχή υπηρεσιών πραγματοποίησης οικονομικών συναλλαγών με ηλεκτρονικό τρόπο) και τα οποία διαθέτουν κοινά χαρακτηριστικά με το σύστημα «mySchool» (όπως πρόσβαση στο σύστημα μέσω διαδικτύου με χρήση πιστοποιητικού TLS και χρήση συνθηματικών ως μηχανισμό αυθεντικοποίησης των χρηστών), παρέχουν τις αντίστοιχες υπηρεσίες χωρίς περιορισμό της δυνατότητας πρόσβασης των χρηστών.

Περαιτέρω, τα προσωπικά δεδομένα που τυγχάνουν επεξεργασίας στο σύστημα «mySchool», όπως προκύπτει από τις καταστάσεις με τα προσωπικά δεδομένα των μαθητών, γονέων/κηδεμόνων και εκπαιδευτικών που εστάλησαν στην Αρχή από το ΙΤΥΕ-Διόφαντος, σύμφωνα και με την Απόφαση 139/2014 (η οποία δεν επιτρέπει την καταχώριση στο «mySchool» των δεδομένων ειδικών κατηγοριών του ατομικού δελτίου υγείας του μαθητή), περιλαμβάνουν κατά κανόνα «απλά» προσωπικά δεδομένα, με εξαίρεση το θρήσκευμα των μαθητών σε συγκεκριμένες, προβλεπόμενες από το νόμο, περιπτώσεις (βλ. σκέψη 4 της Απόφασης 139/2014). Σε κάθε περίπτωση, είτε οι παρεχόμενες υπηρεσίες εντάσσονται στο επίπεδο εμπιστοσύνης 2 («απλά» δεδομένα) είτε στο επίπεδο 3 (δεδομένα ειδικών κατηγοριών), πρέπει να υιοθετηθεί, σύμφωνα με το ΠΠΥΗΔ, επίπεδο αυθεντικοποίησης τουλάχιστον 1 (το οποίο πρέπει να αξιοποιεί ως μηχανισμό αυθεντικοποίησης κατ' ελάχιστον τα συνθηματικά), ενώ το επίπεδο αυθεντικοποίησης 2 συνιστάται για το επίπεδο εμπιστοσύνης 3. Το σύστημα «mySchool» υλοποιεί επίπεδο αυθεντικοποίησης 1 ήτοι συνθηματικά, σύμφωνα με τα προβλεπόμενα στο ΠΠΥΗΔ.

Σύσταση 2η: Κατόπιν τούτων και επειδή το σύστημα «mySchool» υλοποιεί τουλάχιστον επίπεδο αυθεντικοποίησης 1 και, όπως διευκρινίστηκε από το ΥΠΕΘ και το ΙΤΥΕ-Διόφαντος, δεν είναι εφικτός ο περιορισμός της πρόσβασης μόνο στις IP διευθύνσεις του ΠΣΔ για την εύρυθμη λειτουργία και την κατάλληλη αξιοποίηση του συστήματος, κρίνεται ότι πρέπει να εξετασθεί η εφαρμογή αυθεντικοποίησης δύο

παραγόντων (two-factor authentication), για τις συνδέσεις που πραγματοποιούνται στο σύστημα «mySchool» από IP διευθύνσεις εκτός του ΠΣΔ και να ενημερωθεί σχετικά η Αρχή. Σε περίπτωση μη εφαρμογής του τρόπου αυτού της αυθεντικοποίησης, πρέπει να αιτιολογηθούν οι λόγοι.

Γ3) Για τα επιπλέον ζητήματα που τέθηκαν από τον ΣΙΣ με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/2665/29-3-2017 υπόμνημά του σχετικά με την ασφάλεια του συστήματος «mySchool», αναφέρονται τα κάτωθι:

Γ3(α) Σχετικά με την αυθεντικοποίηση των χρηστών του συστήματος «mySchool»:

Τα ζητήματα που ετέθησαν με το ως άνω υπόμνημα σχετικά με την αυθεντικοποίηση των χρηστών και την αντιστοίχιση μεταξύ επιπέδου εμπιστοσύνης της παρεχόμενης υπηρεσίας και επίπεδου αυθεντικοποίησης, (βλ. ιστορικό της παρούσας), εξετάσθηκαν στο σημείο Γ2 του σκεπτικού της παρούσας απόφασης.

Όσον αφορά την κρυπτογράφηση των κωδικών των χρηστών, σύμφωνα με τις απαντήσεις του ΥΠΕΘ και του ΙΤΥΕ-Διόφαντος (βλ. ιστορικό της παρούσας), οι κωδικοί των χρηστών του συστήματος «mySchool» κρυπτογραφούνται από το ΠΣΔ.

Επιπλέον, από επισκόπηση της διεπαφής εισόδου του διαδικτυακού τόπου https://sso.sch.gr/login κατά την εξέταση της υπό κρίση υπόθεσης, φαίνεται ότι δεν χρησιμοποιείται CAPTCHA και υπάρχει δυνατότητα αντιγραφής – επικόλλησης των κωδικών στα αντίστοιχα πεδία. Επισημαίνεται ότι οι διεπαφές εισόδου όλων των διαδικτυακών τόπων που αναφέρθηκαν, για συγκριτικούς λόγους, από τον ΣΙΣ (τράπεζα Eurobank - https://ebanking.eurobank.gr/ebanking/login.faces) και τους ΥΠΕΘ και ΙΤΥΕ-Διόφαντος (τράπεζες Εθνική https://ibankretail.nbg.gr/sts/Account/Login/web, Alpha https://www.alpha.gr/e-banking, Πειραιώς https://www.winbank.gr/sites/idiwtes/el/Pages/default.aspx και taxisnet https://login.gsis.gr/mylogin/pages/login.jsp), δεν εφαρμόζουν CAPTCHA στις αντίστοιχες διεπαφές εισόδου και επιτρέπουν την αντιγραφή – επικόλληση των κωδικών (όπως φαίνεται μετά από επισκόπηση των παραπάνω διαδικτυακών τόπων, επίσης, κατά την εξέταση της υπό κρίση υπόθεσης). Επιπλέον, επισημαίνεται ότι σύμφωνα με δημοσιεύματα[8], η Google αμφισβήτησε ότι το CAPTCHA, το οποίο

[8] Πβλ. ενδεικτικά http://tech.in.gr/news/article/?aid=1231368514, http://www.independent.co.uk/life-style/gadgets-and-tech/news/google-captcha-re-robot-image-recognition-artificial-intelligence-website-a7627331.html, https://gizmodo.com/google-has-finally-killed-the-captcha-1793190374

γενικώς θεωρείται ενοχλητικό από τη διαδικτυακή κοινότητα, μπορεί πλέον να εγγυηθεί την ασφάλεια, καθώς υπάρχουν αλγοριθμικές μέθοδοι που αποδίδουν το παραμορφωμένο κείμενο με μεγάλη ακρίβεια και εισήγαγε τον μηχανισμό reCaptcha (https://www.google.com/recaptcha/intro/invisible.html). Επιπλέον, επισημαίνεται ότι το σύστημα «mySchool» προβλέπει το «κλείδωμα» του λογαριασμού μετά από έναν αριθμό επαναλαμβανόμενων αποτυχημένων προσπαθειών σύνδεσης.

Σύσταση 3η: Κατόπιν τούτων, το ΥΠΕΘ και το ΙΤΥΕ-Διοφάντος, κατά το μέρος που του αναλογεί, πρέπει να αποστείλουν εγγράφως στην Αρχή τεκμηριωμένη γνώμη ως προς το ζήτημα αν α) η διεπαφή εισόδου των χρηστών στο σύστημα «mySchool» είναι ευάλωτη σε επιθέσεις επειδή δεν διαθέτει CAPTCHA και επιτρέπει την αντιγραφή-επικόλληση των κωδικών στα αντίστοιχα πεδία και β) είναι απαραίτητο το σύστημα «mySchool» να απενεργοποιεί τη δυνατότητα των φυλλομετρητών των χρηστών να αποθηκεύουν το συνθηματικό κατά τη σύνδεση, λαμβάνοντας υπόψη ότι για τις συνδέσεις εκτός του ΠΣΔ συνιστάται η εξέταση της εφαρμογής αυθεντικοποίησης δύο παραγόντων. Σε καταφατική περίπτωση, πρέπει να μεριμνήσουν για την υλοποίηση των παραπάνω.

Γ3(β) Σχετικά με τη 6ζ σύστασης της Απόφασης 139/2014 της Αρχής:

Το ζήτημα που ετέθη με το ως άνω υπόμνημα του ΣΙΣ σχετικά με την υποκλοπή των αναγνωριστικών (usernames) και των κωδικών (passwords) των χρηστών, οι οποίοι συνδέονται στο σύστημα «mySchool» από IP διευθύνσεις εκτός του ΠΣΔ (από τυχόν μολυσμένους με ιούς ηλεκτρονικούς υπολογιστές με παλαιά λειτουργικά συστήματα, οι οποίοι μπορεί να βρίσκονται στο σπίτι, σε internet cafe, με χρήση ελεύθερου wi-fi καθώς και από κινητά τηλέφωνα και ταμπλέτες) (βλ. ιστορικό της παρούσας) καλύπτεται από το σημείο Γ2 του σκεπτικού της παρούσας απόφασης.

Εξάλλου, το ζήτημα που ετέθη στο ως άνω υπόμνημα του ΣΙΣ, ότι η χρήση του συστήματος «mySchool» εκτός τυπικού ωραρίου εργασίας αντιβαίνει στην εργατική νομοθεσία, εκφεύγει των αρμοδιοτήτων της Αρχής.

Γ3(γ) Σχετικά με την Πολιτική Ασφαλείας του συστήματος «mySchool»:

Ο ΣΙΣ, βασιζόμενος στο περιεχόμενο της Πολιτικής Ασφαλείας, με το ως άνω υπόμνημά του αναφέρθηκε σε ελλείψεις της Πολιτικής Ασφαλείας και ισχυρίστηκε ότι το σύστημα «mySchool» δεν είναι κατάλληλα σχεδιασμένο για την αποτροπή

απειλών κατά τη διαδικασία εγγραφής και δείχνει να είναι ευάλωτο σε πλήθος επιθέσεων, καθώς αυτές δεν έχουν προβλεφθεί στην Πολιτική Ασφαλείας (βλ. ιστορικό της παρούσας). Επισημαίνεται ότι, πάντως, ελλείψεις (του περιεχομένου) της Πολιτικής Ασφαλείας δεν καταδεικνύουν/τεκμηριώνουν άνευ ετέρου εφαρμογή ελλιπών ή ανεπαρκών μέτρων ασφαλείας ή ότι το σύστημα είναι ευάλωτο σε επιθέσεις.

Σύσταση 4η: Ως εκ τούτου, το ΥΠΕΘ και το ΙΤΥΕ - Διόφαντος οφείλουν να μεριμνήσουν για την αναθεώρηση και επικαιροποίηση της Πολιτικής Ασφαλείας του συστήματος «mySchool», ώστε να αποτυπώνονται με σαφήνεια και πληρότητα οι κανόνες και οι διαδικασίες που ακολουθούνται. Επίσης, πρέπει να υπάρχει αντιστοίχιση μεταξύ των διαδικασιών και κανόνων που αποτυπώνονται στην Πολιτική Ασφαλείας και των μέτρων ασφαλείας που εφαρμόζονται στο σύστημα. Η Πολιτική Ασφαλείας πρέπει να αναθεωρείται σε τακτική βάση και να ενημερώνονται σχετικά οι χρήστες (όπως με ανάρτηση της Πολιτικής Ασφαλείας στο διαδικτυακό τόπο του συστήματος «mySchool»). Ειδικά για τις διαδικασίες δημιουργίας νέου λογαριασμού στο σύστημα «mySchool» και ανάκτησης των στοιχείων πρόσβασης λογαριασμού πρέπει να ληφθεί μέριμνα, ώστε τα στοιχεία του λογαριασμού να αποστέλλονται αποκλειστικά στους χρήστες τους οποίους αφορούν (όπως στους ατομικούς λογαριασμούς ηλεκτρονικού ταχυδρομείου των χρηστών αυτών)

Γ3(δ) Σχετικά με την εκπαίδευση των χρηστών του συστήματος «mySchool»:

Ο ΣΙΣ ισχυρίζεται με το υπόμνημά του ότι οι χρήστες του συστήματος «mySchool» δεν είναι εκπαιδευμένοι σε θέματα ασφάλειας (βλ. ιστορικό της παρούσας).

Με τα υπ' αριθμ. πρωτ. Γ/ΕΙΣ/8320/16-12-2016 και Γ/ΕΙΣ/1964/10-3-2017 έγγραφα, το ΥΠΕΘ και το ΙΤΥΕ-Διόφαντος ενημέρωσαν την Αρχή ότι έχουν πραγματοποιηθεί προγραμματισμένες ενημερωτικές ημερίδες σχετικά με τη λειτουργία του συστήματος «mySchool» σε όλες τις εκπαιδευτικές περιφέρειες με τη συμμετοχή των διευθυντών των σχολικών μονάδων της κάθε περιοχής και άλλων ενδιαφερόμενων εκπαιδευτικών. Στις εν λόγω συναντήσεις παρουσιάστηκαν τα θέματα ασφάλειας και προστασίας των προσωπικών δεδομένων.

Επίσης, η αίτηση δημιουργίας νέου λογαριασμού στο σύστημα περιλαμβάνει όρους χρήσης και δήλωση εμπιστευτικότητας. Στους όρους χρήσης αναφέρεται ότι α) ο παρεχόμενος λογαριασμός σύνδεσης αφορά στον συγκεκριμένο χρήστη και

χρησιμοποιείται αποκλειστικά από τον ίδιο, β) δεν επιτρέπεται η γνωστοποίηση σε και η χρήση του κωδικού από τρίτους και γ) οι ηλεκτρονικές ενέργειες των χρηστών καταγράφονται με στόχο την προστασία της ορθότητας των δεδομένων και την αποφυγή παραβίασης κανόνων δικαίου. Επιπλέον, κάθε χρήστης που συνδέεται για πρώτη φορά στο σύστημα ενημερώνεται για τους όρους χρήσης του λογαριασμού και διαβάζει υποχρεωτικά τα προβλεπόμενα στη δήλωση εμπιστευτικότητας. Μόνο τότε μπορεί να προχωρήσει στη χρήση του συστήματος. Σε επόμενη σύνδεση, τα αναδυόμενα παράθυρα δεν εμφανίζονται, αλλά υπάρχουν ως σύνδεσμοι στο κάτω μέρος της διεπαφής του συστήματος («Όροι Χρήσης», «Δήλωση Εμπιστευτικότητας»).

Σύμφωνα με το ΥΠΕΘ και το ΙΤΥΕ-Διόφαντος, εφόσον η πλατφόρμα δεν υπόκειται σε αλλαγές που να επηρεάζουν θέματα ασφάλειας, η ενημέρωση των χρηστών σε θέματα ασφαλούς χρήσης της εφαρμογής και η ενημέρωση σχετικά με τη χρήση λογαριασμών, τόσο κατά τη διαδικασία της αίτησης ενός χρήστη, όσο και στην τελική απόδοση του λογαριασμού από το ΠΣΔ, είναι επαρκής και ουσιαστική, ώστε οι διευθυντές και λοιποί χρήστες να έχουν απόλυτη επίγνωση της σημασίας των θεμάτων ασφάλειας και των αρχών που πρέπει να διέπουν τη διαφύλαξη των λογαριασμών και κωδικών τους. Για τους λόγους αυτούς, δεν καταρτίστηκε οδηγός των χρηστών σε θέματα ασφάλειας.

Επίσης, αναφέρεται ότι με συχνότητα τουλάχιστον δύο φορές το χρόνο υπάρχει ενημέρωση των χρηστών από την υπηρεσία SSO του ΠΣΔ σε σχέση με τον κωδικό πρόσβασης και την ασφάλεια του και επισυνάπτεται στην απάντηση ένα τέτοιο ενημερωτικό μήνυμα.

Το ως άνω επισυναπτόμενο ενημερωτικό μήνυμα φαίνεται να περιέχει ενημέρωση των χρηστών για αναγνώριση και αποφυγή παραπλανητικών μηνυμάτων τύπου «phishing» και παραπλανητικών ιστοσελίδων υποκλοπής των κωδικών πρόσβασης, διαχείριση των μηνυμάτων ανεπιθύμητης ηλεκτρονικής επικοινωνίας (spam), καθώς και ενημέρωση σχετικά με την πιθανή εξαπάτηση των χρηστών και την εγκατάσταση κακόβουλου λογισμικού στους υπολογιστές τους.

Στο διαδικτυακό τόπο της Κεντρικής Υπηρεσίας Πιστοποίησης του ΠΣΔ (https://sso.sch.gr/safetyInfo.jsp), ο οποίος χρησιμοποιείται για την αυθεντικοποίηση των χρηστών του συστήματος «mySchool», υπάρχουν ανηρτημένες οδηγίες ασφαλούς χρήσης των υπηρεσιών του ΠΣΔ, οι οποίες αφορούν την αυθεντικότητα

της σελίδας της υπηρεσίας, την προστασία και μη αποκάλυψη του συνθηματικού και την ασφαλή αποσύνδεση από την υπηρεσία. Επίσης, στη σελίδα http://www.sch.gr/password του ΠΣΔ για την αλλαγή των συνθηματικών των χρηστών υπάρχει ενότητα «Ασφάλεια και Προστασία», η οποία περιλαμβάνει τις ακόλουθες υπο-ενότητες ενημέρωσης των χρηστών: προστασία από παραπλανητικά μηνύματα, οδηγίες ασφάλειας και προστασίας από ιούς, προστασία από τους ιούς στην αλληλογραφία, τελευταία ενημέρωση σχετικά με ιούς, τείχος προστασίας (firewall), προστασία από ανεπιθύμητη αλληλογραφία (spam), φραγή αλληλογραφίας (rbl), ασφάλεια στο διαδίκτυο.

Σύσταση 5η: Κατόπιν τούτων, το ΥΠΕΘ και το ΙΤΥΕ-Διόφαντος πρέπει, κατ' ελάχιστον, να καταρτίσουν ενιαίο οδηγό, στον οποίο να βρίσκεται συγκεντρωμένη όλη η πληροφορία που απαιτείται για την ενημέρωση των χρηστών του συστήματος «mySchool» σε θέματα ασφάλειας και προστασίας προσωπικών δεδομένων και ο οποίος πρέπει να παρέχεται ευχερώς στους χρήστες (όπως με ανάρτηση στο διαδικτυακό τόπο του συστήματος «mySchool»).

Γ3(ε) Σχετικά με προβλήματα διαθεσιμότητας του συστήματος «mySchool»:

Η αναφορά του ΣΙΣ σε μια μόνο περίπτωση μη λειτουργίας του συστήματος «mySchool», ήτοι από τις 23.30 της 16.3.2017 μέχρι το πρωί της επόμενης μέρας, δεν τεκμηριώνει τον ισχυρισμό του ότι το σύστημα αυτό παρουσιάζει προβλήματα διαθεσιμότητας ή γενικά πρόβλημα ασφάλειας.

7στ) Σχετικά με την έλλειψη δυνατότητας μαζικής εισαγωγής των δεδομένων στο «mySchool» με xml αρχεία:

Η παροχή της λειτουργικότητας/δυνατότητας μαζικής εισαγωγής των δεδομένων από τα πληροφοριακά συστήματα των ιδιωτικών σχολείων στο σύστημα «mySchool» με αρχεία τύπου xml συντείνει στη διευκόλυνση της λειτουργίας του συστήματος «mySchool», δεν αναφέρεται δε από τον ΣΙΣ κάποιο ζήτημα προστασίας και ασφαλούς επεξεργασίας των προσωπικών δεδομένων.

Γ3(ζ) Σχετικά με τη δυνατότητα αναζήτησης και εύρεσης στο σύστημα «mySchool» των στοιχείων, συμπεριλαμβανομένου του ΑΜΚΑ, ιδιωτικού εκπαιδευτικού:

Σύμφωνα με το ως άνω υπόμνημα του ΣΙΣ, το σύστημα «mySchool» παρέχει δυνατότητα αναζήτησης και εύρεσης όλων των στοιχείων ιδιωτικού εκπαιδευτικού, συμπεριλαμβανομένου και του ΑΚΜΑ αυτού, με μόνη την καταχώριση του ΑΦΜ του εκπαιδευτικού στο εν λόγω σύστημα (βλ. ιστορικό της παρούσας).

Σύμφωνα με το εγχειρίδιο χρήσης του συστήματος «mySchool», κατά τη χρήση της λειτουργικότητας «Προσθήκη νέων εργαζομένων για ιδιωτικά σχολεία» επιτρέπεται η αναζήτηση εκπαιδευτικού με βάση το ΑΦΜ του. Στο ως άνω εγχειρίδιο αναγράφεται ότι *«(…) Σε περίπτωση που ο Εκπαιδευτικός υπάρχει ήδη στο ΠΣ «mySchool», το σύστημα επιστρέφει συμπληρωμένα τα στοιχεία του και έχετε τη δυνατότητα να τον προσθέσετε στη μονάδα σας (…) Σε περίπτωση που ο Εκπαιδευτικός δεν υπάρχει στο ΠΣ «mySchool» τότε συμπληρώνετε τα στοιχεία του και τον προσθέτετε στη μονάδα σας (…)».* Τα στοιχεία του εκπαιδευτικού, σύμφωνα με το ως άνω εγχειρίδιο, περιλαμβάνουν ως προς τα βασικά στοιχεία το επώνυμο, το όνομα, το όνομα πατέρα, το όνομα μητέρας, την ημερομηνία γέννησης, το ΑΦΜ, τον ΑΜΚΑ, το φύλο και ως προς τα υπηρεσιακά στοιχεία την ιδιότητα εργαζομένου, τη σχέση εργασίας, τις ώρες υποχρεωτικού διδακτικού ωραρίου υπηρέτησης στον φορέα και την ειδικότητα.

Περαιτέρω, σύμφωνα με την απάντηση του ΥΠΕΘ και του ΙΤΥΕ-Διόφαντος στην Αρχή, με βάση το ρόλο που του αποδίδεται, ο διευθυντής της σχολικής μονάδας διαθέτει πρόσβαση στα στοιχεία εκπαιδευτικών που υπηρετούν στη σχολική μονάδα (και μόνο αναφορικά με την τρέχουσα υπηρέτηση). Ωστόσο, φαίνεται ότι, τουλάχιστον, κατά τη χρήση της ως άνω λειτουργικότητας, μπορεί να έχει πρόσβαση σε στοιχεία εκπαιδευτικών των άλλων σχολικών μονάδων. Συνεπώς πρέπει να εξετασθεί αν, μέσω της ως άνω δυνατότητας αναζήτησης, μπορεί και είναι απαραίτητο να έχει πρόσβαση στα στοιχεία εκπαιδευτικών άλλων σχολικών μονάδων.

Σύσταση 6η: Κατόπιν τούτων, το ΥΠΕΘ και το ΙΤΥΕ- Διόφαντος οφείλουν να διευκρινίσουν, εάν ο ρόλος του διευθυντή της σχολικής μονάδας διαθέτει πρόσβαση στα στοιχεία των εκπαιδευτικών άλλων σχολικών μονάδων. Σε καταφατική περίπτωση, πρέπει να διευκρινιστεί για ποιό λόγο είναι αυτό αναγκαίο και να ενημερωθεί η Αρχή σχετικά με τη δυνατότητα περιορισμού της πρόσβασης μόνο στα δεδομένα των εκπαιδευτικών της οικείας σχολικής μονάδας.

Γ3(η) Σχετικά με τη σύσταση 6β της Απόφασης 139/2014 της Αρχής:

Στο ως άνω υπόμνημα του ΣΙΣ αναφέρεται, σε σχέση με την 6β σύσταση της Απόφασης 139/2014, σύμφωνα με την οποία το ΥΠΕΘ οφείλει *«(…) β) Να μεριμνήσει, ώστε να περιληφθεί στο σύστημα η δυνατότητα δημιουργίας ατομικών λογαριασμών χρηστών που να αποδίδονται σε κατάλληλα εξουσιοδοτημένους*

εκπαιδευτικούς της κάθε σχολικής μονάδας και υπαλλήλους της κάθε διοικητικής δομής όπως διεύθυνση ή περιφερειακή διεύθυνση, ώστε να αποφευχθεί τυχόν κοινή χρήση του μοναδικού λογαριασμού που αποδίδεται στον διευθυντή της σχολικής μονάδας ή της διοικητικής δομής για την διεκπεραίωση όλων των εργασιών που απαιτούνται στο πλαίσιο του συστήματος «mySchool» (…)», ότι είναι γνωστό σε όλη την εκπαιδευτική κοινότητα ότι το «mySchool» χρησιμοποιείται από τουλάχιστον τρεις υπαλλήλους κάθε Διεύθυνσης Εκπαίδευσης ή κάθε Περιφερειακής Διεύθυνσης, εκτός από τον υπεύθυνο Διευθυντή. Αποτέλεσμα τούτου είναι ότι όλοι οι ανωτέρω μπορεί να μοιράζονται το αναγνωριστικό και το συνθηματικό του χρήστη.

Ο ως άνω ισχυρισμός του ΣΙΣ περί χρήσης του λογαριασμού του διευθυντή από άλλους υπαλλήλους των ως άνω διευθύνσεων εκπαίδευσης δεν τεκμηριώνεται με συγκεκριμένα στοιχεία.

Σύμφωνα με την απάντηση του ΙΤΥΕ-Διόφαντος στην Αρχή, στις σχολικές μονάδες αποδίδεται ατομικός λογαριασμός πρόσβασης στον διευθυντή της κάθε μονάδας και υπάρχει δυνατότητα απόδοσης ατομικού λογαριασμού πρόσβασης στους υπεύθυνους εκπαιδευτικούς τμημάτων, όπως αυτοί ορίζονται από τον διευθυντή της κάθε σχολικής μονάδας. Επίσης, αποδίδεται ατομικός λογαριασμός πρόσβασης στους Περιφερειακούς Διευθυντές Εκπαίδευσης, καθώς και στους Διευθυντές Πρωτοβάθμιας και Δευτεροβάθμιας Διεύθυνσης Εκπαίδευσης. Οι παραπάνω λογαριασμοί έχουν τα δικαιώματα πρόσβασης που απορρέουν από τον αντίστοιχο ρόλο στον οποίο εντάσσονται.

Από τα παραπάνω και από το σύνολο των προσκομιζόμενων στοιχείων προκύπτει ότι στο σύστημα «mySchool» δεν υπάρχει δυνατότητα απόδοσης ατομικών λογαριασμών πρόσβασης σε υπαλλήλους των ως άνω διευθύνσεων εκπαίδευσης (πέραν των διευθυντών).

Σύσταση 7η: Κατόπιν τούτων, το ΥΠΕΘ και το ΙΤΥΕ-Διόφαντος, πρέπει, λόγω της σύστασης 6β της Απόφασης 139/2014 της Αρχής, να διευκρινίσουν α) αν είναι απαραίτητη η δυνατότητα απόδοσης ατομικών λογαριασμών πρόσβασης σε επιπλέον υπαλλήλους των ως άνω διευθύνσεων εκπαίδευσης και β) σε καταφατική περίπτωση για ποιο λόγο δεν έχει υλοποιηθεί η δυνατότητα αυτή.

Γ3(θ) Σχετικά με τη σύνδεση του συστήματος «mySchool» με τη βάση δεδομένων του Εθνικού Δημοτολογίου:

Στο ως άνω υπόμνημά του, ο ΣΙΣ αναφέρει ότι η διασύνδεση της βάσης δεδομένων του συστήματος «mySchool» με τη βάση του Εθνικού Δημοτολογίου (βλ. σημείο Β του ιστορικού της παρούσας) δημιουργεί ερωτηματικά ως προς την ασφάλεια και προστασία των προσωπικών δεδομένων.

Καταρχάς, επισημαίνεται ότι η διασύνδεση του συστήματος «mySchool» με την κεντρική βάση δεδομένων του ΟΠΣΕΔ του Εθνικού Δημοτολογίου προβλέπεται στην υπ' αριθμ. ΚΥΑ 1493 (ΦΕΚ Β 298 12-02-2016). Ανεξαρτήτως αυτού, δεν αποδεικνύεται ότι απορρέουν κίνδυνοι για την προστασία των προσωπικών δεδομένων εξαιτίας της σύνδεσης με τη βάση δεδομένων του Εθνικού Δημοτολογίου, ο ως άνω δε ισχυρισμός του ΣΙΣ δεν τεκμηριώνεται..

7ι) Σχετικά με τους κωδικούς της βάσης δεδομένων και της κρυπτογράφησης:

Ο ΣΙΣ, στο ως άνω υπόμνημά του, αναφέρει ότι ενημερώθηκε ότι τους κωδικούς της βάσης δεδομένων και της κρυπτογράφησης έχει μόνο ένα άτομο.

Ο ως άνω ισχυρισμός του ΣΙΣ δεν τεκμηριώνεται και προβάλλεται αναποδείκτως.

Γ3(κ) Σχετικά με την εκπόνηση μελέτης εκτίμησης αντικτύπου:

Όσον αφορά την πρόταση του ΣΙΣ να ζητήσει η Αρχή από το ΥΠΕΘ να διενεργήσει εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων επισημαίνεται ότι η υποχρέωση για διενέργεια εκτίμησης αντικτύπου σε σύστημα που λειτουργεί ήδη τεκμηριώνεται από τον υπεύθυνο επεξεργασίας βάσει του άρθρου 35 παρ. 1, 2 και 4 του ΓΚΠΔ. Συνεπώς, το ΥΠΕΘ οφείλει να εξετάσει τη συμμόρφωσή του με το ως άνω άρθρο.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή:

1. Απορρίπτει την καταγγελία του ΣΙΣ για τους λόγους που αναλύονται στην παρούσα απόφαση.
2. Κρίνει ότι:

Α. Είναι νόμιμη η καταχώριση στο σύστημα «mySchool» μόνο των δεδομένων των εκπαιδευτικών των ιδιωτικών σχολείων που κρίνονται αναγκαία για τον σκοπό της άσκησης της ιεραρχικής και διαβαθμισμένης εποπτείας του ΥΠΕΘ, όπως αυτά περιγράφονται ανωτέρω, με δυνατότητα πρόσβασης σε αυτά μόνο από τους χρήστες που αναφέρονται στην παρούσα (βλ. σκ. 13Α).

Β. Είναι νόμιμη η καταχώριση στο σύστημα «mySchool» των δεδομένων των μαθητών/γονέων-κηδεμόνων των ιδιωτικών σχολείων, η συλλογή και τήρηση των οποίων προβλέπεται ειδικώς από το ισχύον νομοθετικό καθεστώς ή είναι αναγκαία για την άσκηση των αρμοδιοτήτων εποπτείας των οικείων υπηρεσιών του ΥΠΕΘ, όπως αυτά περιγράφονται ανωτέρω, με δυνατότητα πρόσβασης σε αυτά μόνο από τους χρήστες που αναφέρονται στην παρούσα (βλ. σκ. 13Β).

Γ. Το ΥΠΕΘ, ως υπεύθυνος επεξεργασίας και το ΙΤΥΕ-Διόφαντος, ως εκτελών την επεξεργασία, οφείλουν επιπλέον να εφαρμόσουν τις συστάσεις που αναφέρονται στο σημείο 13Γ του σκεπτικού της παρούσας απόφασης και να ενημερώσουν την Αρχή εντός τριών μηνών από την κοινοποίησή της υποβάλλοντας αναλυτικό χρονοδιάγραμμα εφαρμογής των συστάσεων αυτών.

Ο Πρόεδρος **Η γραμματέας**

Κωνσταντίνος Μενουδάκος **Ειρήνη Παπαγεωργοπούλου**