ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 21-12-2012

Αριθ. Πρωτ.: Γ/ΕΞ/8213/21-12-2012

Α Π Ο Φ Α Σ Η ΑΡ. 187 / 2012

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνήλθε μετά από πρόσκληση του Προέδρου της σε τακτική συνεδρίαση στην έδρα της την Πέμπτη 13.12.2012 και ώρα 10:00, προκειμένου να εξετάσει την υπόθεση του αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Γεώργιος Μπατζαλέξης, Αναπληρωτής Πρόεδρος, κωλυομένου του Προέδρου της Αρχής, Πέτρου Χριστόφορου και τα τακτικά μέλη της Αρχής Λεωνίδας Κοτσαλής, ως εισηγητής, Αναστάσιος Πράσσος, Αναστάσιος-Ιωάννης Μεταξάς και Γραμματή Πάντζιου. Δεν παρέστησαν, αν και εκλήθησαν νομίμως εγγράφως, ο Δημήτριος Μπριόλας, τακτικό μέλος και ο Χαράλαμπος Ανθόπουλος, αναπληρωματικό μέλος, λόγω κωλύματος. Στη συνεδρίαση παρέστησαν, επίσης, χωρίς δικαίωμα ψήφου, με εντολή του Προέδρου, οι Ευφροσύνη Σιουγλέ και Λεωνίδας Ρούσσος, πληροφορικοί ελεγκτές του Τμήματος Ελεγκτών, ως βοηθοί εισηγητές και η Μελπομένη Γιαννάκη, υπάλληλος του τμήματος διοικητικών και οικονομικών υποθέσεων της Αρχής, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Η Αρχή, στο πλαίσιο του ετήσιου προγραμματισμού των τακτικών ελέγχων της στον τομέα της ηλεκτρονικής διακυβέρνησης, πραγματοποίησε στις 12, 13 και 14 Δεκεμβρίου 2011 επιτόπιο έλεγχο στα πληροφοριακά συστήματα e-school και e-datacenter του Υπουργείου Παιδείας και Θρησκευμάτων, Πολιτισμού και Αθλητισμού (εφεξής «υπεύθυνος επεξεργασίας») αναφορικά με την προστασία και την ασφάλεια των προσωπικών δεδομένων που τηρούνται και τυγχάνουν επεξεργασίας στο πλαίσιο των

συστημάτων αυτών. Συγκεκριμένα, το σύστημα e-school αφορά στη γραμματειακή υποστήριξη των σχολικών μονάδων πρωτοβάθμιας, δευτεροβάθμιας και τεχνικής – επαγγελματικής εκπαίδευσης και το σύστημα e-datacenter στη συγκρότηση ενός κεντρικού μητρώου διαχείρισης των δεδομένων του εκπαιδευτικού και διοικητικού προσωπικού του υπευθύνου επεξεργασίας.

Ο έλεγχος πραγματοποιήθηκε στην Κεντρική Υπηρεσία του υπευθύνου επεξεργασίας και στα γραφεία της εκτελούσας την επεξεργασία αναδόχου εταιρείας «ΕΠΑΦΟΣ Συστήματα Πληροφορικής ΕΠΕ» από τους ελεγκτές της Αρχής Ε. Σιουγλέ, Λ. Ρούσσο και Κ. Καμπουράκη (εφεξής «ομάδα ελέγχου»), μετά από την υπ' αριθμ. πρωτ. Γ/ΕΞ/8246/8-12-2011 εντολή διενέργειας ελέγχου του Προέδρου της Αρχής.

Η Αρχή ενημέρωσε τον υπεύθυνο επεξεργασίας σχετικά με τη διενέργεια του ελέγχου με το υπ' αριθ. πρωτ. Γ/ΕΞ/7452/09-11-2011 έγγραφό της, με το οποίο του ζήτησε επίσης τη συμπλήρωση ειδικού ερωτηματολογίου για καθένα από τα ελεγχόμενα συστήματα με σκοπό την αποτελεσματικότερη προετοιμασία και διευκόλυνση του ελέγχου. Ο υπεύθυνος επεξεργασίας απέστειλε στην Αρχή τις απαντήσεις των ερωτηματολογίων των ελεγχόμενων συστημάτων, μαζί με συνοδευτικά έγγραφα, στις 30-11-2011, με μηνύματα ηλεκτρονικού ταχυδρομείου. Βάσει των απαντήσεων των ερωτηματολογίων και των συνοδευτικών εγγράφων, καταρτίστηκαν ειδικότερα εσωτερικά πλάνα ελέγχου για καθένα από τα ελεγχόμενα συστήματα προσανατολισμένα στα ιδιαίτερα χαρακτηριστικά της επεξεργασίας.

Κατά τον επιτόπιο έλεγχο, η ομάδα ελέγχου, αφού επέδωσε την εντολή διενέργειας ελέγχου, πραγματοποίησε σειρά συνεντεύξεων βάσει των αντίστοιχων ερωτηματολογίων και πλάνων ελέγχου με τους εκπροσώπους του υπεύθυνου επεξεργασίας και του εκτελούντος και στη συνέχεια διενήργησε τον επιτόπιο έλεγχο, τόσο σε τεχνικό επίπεδο, όσο και σε επίπεδο διαδικασιών. Ο έλεγχος επικεντρώθηκε στα μέτρα ασφαλείας (οργανωτικά, τεχνικά και φυσικής ασφαλείας) που εφαρμόζονται για την επεξεργασία των προσωπικών δεδομένων που τηρούνται σε καθένα από τα ελεγχόμενα συστήματα καθώς και στις υποχρεώσεις του υπευθύνου επεξεργασίας όπως απορρέουν από το ν.2472/1997. Ειδικότερα, οι τομείς του ελέγχου περιλαμβάνουν τα εξής: α) Οργανωτικά μέτρα ασφάλειας ήτοι πολιτική και σχέδιο ασφάλειας, υπεύθυνος ασφαλείας, δέσμευση εμπιστευτικότητας του προσωπικού, διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων, σχέδιο ανάκαμψης από καταστροφές, διαδικασίες ελέγχου ευπαθειών, διαδικασίες καταστροφής δεδομένων ή/και υλικού/εξοπλισμού, διαχείριση αλλαγών, εκτελούντες την επεξεργασία, β) τεχνικά μέτρα ασφάλειας ήτοι ασφάλεια επικοινωνιών,

διαχείριση χρηστών και δικαιωμάτων πρόσβασης, αρχεία καταγραφής ενεργειών και κρίσιμων συμβάντων ασφαλείας, αντίγραφα ασφαλείας, ασφάλεια υπολογιστών γ) μέτρα φυσικής ασφάλειας ήτοι φυσική ασφάλεια κέντρου υπολογιστών και κτιρίου, ασφάλεια φυσικού αρχείου δ) υποχρεώσεις του υπευθύνου επεξεργασίας που απορρέουν από το νόμο 2472/1997 ήτοι γνωστοποίηση της επεξεργασίας και ικανοποίηση των δικαιωμάτων ενημέρωσης, πρόσβασης και αντίρρησης.

Στο πλαίσιο του ελέγχου ζητήθηκε από τους συμμετέχοντες στον έλεγχο η επίδοση μιας σειράς έντυπων και ηλεκτρονικών πειστηρίων (εφεξής «Πειστήρια»). Για τη διασφάλιση της ακεραιότητας των ηλεκτρονικών Πειστηρίων εφαρμόστηκε αλγόριθμος κατακερματισμού (MD5 hash) με χρήση κατάλληλου λογισμικού. Η λίστα των ηλεκτρονικών Πειστηρίων εκτυπώθηκε σε δύο (2) αντίγραφα και υπογράφηκε από την ομάδα ελέγχου, καθώς και από εκπρόσωπο του υπευθύνου επεξεργασίας. Άλλα σχετικά με τον έλεγχο ηλεκτρονικά και έντυπα έγγραφα και κείμενα που ζήτησε η ομάδα ελέγχου υποβλήθηκαν στην Αρχή το επόμενο χρονικό διάστημα.

Μετά την πραγματοποίηση του επιτόπιου ελέγχου, η ομάδα ελέγχου συνέταξε πρακτικά ελέγχου (εφεξής «Πρακτικά») για καθένα από τα ελεγχόμενα συστήματα, στα οποία καταγράφονται οι απαντήσεις/διευκρινήσεις των εκπροσώπων του υπεύθυνου επεξεργασίας και του εκτελούντος, καθώς και οι παρατηρήσεις της ομάδας ελέγχου. Τα Πρακτικά περιέχουν επίσης συνημμένη τη λίστα με τα Πειστήρια. Τα Πρακτικά καθενός εκ των δύο ελεγχόμενων συστημάτων απεστάλησαν στις 6-9-2012, με μηνύματα ηλεκτρονικού ταχυδρομείου, στον υπεύθυνο επεξεργασίας για υποβολή σχολίων, παρατηρήσεων και διευκρινίσεων. Η αποσυμπίεση των συνημμένων στα σχετικά μηνύματα αρχείων των Πρακτικών απαιτούσε τη χρήση ειδικού κωδικού ασφαλείας. Ο υπεύθυνος επεξεργασίας απέστειλε στην Αρχή στις 20/9/2012, με μήνυμα ηλεκτρονικού ταχυδρομείου, δύο παρατηρήσεις αναφορικά με το σύστημα e-datacenter, οι οποίες ενσωματώθηκαν στα Πρακτικά του συστήματος αυτού. Στις 17/09/2012 τα Πρακτικά και των δύο συστημάτων οριστικοποιήθηκαν με το υπ' αριθ. πρωτ. Α/ΕΞ/140/17-10-2012 έγγραφο της Αρχής.

Στη συνέχεια, η ομάδα ελέγχου μελέτησε τα Πρακτικά σε συνδυασμό με τα Πειστήρια που συλλέχθηκαν κατά τη διενέργεια του επιτόπιου ελέγχου καθώς αυτά που εστάλησαν στην Αρχή από τον υπεύθυνο επεξεργασίας και τον εκτελούντα πριν και μετά τον επιτόπιο έλεγχο και συνέταξε πόρισμα διοικητικού ελέγχου (εφεξής «Πόρισμα»), το οποίο υπέβαλε στην Αρχή με το υπ' αρ. πρωτ. Γ/ΕΙΣ/8052/14-12-2012 έγγραφο. Στο Πόρισμα καταγράφονται μεταξύ άλλων τα ευρήματα αναφορικά με ελλιπή μέτρα

ασφάλειας ή διαδικασίες προστασίας προσωπικών δεδομένων που εντοπίστηκαν, καθώς και οι συστάσεις για την αντιμετώπιση των κινδύνων που δημιουργούνται.

Η Αρχή, μετά από εξέταση των προαναφερομένων στοιχείων, αφού άκουσε τον εισηγητή και τους βοηθούς εισηγητές, οι οποίοι στη συνέχεια αποχώρησαν, και κατόπιν διεξοδικής συζήτησης,

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

Τα ευρήματα του ελέγχου σχετίζονται ιδίως με το απόρρητο και την ασφάλεια της επεξεργασίας των προσωπικών δεδομένων που τηρούνται στα πληροφοριακά συστήματα e-school και e-datacenter του υπεύθυνου επεξεργασίας (άρθρο 10 του ν. 2472/1997). Στο πλαίσιο του ελέγχου, πέραν της ασφάλειας, ελέγχθηκε και η γενικότερη συμμόρφωση του υπεύθυνου επεξεργασίας ως προς τις προϋποθέσεις νόμιμης επεξεργασίας προσωπικών δεδομένων (άρθρα 4 και 6 του ν. 2472/1997), καθώς και τις υποχρεώσεις του αναφορικά με την ικανοποίηση των δικαιωμάτων των υποκειμένων των δεδομένων (άρθρα 11, 12 και 13 του ν. 2472/1997).

Το άρθρο 10 του ν. 2472/1997 ορίζει ότι: *«1. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απόρρητη. Διεξάγεται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνον κατ' εντολή του. 2. Για τη διεξαγωγή της επεξεργασίας ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου. 3. 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. Με την επιφύλαξη άλλων διατάξεων, η Αρχή παρέχει οδηγίες ή εκδίδει κανονιστικές πράξεις σύμφωνα με το άρθρο 19 παρ. 1 ι' για τη ρύθμιση θεμάτων σχετικά με τον βαθμό ασφαλείας των δεδομένων και των υπολογιστικών και επικοινωνιακών υποδομών, τα μέτρα ασφάλειας που είναι αναγκαίο να λαμβάνονται για κάθε κατηγορία και επεξεργασία δεδομένων, καθώς και για τη χρήση τεχνολογιών ενίσχυσης της ιδιωτικότητας. 4. Αν η επεξεργασία διεξάγεται για λογαριασμό του υπεύθυνου από πρόσωπο μη εξαρτώμενο από αυτόν, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως. Η*

ανάθεση προβλέπει υποχρεωτικά ότι ο ενεργών την επεξεργασία την διεξάγει μόνο κατ' εντολή του υπεύθυνου και ότι οι λοιπές υποχρεώσεις του παρόντος άρθρου βαρύνουν αναλόγως και αυτόν».

Περαιτέρω, το άρθρο 4 του ν. 2472/1997 προβλέπει 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) Να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής, για την πραγματοποίηση των σκοπών της συλλογής τους και της επεξεργασίας τους...»*

Επίσης, το άρθρο 6 του ν. 2472/1997 προβλέπει ότι *«Ο υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιήσει εγγράφως στην Αρχή, τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας…»*.

Επιπλέον, το άρθρο 11 του ν. 2472/1997 ορίζει ότι: *«ο υπεύθυνος επεξεργασίας οφείλει, κατά το στάδιο της συλλογής δεδομένων προσωπικού χαρακτήρα, να ενημερώνει με τρόπο πρόσφορο και σαφή το υποκείμενο για τα εξής τουλάχιστον στοιχεία: α. την ταυτότητά του και την ταυτότητα του τυχόν εκπροσώπου του, β. τον σκοπό της επεξεργασίας, γ. τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων, δ. την ύπαρξη του δικαιώματος πρόσβασης…»*. Το άρθρο 12 του ν. 2472/1997 προβλέπει ότι *«1. Το υποκείμενο των δεδομένων έχει δικαίωμα να ζητεί και να λαμβάνει από τον υπεύθυνο επεξεργασίας, χωρίς καθυστέρηση και κατά τρόπο εύληπτο και σαφή, τις ακόλουθες πληροφορίες: α) Όλα τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, καθώς και την προέλευσή τους, β) Τους σκοπούς της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών, γ) Την εξέλιξη της επεξεργασίας για το χρονικό διάστημα από την προηγούμενη ενημέρωση ή πληροφόρησή του, δ) Τη λογική της αυτοματοποιημένης επεξεργασίας, ε) κατά περίπτωση, τη διόρθωση, τη διαγραφή ή τη δέσμευση (κλείδωμα) των δεδομένων των οποίων η επεξεργασία δεν είναι σύμφωνη προς τις διατάξεις του παρόντος νόμου, ιδιώς λόγω του ελλιπούς ή ανακριβούς χαρακτήρα των δεδομένων, και στ) την κοινοποίηση σε τρίτους, στους οποίους έχουν ανακοινωθεί τα δεδομένα, κάθε διόρθωσης, διαγραφής ή δέσμευσης (κλειδώματος) που διενεργείται σύμφωνα με την περίπτωση ε', εφόσο τούτο δεν είναι αδύνατον ή δεν προυποθέτει δυσανάλογες προσπάθειες. Το δικαίωμα πρόσβασης μπορεί να ασκείται από το υποκείμενο των δεδομένων και με τη συνδρομή ειδικού»*. Το άρθρο 13 του ν. 2472/1997

προβλέπει ότι «*1. Το υποκείμενο των δεδομένων έχει δικαίωμα να προβάλλει οποτεδήποτε αντιρρήσεις για την επεξεργασία δεδομένων που το αφορούν. Οι αντιρρήσεις απευθύνονται εγγράφως στον υπεύθυνο επεξεργασίας και πρέπει να περιέχουν αίτημα για συγκεκριμένη ενέργεια, όπως διόρθωση, προσωρινή μη χρησιμοποίηση, δέσμευση, μη διαβίβαση ή διαγραφή. Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να απαντήσει εγγράφως επί των αντιρρήσεων μέσα σε αποκλειστική προθεσμία δεκαπέντε (15) ημερών. Στην απάντησή του οφείλει να ενημερώσει το υποκείμενο για τις ενέργειες στις οποίες προέβη ή, ενδεχομένως, για τους λόγους που δεν ικανοποίησε το αίτημα. Η απάντηση σε περίπτωση απόρριψης των αντιρρήσεων πρέπει να κοινοποιείται και στην Αρχή.*».

Λαμβάνοντας υπόψη τα ανωτέρω και μετά από εξέταση των ευρημάτων που αναφέρονται στο Πόρισμα, η Αρχή ενέκρινε τις προτάσεις της ομάδας ελέγχου. Ειδικότερα, η Αρχή διαπίστωσε συγκεκριμένες ελλείψεις ή/και παραλείψεις του υπεύθυνου επεξεργασίας αναφορικά με τα οργανωτικά, τεχνικά και τα μέτρα φυσικής ασφάλειας και προστασίας των προσωπικών δεδομένων που τυγχάνουν επεξεργασίας στο πλαίσιο των συστημάτων e-school και e-datacenter, καθώς και τις γενικότερες υποχρεώσεις του κατά τα προβλεπόμενα στο ν.2472/1997.

Η αναλυτική παρουσίαση των ευρημάτων, των κινδύνων που αυτά ενδέχεται να δημιουργήσουν καθώς και των συστάσεων αντιμετώπισής τους καταγράφονται στο επισυναπτόμενο εμπιστευτικό Πόρισμα. Το Πόρισμα συνοδεύεται από Παράρτημα, το οποίο περιλαμβάνει τα Πρακτικά του ελέγχου καθενός εκ των ελεγχόμενων συστημάτων, καθώς και ειδικό έντυπο που πρέπει να συμπληρωθεί από τον υπεύθυνο επεξεργασίας για την ενημέρωση της Αρχής σχετικά με τη συμμόρφωσή του με τις συστάσεις. Το Παράρτημα αποτελεί αναπόσπαστο μέρος του Πορίσματος, το οποίο κοινοποιείται στον υπεύθυνο επεξεργασίας.

Τα ευρήματα που εντοπίστηκαν αφορούν σε ελλείψεις ως προς τις διαδικασίες και την οργάνωση της ασφάλειας, την επαρκή τεκμηρίωση των εφαρμοζόμενων μέτρων ασφάλειας και τη συστηματική επίβλεψή τους καθώς και ως προς την αυθεντικοποίηση των χρηστών και την διαχείριση και υποστήριξη των συστημάτων.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή απευθύνει προειδοποίηση στον υπεύθυνο επεξεργασίας να συμμορφωθεί με τις συστάσεις που αναφέρονται στο επισυναπτόμενο Πόρισμα και να ενημερώσει σχετικά την

Αρχή εντός έξι (6) μηνών από τη λήψη του Πορίσματος, συμπληρώνοντας το ειδικό έντυπο που περιέχεται στο Παράρτημα αυτού.

Ο Αναπληρωτής Πρόεδρος	**Η Γραμματέας**
Γεώργιος Μπατζαλέξης	**Μελπομένη Γιαννάκη**