**ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑμ**
**ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝμ**
**ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑμ**

Αθήνα, 04-03-2013

Αριθ. Πρωτ.: Γ/ΕΞ/1595/04-03-2013

**Α Π Ο Φ Α Σ Ημ ΑΡ. 27/ 2013**

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνήλθε μετά από πρόσκληση του Προέδρου της σε τακτική συνεδρίαση στην έδρα της την Πέμπτη 21.2.2013 και ώρα 10:00 προκειμένου να εξετάσει την υπόθεση του αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν ο Πρόεδρος, Πέτρος Χριστόφορος και τα τακτικά μέλη της Αρχής Λεωνίδας Κοτσαλής, Αναστάσιος-Ιωάννης Μεταξάς, Δημήτριος Μπριόλας, Αντώνιος Συμβώνης, ως εισηγητής, Κωνσταντίνος Χριστοδούλου και Πέτρος Τσαντίλας. Στη συνεδρίαση παρέστη, επίσης, χωρίς δικαίωμα ψήφου, με εντολή του Προέδρου, ο Λεωνίδας Ρούσσος, πληροφορικός ελεγκτής του Τμήματος Ελεγκτών, ως βοηθός εισηγητή, ενώ η βοηθός εισηγητή Ευφροσύνη Σιουγλέ, πληροφορικός ελεγκτής του Τμήματος Ελεγκτών, δεν παρέστη λόγω κωλύματος. Επίσης, παρέστη, με εντολή του Προέδρου, 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 19 και 20 Δεκεμβρίου 2011 επιτόπιο έλεγχο στην Ηλεκτρονική Υπηρεσία Έκδοσης Δελτίου Ειδικού Εισιτηρίου (νυν Ηλεκτρονική Υπηρεσία Απόκτησης Ακαδημαϊκής Ταυτότητας, εφεξής «ελεγχόμενη υπηρεσία») 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 της υπηρεσίας αυτής. Την ελεγχόμενη υπηρεσία ανέπτυξε, διαχειρίζεται και υποστηρίζει για

λογαριασμό του υπεύθυνου επεξεργασίας η Εθνικό Δίκτυο Έρευνας και Τεχνολογίας Α.Ε. (εφεξής «εκτελών την επεξεργασία»).

Βασικό χαρακτηριστικό της ελεγχόμενης υπηρεσίας αποτελεί η συγκέντρωση των προσωπικών δεδομένων των φοιτητών που απαιτούνται για την παροχή της σε κεντρική βάση δεδομένων που φιλοξενείται στο κέντρο δεδομένων του εκτελούντος την επεξεργασία που βρίσκεται στον χώρο του υπευθύνου επεξεργασίας. Οι φοιτητές έχουν πρόσβαση στην εν λόγω βάση μέσω σχετικής διαδικτυακής εφαρμογής, η οποία για τους προπτυχιακούς φοιτητές χρησιμοποιεί μηχανισμό πρόσβασης που βασίζεται στη διαδικτυακή ταυτοποίησή τους μέσω των οικείων ιδρυμάτων τους.

Ο έλεγχος πραγματοποιήθηκε στις εγκαταστάσεις του εκτελούντος την επεξεργασία, που βρίσκονται στη διεύθυνση Λ. Μεσογείων 56, Αθήνα, από τους υπαλλήλους του Τμήματος Ελεγκτών της Γραμματείας της Αρχής Ευφροσύνη Σιουγλέ, Κωνσταντίνα Καμπουράκη και Λεωνίδα Ρούσσο (εφεξής «ομάδα ελέγχου»), μετά από την υπ' αρ. πρωτ Γ/ΕΞ/8246/08-12-2011 εντολή διενέργειας ελέγχου του Προέδρου της Αρχής.

Η Αρχή ενημέρωσε τον υπεύθυνο επεξεργασίας σχετικά με τη διενέργεια του ελέγχου με την υπ' αρ. πρωτ Γ/ΕΞ/7452/09-11-2011 επιστολή της, στην οποία του ζήτησε επίσης τη συμπλήρωση του ειδικού ερωτηματολογίου με σκοπό την αποδοτικότερη προετοιμασία και διευκόλυνση του ελέγχου. Ο υπεύθυνος επεξεργασίας, απέστειλε στις 30-11-2011 με μήνυμα ηλεκτρονικού ταχυδρομείου και επισυναπτόμενη επιστολή τις απαντήσεις στο ερωτηματολόγιο της Αρχής (υπ' αρ. πρωτ. Γ/ΕΙΣ/8061/02-12-2011 έγγραφο προς την Αρχή), με υπογραφή του Ειδικού Γραμματέα Ανώτατης Εκπαίδευσης.

Κατά τον επιτόπιο έλεγχο, η ομάδα ελέγχου πραγματοποίησε πρώτα σειρά συνεντεύξεων βάσει του ερωτηματολογίου με τους αρμόδιους υπαλλήλους του εκτελούντος και του υπεύθυνου επεξεργασίας και στη συνέχεια διενήργησε επιτόπιο έλεγχο, τόσο σε τεχνικό επίπεδο, όσο και επίπεδο διαδικασιών. Ο έλεγχος επικεντρώθηκε στα μέτρα ασφαλείας (οργανωτικά, τεχνικά και φυσικής ασφαλείας) που εφαρμόζονται για την επεξεργασία των προσωπικών δεδομένων που τηρούνται στην ελεγχόμενη υπηρεσία 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 εκτελούντος την επεξεργασία. Άλλα σχετικά με τον έλεγχο ηλεκτρονικά και έντυπα έγγραφα και κείμενα που ζήτησε η ομάδα ελέγχου υποβλήθηκαν στην Αρχή το επόμενο χρονικό διάστημα.

Μετά από την ολοκλήρωση του ελέγχου, η ομάδα ελέγχου συνέταξε τα Πρακτικά του ελέγχου (εφεξής «Πρακτικά»), στα οποία καταγράφονται οι απαντήσεις/διευκρινήσεις του εκτελούντος την επεξεργασία και του υπεύθυνου επεξεργασίας, καθώς και οι επιτόπιες παρατηρήσεις της ομάδας ελέγχου. Τα Πρακτικά απεστάλησαν στις 6/9/2012 με μήνυμα ηλεκτρονικού ταχυδρομείου σε εκπροσώπους του εκτελούντος και του υπεύθυνου επεξεργασίας για υποβολή σχολίων ή/και παρατηρήσεων. Η αποσυμπίεση των συνημμένων στα σχετικά μηνύματα αρχείων των Πρακτικών απαιτούσε τη χρήση ειδικού κωδικού ασφαλείας. Στις 17/10/2012 τα Πρακτικά οριστικοποιήθηκαν και πρωτοκολλήθηκαν (αριθμός πρωτοκόλλου Α/ΕΞ/143/17-10-2012).

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. Α/ΕΙΣ/16/25-02-2013 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 ΝΟΜΟμ**

Τα ευρήματα του ελέγχου σχετίζονται ιδίως με το απόρρητο και την ασφάλεια της επεξεργασίας των προσωπικών δεδομένων που τηρούνται στο πληροφοριακό σύστημα της ελεγχόμενης υπηρεσίας (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 δεδο ένων προσωπικού χαρακτήρα είναι απόρρητη. Διεξάγεται αποκλειστικά και όνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και όνον κατ' εντολή του. 2. Για τη διεξαγωγή της επεξεργασίας ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα ε αντίστοιχα επαγγελ ατικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου. 3. Ο υπεύθυνος επεξεργασίας οφείλει να λα βάνει τα κατάλληλα οργανωτικά και τεχνικά έτρα για την ασφάλεια των δεδο ένων και την προστασία τους από τυχαία ή αθέ ιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευ ένη διάδοση ή πρόσβαση και κάθε άλλη ορφή αθέ ιτης επεξεργασίας. Αυτά τα έτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδο ένων που είναι αντικεί ενο της επεξεργασίας. Με την επιφύλαξη άλλων διατάξεων, η Αρχή παρέχει οδηγίες ή εκδίδει κανονιστικές πράξεις σύ φωνα ε το άρθρο 19 παρ. 1 ι' για τη ρύθ ιση θε άτων σχετικά ε τον βαθ ό ασφαλείας των δεδο ένων και των υπολογιστικών και επικοινωνιακών υποδο ών, τα έτρα ασφάλειας που είναι αναγκαίο να λα βάνονται για κάθε κατηγορία και επεξεργασία δεδο ένων, καθώς και για τη χρήση τεχνολογιών ενίσχυσης της ιδιωτικότητας. 4. Αν η επεξεργασία διεξάγεται για λογαριασ ό του υπεύθυνου από πρόσωπο η εξαρτώ ενο από αυτόν, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως. Η ανάθεση προβλέπει υποχρεωτικά ότι ο ενεργών την επεξεργασία την διεξάγει όνο 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 δεδο ένα προσωπικού χαρακτήρα για να τύχουν νό ι ης επεξεργασίας πρέπει : α) Να συλλέγονται κατά τρόπο θε ιτό και νό ι ο για καθορισ ένους, σαφείς και νό ι ους σκοπούς και να υφίστανται*

*θε ιτή και νό ι η 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 ενη έρωση. δ) Να διατηρούνται σε ορφή που να επιτρέπει τον προσδιορισ ό της ταυτότητας των υποκει ένων τους όνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής, για την πραγ ατοποίηση 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 δεδο ένων προσωπικού χαρακτήρα, να ενη ερώνει ε τρόπο πρόσφορο και σαφή το υποκεί ενο 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 δεδο ένων, δ. την ύπαρξη του δικαιώ ατος πρόσβασης…»*. Το άρθρο 12 του ν. 2472/1997 προβλέπει ότι *«1. Το υποκεί ενο των δεδο ένων έχει δικαίω α να ζητεί και να λα βάνει από τον υπεύθυνο επεξεργασίας, χωρίς καθυστέρηση και κατά τρόπο εύληπτο και σαφή, τις ακόλουθες πληροφορίες: α) Όλα τα δεδο ένα 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 διάστη α από την προηγού ενη ενη έρωση ή πληροφόρησή του, δ) Τη λογική της αυτο ατοποιη ένης επεξεργασίας, ε) κατά περίπτωση, τη διόρθωση, τη διαγραφή ή τη δέσ ευση (κλείδω α) των δεδο ένων των οποίων η επεξεργασία δεν είναι σύ φωνη προς τις διατάξεις του παρόντος νό ου, ιδίως λόγω του ελλιπούς ή ανακριβούς χαρακτήρα των δεδο ένων, και στ) την κοινοποίηση σε τρίτους, στους οποίους έχουν ανακοινωθεί τα δεδο ένα, κάθε διόρθωσης, διαγραφής ή δέσ ευσης (κλειδώ ατος) που διενεργείται σύ φωνα ε την περίπτωση ε', εφόσον τούτο δεν είναι αδύνατον ή δεν προϋποθέτει δυσανάλογες προσπάθειες. Το δικαίω α πρόσβασης πορεί να ασκείται από το υποκεί ενο των δεδο ένων και ε τη συνδρο ή ειδικού»*. Το άρθρο 13 του ν. 2472/1997 προβλέπει ότι «*1. Το υποκεί ενο των δεδο ένων έχει δικαίω α να προβάλλει οποτεδήποτε αντιρρήσεις για την επεξεργασία δεδο ένων που το αφορούν. Οι αντιρρήσεις απευθύνονται εγγράφως στον υπεύθυνο επεξεργασίας και πρέπει να περιέχουν αίτη α για συγκεκρι ένη ενέργεια, όπως διόρθωση, προσωρινή η χρησι οποίηση, δέσ ευση, η διαβίβαση ή διαγραφή. Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να απαντήσει εγγράφως επί των αντιρρήσεων έσα σε αποκλειστική προθεσ ία δεκαπέντε (15) η ερών. 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 την εφαρμογή συγκεκριμένων οργανωτικών και τεχνικών μέτρων καθώς και μέτρων φυσικής ασφάλειας για την προστασία των προσωπικών δεδομένων που επεξεργάζονται στο πλαίσιο παροχής της υπό έλεγχο υπηρεσίας σε βαθμό ικανοποιητικό. Ωστόσο, τα μέτρα πρέπει να συμπληρωθούν σύμφωνα με τις προτεινόμενες συστάσεις του Πορίσματος.

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, 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.

**ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣμ**

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 Πρόεδροςμ** **Η Γραμματέαςμ**

**Πέτρος Χριστόφοροςμ** **Μελπομένη Γιαννάκημ**