



**ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ  
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ**

Αθήνα, 05-09-2014

Αριθ. Πρωτ.: Γ/ΕΞ/5260/05-09-2014

**Α Π Ο Φ Α Σ Η ΑΡ. 121/2014**

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνήλθε μετά από πρόσκληση του Προέδρου της σε τακτική συνεδρίαση στην έδρα της την 25-06-2014, σε συνέχεια της από 26-03-2014 τακτικής συνεδρίασής της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Π. Χριστόφορος, Πρόεδρος της Αρχής, και τα τακτικά μέλη της Αρχής Λ. Κοτσαλής, Αν. – Ιωάν. Μεταξάς, Δ. Μπριόλας, Α. Συμβώνης, ως εισηγητής, και Κ. Χριστοδούλου. Το τακτικό μέλος Π. Τσαντίλας, αν και προσκλήθηκε νομίμως, δεν προσήλθε λόγω κωλύματος. Στη συνεδρίαση παρέστησαν, επίσης, με εντολή του Προέδρου, οι Γ. Ρουσόπουλος, ειδικός επιστήμων – πληροφορικός, και Κ. Λιμνιώτης, ειδικός επιστήμων – πληροφορικός, ως βοηθοί εισηγητή. Επίσης, παρέστη, με εντολή του Προέδρου, και η Ε. Παπαγεωργοπούλου, υπάλληλος του Διοικητικού – Οικονομικού Τμήματος της Αρχής, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (εφεξής ΑΔΑΕ) διαβίβασε στην Αρχή δύο καταγγελίες σχετικά με την επεξεργασία προσωπικών δεδομένων χρηστών δύο διαδικτυακών τόπων του Υπουργείου Παιδείας και Θρησκευμάτων (εφεξής, υπεύθυνος επεξεργασίας). Ειδικότερα, οι δύο καταγγελίες αφορούσαν τα κάτωθι (βλ. α' και β' αντιστοίχως):

α) Η ΑΔΑΕ διαβίβασε στην Αρχή, με το υπ' αριθμ. πρωτ. 2589/06.12.2013 έγγραφό της (αριθμ. πρωτ. Αρχής: Γ/ΕΙΣ/7918/12-12-2013), την καταγγελία που της υποβλήθηκε από το

Δημήτριο Λαμπράκη αναφορικά με την ασφάλεια του διαδικτυακού τόπου <http://odysseas.it.minedu.gov.gr/><sup>1</sup> του υπευθύνου επεξεργασίας, μέσω του οποίου απογράφησαν οι υπάλληλοι συγκεκριμένων κλάδων οκτώ Πανεπιστημίων, σύμφωνα με την υπ' αριθμ. ΔΙΠΙΔΔ/Β.2/Δ/33/οικ.27653/11-10-2013 Υπουργική Απόφαση. Όπως αναφέρεται στην ως άνω καταγγελία, η σύνδεση των χρηστών στον ανωτέρω διαδικτυακό τόπο δεν ήταν κρυπτογραφημένη, ενώ επίσης δεν ήταν σε ισχύ επαρκείς μηχανισμοί για την αυθεντικοποίηση των χρηστών της συγκεκριμένης διαδικτυακής εφαρμογής, αφού για την πρόσβαση σε αυτή απαιτείτο η εισαγωγή προσωπικών στοιχείων του εκάστοτε υπαλλήλου τα οποία δύναται να γνωρίζουν και άλλοι, χωρίς να πραγματοποιείται κανένας άλλος έλεγχος σχετικά με την επιβεβαίωση της ταυτότητάς του. Επίσης, βάσει της καταγγελίας, ο συγκεκριμένος διαδικτυακός τόπος δεν παρείχε ενημέρωση περί του ακριβούς είδους της επεξεργασίας και των αποδεκτών των δεδομένων.

Η Αρχή, στο πλαίσιο εξέτασης της εν λόγω καταγγελίας, απέστειλε στον υπεύθυνο επεξεργασίας το υπ' αριθμ. πρωτ. Γ/ΕΞ/131/10-01-2014 έγγραφο, με το οποίο ζητούσε μεταξύ άλλων τις απόψεις επί των καταγγελλομένων, καθώς επίσης και ειδικότερες διευκρινίσεις περί του τρόπου λειτουργίας του ανωτέρω διαδικτυακού τόπου, του ακριβούς είδους της επεξεργασίας προσωπικών δεδομένων αλλά και των μέτρων ασφαλείας που ελήφθησαν για την εν λόγω επεξεργασία, λαμβάνοντας υπόψη ότι οι κανόνες και πρότυπα αναφορικά με την εγγραφή, ταυτοποίηση και ηλεκτρονική αναγνώριση πολιτών σε ηλεκτρονικές υπηρεσίες του δημόσιου τομέα καθορίζονται στο Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης (ΥΑΠ Φ.40.4/1/989, ΦΕΚ 1301/Β/2012) – εφεξής, ΠΠΥΗΔ - και, μάλιστα, στο Παράρτημα ΙΙΙ αυτού (Πλαίσιο Ψηφιακής Αυθεντικοποίησης).

Ο υπεύθυνος επεξεργασίας (ειδικότερα μέσω της Δ/σης Λειτουργικής Ανάπτυξης Πληροφοριακών Συστημάτων) απάντησε στην Αρχή με το υπ' αριθμ. πρωτ. 16522/ΣΤ4 και με ημερομηνία 06-02-2014 έγγραφο (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/858/10-02-2014), στο οποίο επισημαίνονται τα εξής:

ι) Όπως προβλέπεται από την παρ. 3 του άρθρου 2 της με αριθμ. ΔΙΠΙΔΔ/Β.2/2/οι.21634/2.8.2013 (ΦΕΚ 1914/Β/7.8.2013) Απόφασης του Υπουργού Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης, το Ανώτατο Συμβούλιο Επιλογής Προσωπικού (εφεξής ΑΣΕΠ) παρέχει ενιαίο λογισμικό για τη σύνταξη πινάκων συνδρομής κριτηρίων επιλογής, σε ψηφιακή μορφή, για τη θέση σε διαθεσιμότητα. Ως εκ τούτου, για το εν λόγω πληροφοριακό σύστημα, σχεδιάστηκαν ηλεκτρονικές φόρμες

---

1

Ο εν λόγω διαδικτυακός τόπος δεν είναι πλέον σε λειτουργία

αντίστοιχες με αυτές του ΑΣΕΠ, ακολουθώντας τις σχετικές επεξηγηματικές οδηγίες.

ii) Τα δεδομένα που συλέχθηκαν παραδόθηκαν εν συνεχεία στην αρμόδια υπηρεσία του υπευθύνου επεξεργασίας για τις περαιτέρω ενέργειες. Όπως προβλέπεται από τις προαναφερθείσες διατάξεις, το ΑΣΕΠ μοριοδότησε τα προσόντα των υπαλλήλων, κατάρτισε Πίνακα κατάταξης υπαλλήλων κατά φθίνουσα σειρά βαθμολογίας, ανά φορέα, κατηγορία, κλάδο ή/και ειδικότητα, και διαβίβασε τους σχετικούς πίνακες στο αρμόδιο τριμελές ειδικό υπηρεσιακό συμβούλιο του οικείου φορέα, το οποίο και εξέδωσε τους τελικούς πίνακες που αναρτήθηκαν σε επίσημους διαδικτυακούς τόπους του Υπουργείου Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης και του ΑΣΕΠ. Λόγω της προβλεπόμενης στην προαναφερθείσα Υπουργική Απόφαση δημόσιας ανάρτησης των στοιχείων των απογραφέντων υπαλλήλων, κρίθηκαν επαρκή τα μέτρα ασφαλείας για το εν λόγω πληροφοριακό σύστημα. Περαιτέρω, όλα τα απαραίτητα δικαιολογητικά των στοιχείων που δηλώθηκαν από τους απογραφέντες έπρεπε να κατατεθούν και εγγράφως στο αρμόδιο Τμήμα του υπευθύνου επεξεργασίας, σύμφωνα με το αρ. πρωτ. 150628/B2/15.10.2013 έγγραφο της Δ/σης Ανωτάτης Πανεπιστημιακής Εκπαίδευσης του Υπουργείου, οπότε και – όπως αναφέρεται στην ως άνω απάντηση του υπευθύνου επεξεργασίας – διασφαλιζόταν η ακεραιότητα των δεδομένων, η αποτροπή κακόβουλης πρόσβασης καθώς και κάθε άλλη μορφή αθέμιτης ενέργειας. Συνεπώς, κρίθηκε μη αναγκαία η χρήση πρόσθετων μηχανισμών αποφυγής κακόβουλης παραποίησης των καταγεγραμμένων ηλεκτρονικών δεδομένων.

iii) Η εν λόγω διαδικτυακή υπηρεσία, κατά τον υπεύθυνο επεξεργασίας, ήταν σύμφωνη με τους κανόνες που αναφέρονται στο ΠΠΥΗΔ: ειδικότερα, η υπηρεσία εντάχθηκε στο επίπεδο εμπιστοσύνης 2, λόγω της φύσης των δεδομένων, και στο επίπεδο αυθεντικοποίησης 1 λόγω του ότι θα ακολουθούσε επικοινωνία του χρήστη με τον φορέα και σε φυσικό επίπεδο. Ως εκ τούτου, κρίθηκε επαρκές το να χρησιμοποιηθεί ο συνδυασμός του Αριθμού Φορολογικού Μητρώου (ΑΦΜ) και του Αριθμού Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ) ως μηχανισμός αυθεντικοποίησης των χρηστών.

β) Η ΑΔΑΕ διαβίβασε στην Αρχή, με το υπ' αριθμ. πρωτ. 2588/06.12.2013 έγγραφό της (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/7919/12-12-2013) καταγγελία του Αχιλλέα Μαλισώβα αναφορικά με την ασφάλεια του διαδικτυακού τόπου <http://iekteachers.sch.gr/Login> του υπευθύνου επεξεργασίας, μέσω του οποίου καθηγητές υπέβαλαν αιτήσεις για απασχόληση σε Δημόσια ΙΕΚ. Ειδικότερα, με βάση την καταγγελία, τα δεδομένα που αποστέλλονται στον ανωτέρω διαδικτυακό τόπο, όπως ο Αριθμός Φορολογικού Μητρώου και ο Αριθμός Μητρώου Κοινωνικής Ασφάλισης, δεν είναι κρυπτογραφημένα.

Η Αρχή, στο πλαίσιο εξέτασης την εν λόγω υπόθεσης, και δεδομένου ότι δεν ήταν σαφής ο υπεύθυνος του εν λόγω διαδικτυακού τόπου, απέστειλε στο Ίδρυμα Νεολαίας και Δια Βίου Μάθησης (Ι.ΝΕ.ΔΙ.ΒΙ.Μ.), με κοινοποίηση στο Υπουργείο Παιδείας και Θρησκευμάτων, το υπ' αριθμ. πρωτ. Γ/ΕΞ/448/22-01-2014 έγγραφο, με το οποίο ζητούσε τις απόψεις επί των καταγγελλομένων. Ακολούθως, το Υπουργείο Παιδείας (και ειδικότερα η Δ/νση Διοικητικού - Οικονομικού), ως υπεύθυνος επεξεργασίας, απέστειλε στην Αρχή το με αρ. πρωτ. 965 και με ημ/νία 07-02-2014 έγγραφο (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/966/13-02-2014), στο οποίο αναφέρονται τα εξής:

i) Η πιστοποίηση των χρηστών της εν λόγω υπηρεσίας γίνεται με τον ΑΦΜ, τον ΑΜΚΑ, και προσωπικό συνθηματικό που επιλέγει ο κάθε χρήστης. Αναφορικά με τη μη χρήση κρυπτογράφησης (πρωτόκολλο HTTP αντί για το HTTPS), ο υπεύθυνος επεξεργασίας αναφέρει ότι υποκλοπή στοιχείων ενός χρήστη θα μπορούσε να γίνει μόνο αν κάποιος τρίτος αποκτούσε πρόσβαση στη δικτυακή κίνηση από το μηχάνημα από το οποίο γίνεται η υποβολή, κάτι το οποίο αποτελεί έναν μόνιμο κίνδυνο που δεν αντιμετωπίζεται με το πρωτόκολλο HTTPS.

ii) Η σχετική βάση δεδομένων βρίσκεται σε εξαιρετικά ασφαλή υποδομή, με σχήμα κατανεμημένων εξυπηρετητών και «τείχος προστασίας» (firewall), με πρόσβαση μόνο μέσω εικονικού ιδεατού δικτύου (VPN).

Το Υπουργείο Παιδείας και Θρησκευμάτων κλήθηκε νομίμως, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/1750/17-03-2014 έγγραφο της Αρχής, σε ακρόαση ενώπιον της Αρχής στη συνεδρίαση της 26-03-2014, ως υπεύθυνος επεξεργασίας, για να δώσει περαιτέρω διευκρινίσεις και να εκθέσει διεξοδικά τις απόψεις του επί των ανωτέρω. Στη συνεδρίαση της 26-03-2014, παρέστησαν νομίμως, ως εκπρόσωποι του Υπουργείου, η κα. Κουρούπη Γεωργία, Διευθύντρια της Δ/νσης Προσωπικού Ανωτάτης Εκπαίδευσης, και η κα. Μαρούγκα Καλομοίρα, Αναπληρώτρια Δ/ντρια της Δ/νσης Λειτουργίας και Ανάπτυξης Πληροφοριακών Συστημάτων, για το ζήτημα της υπό του ανωτέρω σημείου α' καταγγελίας (ήτοι της απογραφής υπαλλήλων), καθώς επίσης και ο κ. Πιτσικάλης Σταύρος, στέλεχος του Τμήματος Επαγγελματικής Επιμόρφωσης Γενικής Γραμματείας Δια βίου Μάθησης, για το ζήτημα της υπό του ανωτέρω σημείου β' καταγγελίας (ήτοι των αιτήσεων εκπαιδευτών). Κατά την ακρόαση, οι ως άνω εκπρόσωποι εξέθεσαν προφορικά τις απόψεις τους. Κατόπιν της ακρόασης, ο υπεύθυνος επεξεργασίας κατέθεσε εμπροθέσμως σχετικά υπομνήματα τόσο για το ζήτημα της απογραφής υπαλλήλων (υπ' αριθμ. πρωτ. 50297/B2 και με ημερομηνία 02-04-2014 έγγραφο - αρ. πρωτ. Αρχής: Γ/ΕΙΣ/2126/02-04-2014), όσο και για το ζήτημα των

αιτήσεων εκπαιδευτών (υπ' αριθμ. πρωτ. 3511 και με ημερομηνία 02-04-2014 έγγραφο - αρ. πρωτ. Αρχής: Γ/ΕΙΣ/2119/02-04-2014).

Με βάση τα όσα εκτέθηκαν προφορικά κατά τη συνεδρίαση της Αρχής, αλλά και όσα παρατίθενται στα ως άνω υπομνήματα, προκύπτουν τα κάτωθι για την επεξεργασία δεδομένων μέσω των δύο διαδικτυακών τόπων (βλ. α' για την απογραφή υπαλλήλων και β' για τις αιτήσεις εκπαιδευτών αντιστοίχως):

α) Το Υπουργείο, μετά τη δημοσίευση της υπ' αριθμ. 135211/B2/23-9-2013 (ΦΕΚ 2384/B/2013) ΚΥΑ, όπως τροποποιήθηκε με την υπ' αριθ. 150539/B2/15-10-2013 (ΦΕΚ 2601/B/2013) ΚΥΑ, δυνάμει της οποίας καταργήθηκαν 1349 οργανικές και προσωποπαγείς θέσεις μόνιμου και με σχέση εργασίας ιδιωτικού δικαίου αορίστου χρόνου διοικητικού προσωπικού οκτώ Πανεπιστημίων, απέστειλε τη με αριθ. 139550/B2/30-09-2013 εγκύκλιο του Γενικού Γραμματέα, σχετικά με την εφαρμογή των διατάξεων διαθεσιμότητας Διοικητικού Προσωπικού Πανεπιστημίων, σύμφωνα με το άρθρο 90 του ν. 4172/2013. Σημειώνεται ότι η διαδικασία επιλογής των υπαλλήλων που τίθενται σε διαθεσιμότητα, τα κριτήρια επιλογής και κατάταξής τους, ο τρόπος μοριοδότησής τους και λοιπά συναφή ζητήματα καθορίζονται με την υπ' αριθ. ΔΙΠΙΔΔ/B.2/2/οικ.21634/2-8-2013 (ΦΕΚ 1914/B/2013) απόφαση του Υπουργού Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης, κατ' εξουσιοδότηση των διατάξεων της περ. Ε' της παρ. 2 του άρθρου 90 του ν. 4172/2013.

Σύμφωνα με τις ανωτέρω διατάξεις, οι Δ/νσεις Διοικητικού Προσωπικού των οικείων Πανεπιστημίων, εντός δεκαπέντε ημερών από τη δημοσίευση της 135211/B2/23-9-2013 ΚΥΑ, είχαν υποχρέωση να συντάξουν πίνακες συνδρομής κριτηρίων σε ψηφιακή μορφή, σύμφωνα με ενιαίο λογισμικό που παρέχει για το σκοπό αυτό το ΑΣΕΠ, και να καταγράψουν σε αυτούς τα προσόντα όλων των υπαλλήλων του κλάδου ή/και της ειδικότητας που ανήκαν οι υπό κατάργηση θέσεις. Επίσης, εντός της ανωτέρω προθεσμίας, οι σχετικοί πίνακες έπρεπε να αποσταλούν τόσο εγγράφως, όσο και σε ψηφιακή μορφή, στο ΑΣΕΠ. Παράλληλα, οι Δ/νσεις Διοικητικού Προσωπικού των οικείων Πανεπιστημίων όφειλαν να αναζητήσουν, από τους υπαλλήλους που ενέπιπταν στις εξαιρέσεις από τη διαθεσιμότητα σύμφωνα με την περ. Δ της παρ. 2 του άρθρου 90 του ν. 4172/2013, τα νόμιμα σχετικά δικαιολογητικά και αφού τα ελέγξουν, να τα αποστείλουν εντός της ως άνω αποκλειστικής προθεσμίας στο ΑΣΕΠ αλλά και στο Τριμελές Ειδικό Υπηρεσιακό Συμβούλιο, το οποίο έχει συσταθεί με την υπ' αριθμ. 129808/B2/16-9-2013 (ΦΕΚ 2337/B/20103) Απόφαση του Υπουργού Παιδείας και Θρησκευμάτων, και εδρεύει στην Κεντρική Υπηρεσία του Υπουργείου.

Αφού παρήλθε άπρακτη η ως άνω προθεσμία των δεκαπέντε ημερών, το Υπουργείο εξέδωσε την υπ' αριθ. 15628/B2/15-10-2013 πρόσκληση απογραφής των υπηρετούντων υπαλλήλων για τα εν λόγω Πανεπιστήμια, προς εφαρμογή των διατάξεων της διαθεσιμότητας (σύμφωνα με την υπ' αριθ. ΔΙΠΙΔΔ/Β.2/2/οικ.21634/2-8-2013 (ΦΕΚ 1914/Β/2013) Υπουργική Απόφαση, όπως τροποποιήθηκε με την υπ' αριθ. ΔΙΠΙΔΔ/Β.2/Δ/33/οι. 27653/11-10-2013 (ΦΕΚ 2560/Β/2013) Υπουργική Απόφαση). Η απογραφή αποτελείτο από δύο σκέλη: i) την ηλεκτρονική απογραφή μέσω του ανωτέρω διαδικτυακού τόπου, ii) την κατάθεση των απαραίτητων δικαιολογητικών των στοιχείων που δηλώθηκαν στην ηλεκτρονική απογραφή, η οποία έλαβε χώρα από 16-10-2013 μέχρι και 22-10-2013. Την ίδια υποχρέωση είχαν και οι υπάλληλοι που ενέπιπταν στις κατηγορίες των εξαιρέσεων της περίπτωσης Δ της παραγράφου 2 του άρθρου 90 του ν. 4172/2013 και του άρθρου 53 του ν. 4186/2013 (ΦΕΚ 193/Α/2013).

Σημειώνεται ότι, όπως επιβεβαιώθηκε και από τους εκπροσώπους του Υπουργείου κατά την ακρόασή τους ενώπιον της Αρχής, κατά την ως άνω διαδικασία της ηλεκτρονικής απογραφής, οι υπάλληλοι που ενέπιπταν στις ως άνω εξαιρέσεις της διαθεσιμότητας δήλωναν ηλεκτρονικά ρητώς την εξαίρεση στην οποία ενέπιπταν (όπως για παράδειγμα, αν ο υπάλληλος είναι ανάπηρος σε ποσοστό τουλάχιστον 67%, ή αν ο/η σύζυγος ή τέκνο που ανήκει στην κατηγορία των εξαρτώμενων μελών έχει αναπηρία σε ποσοστό τουλάχιστον 67% και εφόσον το ετήσιο εισόδημα είναι χαμηλότερο των 12000 €).

Τα δεδομένα που συλέχθηκαν από το εν λόγω πληροφοριακό σύστημα παραδόθηκαν στην αρμόδια υπηρεσία του Υπουργείου για τις περαιτέρω ενέργειες. Ο υπεύθυνος επεξεργασίας επισημαίνει στο υπόμνημά του ότι η ως άνω διαδικασία αποτιμήσεως προσόντων των υπό καθεστώς διαθεσιμότητας υπαλλήλων των Πανεπιστημίων επιβλήθηκε εκ του νόμου και χάριν του δημοσίου σκοπού αυτού, ως υποχρέωση των αρμοδίων υπηρεσιών των ιδρυμάτων αυτών, του ΑΣΕΠ, των υπηρεσιών του εποπτεύοντος Υπουργείου και, προεχόντως, των υπαχθέντων στην εν λόγω διαδικασία υπαλλήλων, δια του συστήματος της αυτο-απογραφής τους.

Όσον αφορά την ασφάλεια της επεξεργασίας, οι εκπρόσωποι του Υπουργείου, κατά την ακρόασή τους ενώπιον της Αρχής, επανέλαβαν τους ισχυρισμούς που είχαν ήδη διατυπωθεί στο υπ' αριθμ. πρωτ. 16522/ΣΤ4 και με ημερομηνία 06-02-2014 έγγραφο (βλ. ανωτέρω) – οι οποίοι ισχυρισμοί διατυπώνονται εκ νέου και στο υπ' αριθμ. πρωτ. 50297/Β2 και με ημερομηνία 02-04-2014 υπόμνημα. Δεδομένου ωστόσο ότι δεν ήταν απόλυτα σαφές από το ως άνω υπόμνημα εάν πραγματοποιήθηκε από την πλευρά του υπευθύνου επεξεργασίας αντιπαραβολή των δεδομένων της απογραφής με όσα έγγραφα δικαιολογητικά απέστειλαν οι

υπόχρεοι απογραφής, πριν την αποστολή αυτών στο ΑΣΕΠ, η Αρχή απηύθυνε εκ νέου προς τον υπεύθυνο επεξεργασίας ερωτήματα για αυτό το ζήτημα με το υπ' αριθμ. πρωτ. Γ/ΕΞ/2805/06-05-2014 έγγραφό της. Ο υπεύθυνος επεξεργασίας απάντησε με το υπ' αριθμ. πρωτ. 79361/B2/21-05-2014 έγγραφό του (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/3191/22-05-2014), όπου και αναφέρει: *«παρότι έγινε η αντιπαραβολή των δηλωθέντων στοιχείων με τα προσκομισθέντα δικαιολογητικά, εν τούτοις δεν έγινε καμία επέμβαση στα στοιχεία που εστάλησαν στο ΑΣΕΠ»*. Στο ίδιο έγγραφο σημειώνει ότι οι σχετικοί πίνακες μοριοδότησης που ανήρτησε το ΑΣΕΠ στις 18 και 21 Νοεμβρίου 2013 με βάση τα στοιχεία που του απέστειλε ο υπεύθυνος επεξεργασίας είναι πλέον άνευ αντικειμένου και δεν έχουν ισχύ, αφού έκτοτε οι Διευθύνσεις Διοικητικού των αντίστοιχων Ιδρυμάτων έστειλαν απευθείας στο ΑΣΕΠ, όπως αρχικά είχε προβλεφθεί, τα στοιχεία των υπαλλήλων τους και βάσει αυτών αναρτήθηκαν από το ΑΣΕΠ νέοι πίνακες μοριοδότησης εντός του διαστήματος Ιανουαρίου – Φεβρουαρίου 2014, οπότε και εν συνεχεία εξεδόθη η υπ' αριθ. πρωτ. 70810/B2/8-5-2014 Διαπιστωτική Πράξη του Υπουργού Παιδείας και Θρησκευμάτων που αφορά στη διαθεσιμότητα των διοικητικών υπαλλήλων των οκτώ Πανεπιστημίων, η οποία στηρίζεται αποκλειστικά στα ορθά στοιχεία που εστάλησαν από τα συγκεκριμένα Πανεπιστήμια και είναι, ως εκ τούτου, η μόνη ισχυρή.

β) Η Γενική Γραμματεία Δία Βίου Μάθησης του Υπουργείου Παιδείας και Θρησκευμάτων (εφεξής, ΓΓΔΒΜ) απηύθυνε – δυνάμει του ν. 4186/2013 – πρόσκληση (αρ. πρωτ. 11871/16-10-2013) εκδήλωσης ενδιαφέροντος εκπαιδευτών ενηλίκων, για την κάλυψη των αναγκών ωρομισθίων εκπαιδευτικών στα Ι.Ε.Κ. κατά την περίοδο 2013-2014. Οι υποψήφιοι εκλήθησαν να υποβάλλουν, εντός συγκεκριμένης προθεσμίας, ηλεκτρονική αίτηση στο ειδικό πληροφοριακό σύστημα που παρέχεται στο διαδικτυακό σύνδεσμο <http://iekteachers.sch.gr>. Για την υποβολή της αίτησης εισάγεται ο ΑΜΚΑ καθώς και ένα συνθηματικό που επιλέγει ο κάθε υποψήφιος. Άπαξ και συνδεθεί ο χρήστης, συμπληρώνει τα προσωπικά του στοιχεία, καταχωρεί τα στοιχεία εκπαίδευσης και διδακτικής του εμπειρίας, καθώς και τα κοινωνικά κριτήρια που τον χαρακτηρίζουν (π.χ. ΑΜΕΑ, πολυτεκνία κτλ.). Μετά το πέρας της προθεσμίας υποβολής των αιτήσεων, οι υποψήφιοι κατατάσσονται σε αξιολογικό πίνακα κατάταξης, ανά Διεύθυνση Δία Βίου Μάθησης, σύμφωνα με την ειδικότητά τους και την κατηγορία εκπαίδευσης, τα κριτήρια και τη μοριοδότησή τους, όπως αυτά ορίζονται στη με αριθ. πρωτ. 11869/16-10-2013 Απόφαση του Υπουργού Παιδείας και Θρησκευμάτων. Όλα τα απαραίτητα δικαιολογητικά των στοιχείων που δηλώνονται στο ανωτέρω πληροφοριακό σύστημα, καθώς και το αντίγραφο της αίτησης - την οποία μπορεί

να εκτυπώσει ο χρήστης – πρέπει να κατατεθούν, από όσους επιλεγούν και κληθούν να αναλάβουν υπηρεσία και καθήκοντα, στο αντίστοιχο ΙΕΚ ή ΣΕΚ.

Η Αρχή, μετά από εξέταση των προαναφερομένων στοιχείων, αφού αναγνώστηκαν τα πρακτικά της συνεδρίασης της 26-03-2014, άκουσε τον εισηγητή και τους βοηθούς εισηγητή, οι οποίοι στη συνέχεια αποχώρησαν, και κατόπιν διεξοδικής συζήτησης,

#### ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Το άρθρο 2 του ν. 2472/1997, ορίζει ότι «δεδομένα προσωπικού χαρακτήρα» είναι «κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων». «Υποκείμενο των δεδομένων» είναι «το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική».

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

Στο ίδιο άρθρο επίσης ορίζεται ως επεξεργασία δεδομένων προσωπικού χαρακτήρα «κάθε εργασία ή σειρά εργασιών που πραγματοποιείται, από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή». Επίσης, ως υπεύθυνος επεξεργασίας ορίζεται οποιοσδήποτε καθορίζει το σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός.

2. Σύμφωνα με το αρ. 4 παρ. 1 στοιχ. α) του ν. 2472/1997, τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει να συλλέγονται με τρόπο θεμιτό και



νόμιμο, για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών (αρχή του σκοπού). Επιπλέον, σύμφωνα με το αρ. 4 παρ. 1 στοιχ. β) του ν. 2472/1997, τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας (αρχή της αναλογικότητας), ενώ σύμφωνα με το αρ. 4 παρ. 1 στοιχ. γ) του ν. 2472/1997, τα δεδομένα πρέπει να είναι ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση.

Περαιτέρω, η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο όταν το υποκείμενο έχει δώσει τη συγκατάθεσή του, όπως επιτάσσει το αρ. 5 παρ. 1 του ν. 2472/1997, εκτός εάν συντρέχει μία από τις προβλεπόμενες από την παράγραφο 2 του ίδιου άρθρου εξαιρέσεις, οπότε είναι νόμιμη η επεξεργασία και χωρίς τη συγκατάθεση του υποκειμένου. Ως προς τα ευαίσθητα δεδομένα, προϋπόθεση της νόμιμης επεξεργασίας αποτελεί η χορήγηση άδειας κατά το άρθρο 7 παρ. 2 του ίδιου νόμου, μόνο εφόσον συντρέχει μία ή περισσότερες από τις προϋποθέσεις που ρητώς επισημαίνονται στο άρθρο 7 παρ. 2 του ν. 2472/1997. Ο υπεύθυνος επεξεργασίας απαλλάσσεται από την υποχρέωση λήψης άδειας εφόσον η επεξεργασία εμπίπτει σε κάποια από τις εξαιρέσεις που προβλέπονται στο άρθρο 7<sup>Α</sup> του ν. 2472/1997.

3. Σύμφωνα με το άρθρο 6 του ν. 2472/1997, ο υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιήσει εγγράφως στην Αρχή τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας – εκτός αν εμπίπτει σε κάποια από τις εξαιρέσεις που προβλέπονται στο άρθρο 7<sup>Α</sup> του ν. 2472/1997.

4. Από τις διατάξεις των άρθρων 2, 4 παρ. 1 και 5 παρ. 2 του ν. 2472/1997 προκύπτει ότι η επεξεργασία απλών προσωπικών δεδομένων επιτρέπεται και χωρίς τη συγκατάθεση των υποκειμένων των δεδομένων στην περίπτωση που ο σκοπός της επεξεργασίας είναι νόμιμος, σαφής και καθορισμένος, τα δεδομένα τα οποία τυγχάνουν επεξεργασίας είναι συναφή, πρόσφορα και όχι περισσότερα από όσα απαιτούνται για την επίτευξη του σκοπού της επεξεργασίας και επιπλέον συντρέχει μία από τις προϋποθέσεις που προβλέπονται στο άρθρο 5 παρ. 2 του προαναφερθέντος νόμου, όπως π.χ. η επεξεργασία να είναι αναγκαία για την εκπλήρωση υποχρέωσης του υπευθύνου επεξεργασίας, η οποία επιβάλλεται από νόμο (στοιχ. β'). Εξάλλου, η επεξεργασία προσωπικών δεδομένων από δημόσια αρχή για τους απασχολούμενους στη δημόσια διοίκηση λειτουργεί και αναπτύσσει τις συνέπειές της στο πλαίσιο του κράτους δικαίου και της αρχής της νομιμότητας. Όπως παγίως γίνεται δεκτό, η αρχή της νομιμότητας λειτουργεί ως περιοριστικό όριο της διοικητικής δράσης, ή, με αντίστροφο συλλογισμό, η διοικητική ενέργεια πρέπει να είναι σύμφωνη προς τον κανόνα

δικαίου που διέπει τη δράση της διοίκησης.

Για την επεξεργασία προσωπικών δεδομένων μέσω του διαδικτυακού τόπου <http://odysseas.it.minedu.gov.gr/> (εφεξής, διαδικτυακός τόπος απογραφής υπαλλήλων), ο σκοπός της επεξεργασίας αλλά και οι κατηγορίες των υπό επεξεργασία δεδομένων (ήτοι κριτήρια αποτίμησης προσόντων για την επιλογή υπαλλήλων που θα τεθούν σε διαθεσιμότητα) προσδιορίζεται από την υπ' αριθμ. ΔΙΠΙΔΔ/Β.2/2/οι.21634/2.8.2013 (ΦΕΚ 1914/Β/7.8.2013) Υπουργική Απόφαση, κατ' εξουσιοδότηση του άρθρου 90 του ν. 4172/2013 (περ. Ε', παρ. 2). Το είδος της επεξεργασίας (ήτοι ηλεκτρονική υποβολή των στοιχείων, σε συνδυασμό με έγγραφη κατάθεση των απαραίτητων δικαιολογητικών) προσδιορίστηκε με την υπ' αριθμ. ΔΙΠΙΔΔ/Β.2/Δ/33/οικ.27653/11-10-2013 Υπουργική Απόφαση (ΦΕΚ 2560/Β/2013), όπου αναφέρεται ότι «οι υπηρετούντες με οποιαδήποτε σχέση εργασίας σε εποπτευόμενα από Υπουργεία ΝΠΔΔ υποχρεούνται, εντός πέντε (5) ημερών από την δημοσίευση σχετικής πρόσκλησης από το εποπτεύον Υπουργείο, να απογραφούν σε ειδικό πληροφοριακό σύστημα που το εποπτεύον Υπουργείο παρέχει και λειτουργεί για το σκοπό αυτό. Όλα τα απαραίτητα δικαιολογητικά κατατίθενται και εγγράφως στην οικεία Διεύθυνση Διοικητικού/ Προσωπικού του εποπτεύοντος Υπουργείου». Σημειώνεται επίσης ότι για την εν λόγω ηλεκτρονική εφαρμογή της απογραφής υπαλλήλων, τα προσωπικά δεδομένα που συνελέγησαν και υπέστησαν περαιτέρω επεξεργασία ήταν συναφή, πρόσφορα και όχι περισσότερα από όσα απαιτούνταν εν όψει του σκοπού της επεξεργασίας, αφού οι χρήστες κλήθηκαν να υποβάλουν ηλεκτρονικά – πέραν των στοιχείων ταυτοποίησής τους - εκείνα τα στοιχεία τα οποία αποτέλεσαν κριτήρια αξιολόγησης προκειμένου να καταρτιστούν οι σχετικοί πίνακες κατάταξης.

Περαιτέρω, αναφορικά με το διαδικτυακό τόπο <http://iekteachers.sch.gr> (εφεξής, διαδικτυακός τόπος αίτησης εκπαιδευτών), σημειώνεται ότι έχει επίσης εφαρμογή η ανωτέρω εξαίρεση του άρθρου 5 παρ. 2 στοιχ. β' του ν. 2472/1997, δεδομένου ότι η εν λόγω επεξεργασία προβλέπεται σε νόμο. Επίσης, και σε αυτήν την περίπτωση, τα προσωπικά δεδομένα που συνελέγησαν και υπέστησαν περαιτέρω επεξεργασία ήταν συναφή, πρόσφορα και όχι περισσότερα από όσα απαιτούνταν εν όψει του σκοπού της επεξεργασίας (ήτοι τη συλλογή αιτήσεων ενδιαφερομένων εκπαιδευτών για δημόσια ΙΕΚ και ΣΕΚ, με τα στοιχεία που αποτελούν κριτήρια αξιολόγησης).

Σημειώνεται ότι και στις δύο περιπτώσεις πραγματοποιήθηκε, μέσω των σχετικών διαδικτυακών εφαρμογών, επεξεργασία και ευαίσθητων δεδομένων υγείας, όπως επισημάνθηκε ανωτέρω (δήλωση για ποσοστό αναπηρίας άνω του 67% για το διαδικτυακό τόπο απογραφής υπαλλήλων, καθώς και δήλωση για ΑΜΕΑ για το διαδικτυακό τόπο

αίτησης εκπαιδευτών). Επιπροσθέτως, μέσω του διαδικτυακού τόπου αίτησης υπαλλήλων, πραγματοποιήθηκε και επεξεργασία δεδομένων εργασιακής κατάστασης (άνεργος, ιδιωτικός/δημόσιος υπάλληλος κτλ.): σημειώνεται ότι οι πληροφορίες περί ανεργίας συνιστούν, όπως παγίως κρίνει η Αρχή, ευαίσθητα δεδομένα προσωπικού χαρακτήρα σχετικά με την κοινωνική πρόνοια (Βλ., π.χ., τις αποφάσεις της Αρχής 1/2009, 117/2011, 133/2011 και 134/2011). Και στις δύο περιπτώσεις ωστόσο (διαδικτυακοί τόποι απογραφής υπαλλήλων και αίτησης εκπαιδευτών), ως προς για την επεξεργασία ευαίσθητων δεδομένων έχει εφαρμογή η εξαίρεση του άρθρου 7<sup>Α</sup> παρ. 1 στοιχ. α' του ν. 2472/1997, όπου αναφέρεται ότι ο υπεύθυνος επεξεργασίας απαλλάσσεται από την υποχρέωση γνωστοποίησης και λήψης άδειας *«όταν η επεξεργασία πραγματοποιείται αποκλειστικά για σκοπούς που συνδέονται άμεσα με σχέση εργασίας ή έργου ή με παροχή υπηρεσιών στο δημόσιο τομέα και είναι αναγκαία για την εκπλήρωση υποχρέωσης που επιβάλλει ο νόμος ή για την εκτέλεση των υποχρεώσεων από τις παραπάνω σχέσεις και το υποκείμενο έχει προηγουμένως ενημερωθεί»*.

5. 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.

6. Ζητήματα ασφάλειας κατά την ηλεκτρονική επικοινωνία των φορέων του δημόσιου τομέα με φυσικά (ή νομικά) πρόσωπα ρυθμίζονται στο ν. 3979/2011 περί ηλεκτρονικής διακυβέρνησης (βλ. ιδίως άρθρο 21 παρ. 2, άρθρο 22 παρ. 1, άρθρο 32 παρ. 4), όπου και αναφέρεται ότι τα σχετικά ζητήματα ρυθμίζονται με απόφαση του εκάστοτε αρμόδιου Υπουργού καθώς και με το Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης - ΠΠΥΗΔ, το οποίο επικαιροποιείται σύμφωνα με τα όσα προβλέπονται στο άρθρο 17 παρ. 4 του ν. 3979/2011.

6α. Ειδικότερα, κανόνες και πρότυπα αναφορικά με την εγγραφή, ταυτοποίηση και ηλεκτρονική αναγνώριση πολιτών σε ηλεκτρονικές υπηρεσίες του δημόσιου τομέα καθορίζονται στο ΠΠΥΗΔ (ΥΑΠ Φ.40.4/1/989, ΦΕΚ 1301/Β/2012) και, ειδικότερα, στο Παράρτημα ΙΙΙ αυτού. Όπως επισημαίνεται στο εν λόγω Πλαίσιο, οι διαδικασίες εγγραφής και αυθεντικοποίησης των χρηστών καθορίζονται από το επίπεδο εμπιστοσύνης στο οποίο εντάσσονται οι παρεχόμενες ηλεκτρονικές υπηρεσίες. Η κατηγοριοποίηση των υπηρεσιών σε επίπεδα εμπιστοσύνης (η οποία γίνεται από τον εκάστοτε φορέα που παρέχει την υπηρεσία)

ορίζεται από το είδος των υπό επεξεργασία δεδομένων και τις πιθανές επιπτώσεις που μπορεί να προκληθούν σε περίπτωση μη ορθής λειτουργίας ή διαχείρισής τους.

Σύμφωνα με τα όσα αναφέρονται στο ΠΠΥΗΔ, τα επίπεδα εμπιστοσύνης είναι τέσσερα, και αριθμούνται από 0 (το χαμηλότερο) έως 3 (το υψηλότερο). 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 υπηρεσίες που απαιτούν είτε ανταλλαγή ευαίσθητων προσωπικών δεδομένων είτε υπηρεσίες όπου ο χρήστης πραγματοποιεί ολοκληρωμένες οικονομικές συναλλαγές με ηλεκτρονικό τρόπο. Περαιτέρω, ως υποχρεωτικοί κανόνες<sup>2</sup> επισημαίνονται, μεταξύ άλλων, οι κάτωθι:

i) Ο φορέας που προσφέρει μια ηλεκτρονική υπηρεσία πρέπει να προσδιορίσει την κατηγορία των δεδομένων που επεξεργάζεται η συγκεκριμένη υπηρεσία (βλ. Κ.Υ. 5 στο Παράρτημα ΙΙΙ του ΠΠΥΗΔ), καθώς επίσης και ακολούθως το επίπεδο εμπιστοσύνης στο οποίο εντάσσεται η συγκεκριμένη υπηρεσία (βλ. Κ.Υ. 6 στο Παράρτημα ΙΙΙ του ΠΠΥΗΔ).

ii) Υπηρεσίες που έχουν ενταχθεί στο επίπεδο εμπιστοσύνης 2 πρέπει να υιοθετήσουν επίπεδο εγγραφής 2 και επίπεδο αυθεντικοποίησης τουλάχιστον 1 (βλ. Κ.Υ. 9 στο Παράρτημα ΙΙΙ του ΠΠΥΗΔ), ενώ υπηρεσίες που έχουν ενταχθεί στο επίπεδο εμπιστοσύνης 3 πρέπει να υιοθετήσουν επίπεδο εγγραφής 3 και επίπεδο αυθεντικοποίησης τουλάχιστον 1, ενώ συνιστάται επίπεδο αυθεντικοποίησης 2 (βλ. Κ.Υ. 10 στο Παράρτημα ΙΙΙ του ΠΠΥΗΔ).

iii) Υπηρεσίες που έχουν υιοθετήσει το επίπεδο αυθεντικοποίησης 1 πρέπει να αξιοποιήσουν ως μηχανισμό αυθεντικοποίησης κατ' ελάχιστο τα συνθηματικά<sup>3</sup> (βλ. Κ.Υ. 11 στο Παράρτημα ΙΙΙ του ΠΠΥΗΔ).

Σημειώνεται ότι τα επίπεδα εγγραφής περιγράφονται επίσης στο ΠΠΥΗΔ: ιδιαίτερα επισημαίνεται ότι, για την περίπτωση των επιπέδων εγγραφής 2 και 3, ο χρήστης παραλαμβάνει τα διακριτικά αυθεντικοποίησής του από την αρμόδια υπηρεσία, αφού πρώτα ταυτοποιηθεί από τον αρμόδιο υπάλληλο επιδεικνύοντας και υποβάλλοντας δημόσια έγγραφα που αναγράφουν τα αναγνωριστικά του.

7. Αναφορικά με τα μέτρα για την προστασία των προσωπικών δεδομένων για το διαδικτυακό τόπο της απογραφής υπαλλήλων, σημειώνεται ότι, λαμβάνοντας υπόψη το είδος

<sup>2</sup>

Σύμφωνα με το ΠΠΥΗΔ, υποχρεωτικοί είναι οι κανόνες που η συμμόρφωση με τις προδιαγραφές που τίθενται είναι επιβεβλημένη για τους φορείς του Δημόσιου τομέα.

<sup>3</sup>

Όπως ορίζεται στο ΠΠΥΗΔ, τα συνθηματικά αποτελούν τον ευρύτερα αποδεκτό τρόπο αυθεντικοποίησης, όπου ο χρήστης πιστοποιεί την ορθότητα της ταυτότητάς του κάνοντας χρήση μυστικού κωδικού που είναι γνωστός μόνο σε αυτόν.

των υπό επεξεργασία δεδομένων και τις πιθανές επιπτώσεις που μπορεί να προκληθούν σε περίπτωση μη ορθής λειτουργίας ή διαχείρισής τους<sup>4</sup>, γίνεται επιβεβλημένη η λήψη των πλέον κατάλληλων μέτρων για την ασφάλεια της επεξεργασίας – ιδίως δε της ορθής πιστοποίησης της ταυτότητας των χρηστών. Ως εκ τούτου, με βάση το άρθρο 10 του ν. 2472/1997 αλλά και τους ειδικότερους κανόνες για την αυθεντικοποίηση που προσδιορίζονται στο ΠΠΥΗΔ, η εν λόγω ηλεκτρονική υπηρεσία θα έπρεπε να ενταχθεί, από τον υπεύθυνο επεξεργασίας, σε υψηλό επίπεδο εμπιστοσύνης.

Το επίπεδο που τελικά επελέγη, με βάση τα όσα δήλωσε ο υπεύθυνος επεξεργασίας στην απάντησή του προς την Αρχή, είναι το επίπεδο 2. Ωστόσο, ακόμα και για το επίπεδο 2, θα έπρεπε – βάσει των προαναφερθέντων κανόνων του ΠΠΥΗΔ – να υιοθετηθεί ως μηχανισμός αυθεντικοποίησης η χρήση συνθηματικών, τα οποία συνθηματικά – ως διακριτικά αυθεντικοποίησης – θα έπρεπε να επιδοθούν στους χρήστες με ασφαλή τρόπο (επίπεδο εγγραφής 2). Επισημαίνεται ότι ο μηχανισμός αυθεντικοποίησης που τελικά επελέγη (εισαγωγή ΑΦΜ και ΑΜΚΑ) δεν μπορεί να εκληφθεί ως χρήση συνθηματικού, αφού τα ως άνω στοιχεία ενός υπαλλήλου είναι πιθανό να περιέλθουν εις γνώσιν τρίτου (για παράδειγμα, είναι στοιχεία που κατά κανόνα επεξεργάζονται οι εκκαθαριστές μισθοδοσίας), οπότε και δεν είναι σύμφωνος με τα όσα προβλέπονται στο ΠΠΥΗΔ. Ο υπεύθυνος επεξεργασίας επισήμανε, τόσο κατά την ακρόαση των εκπροσώπων του ενώπιον της Αρχής όσο και στα σχετικά έγγραφά του προς την Αρχή, ότι η επακόλουθη έγγραφη υποβολή των δικαιολογητικών των στοιχείων που δηλώθηκαν από τους απογραφέντες διασφάλιζε την αποτροπή κάθε αθέμιτης ενέργειας – και, κατ' επέκταση, καθιστούσε το συγκεκριμένο μηχανισμό αυθεντικοποίησης επαρκή. Ωστόσο, όπως τελικά προκύπτει από το υπ' αριθμ. πρωτ. 79361/Β2 και ημερομηνίας 21-05-2014 έγγραφο του υπεύθυνου επεξεργασίας, εστάλησαν στο ΑΣΕΠ στοιχεία βάσει των όσων δήλωσαν ηλεκτρονικά οι απογραφέντες, μέσω της προαναφερθείσας μη ασφαλούς διαδικασίας αυθεντικοποίησης, και περαιτέρω δεν υπήρξε έγγραφη επιβεβαίωση ότι τα απεσταλμένα στοιχεία επαληθεύτηκαν από τα προσκομισθέντα δικαιολογητικά. Συνεπώς, ο υπεύθυνος επεξεργασίας δεν αποδεικνύεται ότι υλοποίησε το μηχανισμό αυθεντικοποίησης που περιέγραψε.

Σε κάθε περίπτωση, επισημαίνεται ότι εφόσον μέσω της συγκεκριμένης διαδικτυακής εφαρμογής υπήρχε η πιθανότητα επεξεργασίας ευαίσθητων προσωπικών δεδομένων, τότε θα έπρεπε, με βάση τους ειδικούς κανόνες του ΠΠΥΗΔ, να επιλεγεί το επίπεδο εμπιστοσύνης 3,

---

<sup>4</sup> Προς επίρρωση αυτού, σημειώνουμε επίσης και τη δυνατότητα που φαίνεται ότι παρείχε το σύστημα, με βάση και το σχετικό εγχειρίδιο οδηγιών της εφαρμογής, στους χρήστες του να δηλώσουν οικιοθελώς ότι επιθυμούν να ενταχθούν σε καθεστώς διαθεσιμότητας

γεγονός που με τη σειρά του επιτάσσει την απόδοση διαπιστευτηρίων (π.χ. συνθηματικών) στους χρήστες κατόπιν ασφαλούς διαδικασίας εγγραφής τους (βλ. επίπεδο εγγραφής 3 στο ΠΠΥΗΔ). Εναλλακτικά, τα ευαίσθητα δεδομένα δεν θα έπρεπε να συλλέγονται μέσω της ηλεκτρονικής υπηρεσίας (τα σχετικά δικαιολογητικά εξάλλου υποβάλλονται εγγράφως στο Υπουργείο).

Ως εκ τούτου, ο υπεύθυνος επεξεργασίας δεν ακολούθησε επαρκή μέθοδο αυθεντικοποίησης των χρηστών της εν λόγω υπηρεσίας. Το γεγονός αυτό με τη σειρά του έθεσε σε κίνδυνο την ακρίβεια των δεδομένων (άρθρο 4 παρ. 1 στοιχ. γ' του ν. 2472/1997), αφού για τα ηλεκτρονικώς υποβληθέντα στοιχεία ενός υπαλλήλου δεν υπήρχαν τα εχέγγυα ότι υποβλήθηκαν πράγματι από τον ίδιο - και, συνεπακόλουθα, υπήρξε ο κίνδυνος δυσμενών επιπτώσεων για τους απογραφέντες (βλ. και επόμενη Σκέψη 8).

Περαιτέρω, αναφορικά με τα λοιπά μέτρα για την ασφάλεια της επεξεργασίας, σημειώνεται ότι η ανταλλαγή δεδομένων με την εν λόγω ηλεκτρονική υπηρεσία δεν ήταν κρυπτογραφημένη, αφού δεν ήταν σε λειτουργία το πρωτόκολλο HTTPS. Σημειώνεται ότι η χρήση του πρωτοκόλλου (το οποίο ουσιαστικά βασίζεται στα κρυπτογραφικά πρωτόκολλα SSL/TLS) διασφαλίζει την εμπιστευτικότητα της μεταδιδόμενης πληροφορίας μεταξύ δύο επικοινωνούντων κόμβων (ήτοι του υπολογιστή του χρήστη και της ιστοσελίδας που επισκέπτεται) μέσω κρυπτογράφησης των δεδομένων που ανταλλάσσονται. Με αυτόν τον τρόπο, αποτρέπεται η διαρροή δεδομένων κατά τη μετάδοσή τους, διαμέσου άλλων κόμβων, στο Διαδίκτυο. Για παράδειγμα, επισημαίνεται ότι πολλοί ενδιάμεσοι κόμβοι υποδομής (π.χ. διακομιστές μεσολάβησης - HTTP proxies) πραγματοποιούν προσωρινή αποθήκευση δεδομένων, γεγονός που αυξάνει σημαντικά τον κίνδυνο διαρροής της μεταδιδόμενης πληροφορίας σε τρίτους όταν αυτή δεν είναι κρυπτογραφημένη. Περαιτέρω, ο κίνδυνος αυτός, για την περίπτωση μη κρυπτογραφημένης μετάδοσης, ελλοχεύει και εκ του γεγονότος ότι πολλοί χρήστες διασυνδέονται στο Διαδίκτυο μέσω ασύρματων δικτύων, πολλά εκ των οποίων δεν παρέχουν επαρκή επίπεδα ασφαλείας.

Επιπροσθέτως, η χρήση του πρωτοκόλλου HTTPS, σε συνδυασμό με εγκατάσταση έγκυρων ψηφιακών πιστοποιητικών από την πλευρά του διαδικτυακού εξυπηρετητή, παρέχει στους επισκέπτες του διαδικτυακού τόπου (χρήστες) τη δυνατότητα ελέγχου της γνησιότητας αυτού. Σε διαφορετική περίπτωση, εάν δεν είναι εφικτή η πιστοποίηση του διαδικτυακού τόπου από τους επισκέπτες του, ελλοχεύει ο κίνδυνος διαρροής προσωπικών δεδομένων αφού οι χρήστες δεν είναι δυνατό να γνωρίζουν εγγυημένα αν τα στοιχεία τους υποβάλλονται πράγματι στον αρμόδιο φορέα.

Τέλος, σημειώνεται ότι το πρωτόκολλο SSL διασφαλίζει και την ακεραιότητα της

μεταδιδόμενης πληροφορίας, υπό την έννοια ότι κάθε αλλοίωση/τροποποίηση των δεδομένων κατά τη μετάδοσή τους γίνεται αντιληπτή στον παραλήπτη αυτών.

Ως εκ τούτου, λαμβάνοντας επίσης υπόψη το άρθρο 10 του ν. 2472/1997, αλλά και τη φύση της επεξεργασίας προσωπικών δεδομένων που πραγματοποιήθηκε μέσω του εν λόγω διαδικτυακού τόπου (Αριθμός Φορολογικού Μητρώου, Αριθμός Μητρώου Κοινωνικής Ασφάλισης, λοιπά προσωπικά δεδομένα σχετικά με προσόντα, καθώς και ευαίσθητα δεδομένα υγείας για όσους ενέπιπταν στις συγκεκριμένες εξαιρέσεις), προκύπτει ότι θα έπρεπε για τη συγκεκριμένη υπηρεσία να εφαρμόζεται κρυπτογράφηση με το πρωτόκολλο HTTPS κατά τη μετάδοση και ανταλλαγή δεδομένων, καθώς επίσης και να είναι σε ισχύ, για τον ως άνω διαδικτυακό τόπο, ένα έγκυρο ψηφιακό πιστοποιητικό. Τούτο δε εξάλλου έχει έρεισμα και στα όσα ειδικότερα επισημαίνονται στο Παράρτημα Ι του ΠΠΥΗΔ αυτού, όπου ως υπό διαμόρφωση<sup>5</sup> κανόνας αναφέρεται ότι «τα στοιχεία που ανταλλάσσονται κατά την επικοινωνία ενός χρήστη με ένα Διαδικτυακό Τόπο φορέα της Δημόσιας Διοίκησης να προστατεύονται μέσω χρήσης του πρωτοκόλλου HTTPS, το οποίο να βασίζεται στη χρήση πιστοποιητικών που χαρακτηρίζονται ως ασφαλή από τους κατασκευαστές των φυλλομετρητών, όταν αυτό απαιτείται από τη φύση των στοιχείων».

Συνεπώς, για την περίπτωση του διαδικτυακού τόπου της απογραφής υπαλλήλων, ο υπεύθυνος επεξεργασίας δεν υιοθέτησε τα πλέον ενδεδειγμένα μέτρα για την ασφάλεια της επεξεργασίας (άρθρο 10 του ν. 2472/1997).

8. Παρά το γεγονός ότι οι σχετικοί πίνακες μοριοδότησης των απογραφέντων υπαλλήλων που ανήρτησε το ΑΣΕΠ στις 18 και 21 Νοεμβρίου 2013 με βάση τα στοιχεία που του απέστειλε ο υπεύθυνος επεξεργασίας είναι πλέον άνευ αντικειμένου και δεν έχουν ισχύ, υπήρξε εν τέλει δημοσιοποίηση στο Διαδίκτυο προσωπικών δεδομένων τα οποία δεν ήταν ακριβή. Σημειώνεται δε ότι με βάση τους ανωτέρω πίνακες, οι οποίοι περιείχαν μη ακριβή προσωπικά δεδομένα, εκδόθηκε η με αρ. πρωτ. 178387/B2-21/11/2013 Διαπιστωτική Πράξη του Υπουργού Παιδείας και Θρησκευμάτων που αφορούσε στη διαθεσιμότητα των διοικητικών υπαλλήλων των οκτώ Πανεπιστημίων. Η εν λόγω Διαπιστωτική Πράξη (η οποία εμφανίζει διαφορές ως προς την νεότερη Διαπιστωτική Πράξη που εκδόθηκε το Μάιο του 2014) δεν είναι πλέον σε ισχύ, όπως προκύπτει από τα όσα αναφέρονται στο υπ' αριθμ. πρωτ. 79361/B2/21-05-2014 έγγραφο του υπεύθυνου επεξεργασίας. Ωστόσο, από τα παραπάνω συνάγεται ότι η συγκεκριμένη διαδικασία επέφερε δυσμενείς επιπτώσεις σε

---

<sup>5</sup> Κανόνες υπό Διαμόρφωση/Μελέτη είναι οι κανόνες που έχουν προδιαγραφές, τις οποίες το Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης επεξεργάζεται και ενδέχεται να υιοθετήσει σε επόμενη έκδοσή του.

υποκείμενα των δεδομένων αφού εσφαλμένα αναφέρθηκαν στην πρώτη διαπιστωτική πράξη (υπαγωγή τους σε καθεστώς διαθεσιμότητας, σχετική δημοσιοποίηση στο Διαδίκτυο).

Δεδομένης της διαδικασίας που υιοθέτησε ο υπεύθυνος επεξεργασίας για την απογραφή, η αντιπαραβολή των ηλεκτρονικά δηλωθέντων στοιχείων με τα αντίστοιχα έγγραφα δικαιολογητικά ήταν απαραίτητη διαδικασία για την εξασφάλιση της ακρίβειας των δεδομένων. Η διαδικασία αυτή, όπως αναλύθηκε στη Σκέψη 7, δεν αποδεικνύεται ότι έλαβε χώρα.

Κατά συνέπεια, για την περίπτωση του διαδικτυακού τόπου της απογραφής υπαλλήλων, ο υπεύθυνος επεξεργασίας δεν υιοθέτησε τα πλέον ενδεδειγμένα μέτρα για την ακρίβεια των δεδομένων, το οποίο συνετέλεσε σε δυσμενείς συνέπειες για τα υποκείμενα των δεδομένων (άρθρο 4 παρ. 1 στοιχ. γ' του ν. 2472/1997), έστω και αν η με αρ. πρωτ. 178387/B2-21/11/2013 Διαπιστωτική Πράξη του Υπουργού Παιδείας και Θρησκευμάτων δεν είναι πλέον σε ισχύ.

9. Αναφορικά με τα μέτρα για την προστασία των προσωπικών δεδομένων για το διαδικτυακό τόπο της αίτησης εκπαιδευτών, σημειώνεται επίσης ότι, δεδομένου ότι υφίσταται επεξεργασία ευαίσθητων προσωπικών δεδομένων, θα έπρεπε να είναι σε εφαρμογή τα όσα ρητώς αναφέρονται στο ΠΠΥΗΔ αναφορικά με το επίπεδο εμπιστοσύνης 3 μίας υπηρεσίας – ήτοι οι χρήστες θα έπρεπε να εγγραφούν σε αυτή με ασφαλή τρόπο (βλ. επίπεδο εγγραφής 3, όπως περιγράφεται στο Παράρτημα ΙΙΙ του ΠΠΥΗΔ) προκειμένου να λάβουν τα διαπιστευτήριά τους (π.χ. συνθηματικό), και όχι να επιλέγουν μόνοι τους απομακρυσμένα κάποιο συνθηματικό (η οποία υλοποίηση και τελικά υιοθετήθηκε). Εναλλακτικά, τα ευαίσθητα δεδομένα δεν θα έπρεπε να συλλέγονται μέσω της εν λόγω ηλεκτρονικής υπηρεσίας.

Περαιτέρω, και σε αυτήν την περίπτωση, λαμβάνοντας υπόψη το άρθρο 10 του ν. 2472/1997, αλλά και τη φύση της επεξεργασίας προσωπικών δεδομένων που πραγματοποιήθηκε μέσω του εν λόγω διαδικτυακού τόπου (Αριθμός Φορολογικού Μητρώου, Αριθμός Μητρώου Κοινωνικής Ασφάλισης, λοιπά δεδομένα χρηστών, συμπεριλαμβανομένων ευαίσθητων δεδομένων, συνθηματικό των χρηστών - καθώς επίσης και το γεγονός ότι πολλοί χρήστες συνηθίζουν να χρησιμοποιούν κοινά συνθηματικά για διαφορετικές ηλεκτρονικές υπηρεσίες), προκύπτει ότι θα έπρεπε για τη συγκεκριμένη υπηρεσία, προκειμένου να διασφαλίζεται η εμπιστευτικότητα των δεδομένων, να εφαρμόζεται κρυπτογράφηση κατά τη μετάδοση και ανταλλαγή δεδομένων (πρωτόκολλο HTTPS), καθώς επίσης και να είναι σε ισχύ, για τον ως άνω διαδικτυακό τόπο, ένα έγκυρο ψηφιακό πιστοποιητικό. Ο ισχυρισμός του υπευθύνου επεξεργασίας περί δυνατότητας



υποκλοπής των δεδομένων του χρήστη – λόγω της μη υλοποίησης του πρωτοκόλλου HTTPS - μόνο απευθείας από τον υπολογιστή από όπου εισάγονται τα δεδομένα δεν είναι ακριβής, για τους λόγους που έχουν εξηγηθεί στην ανωτέρω Σκέψη 7.

Συνεπώς, και για την περίπτωση του διαδικτυακού τόπου αίτησης εκπαιδευτών, ο υπεύθυνος επεξεργασίας δεν υιοθέτησε τα πλέον ενδεδειγμένα μέτρα για την ασφάλεια της επεξεργασίας (άρθρο 10 του ν. 2472/1997).

10. Σύμφωνα με το άρθρο 11 του ν. 2472/1997 ο υπεύθυνος επεξεργασίας οφείλει να ενημερώνει τα υποκείμενα των δεδομένων, με τρόπο πρόσφορο και σαφή, για τα βασικά χαρακτηριστικά της επεξεργασίας καθώς και για τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων τους.

Για την περίπτωση του διαδικτυακού τόπου της απογραφής υπαλλήλων, δεν υπήρχε ενημέρωση περί των αποδεκτών των δεδομένων. Ωστόσο, σημειώνεται ότι εφόσον ο σκοπός και τα λοιπά χαρακτηριστικά της συγκεκριμένης επεξεργασίας (μοριοδότηση των δηλωθέντων προσόντων από το ΑΣΕΠ κτλ.) προβλέπεται από διάταξη νόμου, δύναται να θεωρηθεί ότι αποτελεί κοινή γνώση του επιμελούς πολίτη και, κατά συνέπεια, δεν απαιτείται η προηγούμενη ενημέρωση αυτών.

Επομένως, στο βαθμό που στη σχετική ιστοσελίδα ήταν αναρτημένες οι σχετικές διατάξεις, ως προς το σκέλος της ενημέρωσης των υποκειμένων των δεδομένων η καταγγελία δεν ευσταθεί.

11. Ενόψει των παραβάσεων που διαπιστώθηκαν, λαμβάνοντας επίσης υπόψη ότι οι πίνακες μοριοδότησης προσόντων των υπαλλήλων που βασίστηκαν σε μη ακριβή δεδομένα δεν έχουν πλέον ισχύ, η Αρχή κρίνει ότι πρέπει να επιβληθεί στον υπεύθυνο επεξεργασίας η προβλεπόμενη στο άρθρο 21 παρ. 1 στοιχ. α' του ν. 2472/1997 κύρωση της προειδοποίησης όσον αφορά στην ακρίβεια των δεδομένων της απογραφής. Επίσης, η ίδια κύρωση πρέπει να επιβληθεί στον υπεύθυνο επεξεργασίας και για την μη λήψη των ενδεδειγμένων μέτρων ασφαλείας κατά την επεξεργασία προσωπικών δεδομένων μέσω των διαδικτυακών του εφαρμογών..

Ειδικότερα, για οποιαδήποτε διαδικτυακή εφαρμογή του Υπουργείου απαιτείται η σύνδεση χρηστών μέσω διακριτικών αυθεντικοποίησης, θα πρέπει να πληρούνται τα κάτωθι:

α) Ως προς τους μηχανισμούς αυθεντικοποίησης των χρηστών, θα πρέπει να ακολουθούνται τα όσα ρητώς επισημαίνονται στο Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης. Επισημαίνεται ιδιαίτερα ότι σε καμία περίπτωση δεν επιτρέπεται να βασίζεται η αυθεντικοποίηση των χρηστών των διαδικτυακών εφαρμογών μόνο σε αναγνωριστικά τα οποία δύναται να είναι εις γνώσιν άλλων (όπως είναι, για

παράδειγμα, ο Αριθμός Φορολογικού Μητρώου), ακόμα και εάν επίκειται υποβολή εγγράφων αποδεικτικών των υποβληθέντων στοιχείων.

β) Αναφορικά με την απόδοση διαπιστευτηρίων στους χρήστες (ήτοι την εγγραφή τους στις ηλεκτρονικές υπηρεσίες), θα πρέπει να ακολουθούνται τα όσα ρητώς επισημαίνονται στο Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης. Επισημαίνεται ιδιαίτερα ότι, εφόσον πραγματοποιείται επεξεργασία ευαίσθητων προσωπικών δεδομένων μέσω διαδικτυακής εφαρμογής, ο χρήστης θα πρέπει να παραλαμβάνει τα διακριτικά αυθεντικοποίησής του με φυσική του παρουσία στην αρμόδια Υπηρεσία, σύμφωνα με τα όσα αναφέρονται στο Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης.

γ) Η σύνδεση των χρηστών με τη διαδικτυακή εφαρμογή θα πρέπει να είναι κρυπτογραφημένη με χρήση του πρωτοκόλλου HTTPS, το οποίο να βασίζεται στη χρήση πιστοποιητικών που χαρακτηρίζονται ως ασφαλή από τα προγράμματα πλοήγησης στο Διαδίκτυο (φύλλομετρητές).

#### ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,

Απευθύνει, με βάση το άρθρο 21 παρ. 1 στοιχ. α' του ν. 2472/1997, αυστηρή προειδοποίηση στο Υπουργείο Παιδείας και Θρησκευμάτων, ως υπεύθυνο επεξεργασίας, για παραβίαση του άρθρου 4 παρ. 1 στοιχ. γ' του ν. 2472/1997 και για την παραβίαση του άρθρου 10 του ν. 2472/1997.

Καλεί το Υπουργείο Παιδείας να εφαρμόζει κατάλληλα μέτρα ασφάλειας κατά την επεξεργασία προσωπικών δεδομένων μέσω των διαδικτυακών του εφαρμογών, όπως αυτά περιγράφονται στο σημείο 11 του σκεπτικού της παρούσας.

**Ο Πρόεδρος**

**Η γραμματέας**

**Πέτρος Χριστόφορος**

**Ειρήνη Παπαγεωργοπούλου**

## **Αποδέκτες**

α) Υπουργείο Παιδείας και Θρησκευμάτων

Ανδρέα Παπανδρέου 37,

Μαρούσι, 15180

β) Δημήτριος Λαμπράκης

Ηλεκτρονική Διεύθυνση: [dlab@central.ntua.gr](mailto:dlab@central.ntua.gr)

γ) Αχιλλέας Μαλισώβας

Ηλεκτρονική Διεύθυνση: [malislak@yahoo.gr](mailto:malislak@yahoo.gr)

## **Κοινοποίηση:**

α) Υπουργείο Παιδείας και Θρησκευμάτων

Γενική Διεύθυνση Διοικητικής Υποστήριξης

Δ/ση Λειτουργικής Ανάπτυξης Πληροφοριακών Συστημάτων

Ανδρέα Παπανδρέου 37,

Μαρούσι, 15180

β) Υπουργείο Παιδείας και Θρησκευμάτων

Διεύθυνση Προσωπικού Ανώτατης

Πανεπιστημιακής Εκπαίδευσης

Τμήμα Γ' Διοικητικού Προσωπικού

Ανδρέα Παπανδρέου 37,

Μαρούσι, 15180

γ) Υπουργείο Παιδείας και Θρησκευμάτων

Γενική Γραμματεία Δια Βίου Μάθησης

Διεύθυνση Διοικητικού - Οικονομικού

Τμήμα Διοικητικού

Ανδρέα Παπανδρέου 37,

Μαρούσι, 15180

## Τίτλος

Επεξεργασία προσωπικών δεδομένων μέσω διαδικτυακών τόπων του Υπουργείου Παιδείας

## Σύνοψη

Διαβιβάστηκαν στην Αρχή, από την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), δύο καταγγελίες σχετικά με την επεξεργασία προσωπικών δεδομένων χρηστών δύο διαδικτυακών τόπων του Υπουργείου Παιδείας και Θρησκευμάτων (εφεξής, υπεύθυνος επεξεργασίας). Η πρώτη καταγγελία αφορούσε το διαδικτυακό τόπο <http://odysseas.it.minedu.gov.gr/>, μέσω του οποίου απογράφησαν οι υπάλληλοι συγκεκριμένων κλάδων οκτώ Πανεπιστημίων, σύμφωνα με την υπ' αριθμ. ΔΠΠΔΔ/Β.2/Δ/33/οικ.27653/11-10-2013 Υπουργική Απόφαση. Όπως αναφέρεται στην ως άνω καταγγελία, η σύνδεση των χρηστών στον ανωτέρω διαδικτυακό τόπο δεν ήταν κρυπτογραφημένη, ενώ επίσης δεν ήταν σε ισχύ επαρκείς μηχανισμοί για την αυθεντικοποίηση των χρηστών της συγκεκριμένης διαδικτυακής εφαρμογής, αφού για την πρόσβαση σε αυτή απαιτείτο η εισαγωγή προσωπικών στοιχείων του εκάστοτε υπαλλήλου τα οποία δύνανται να γνωρίζουν και άλλοι, χωρίς να πραγματοποιείται κανένας άλλος έλεγχος σχετικά με την επιβεβαίωση της ταυτότητάς του. Η δεύτερη καταγγελία αφορούσε την ασφάλεια του διαδικτυακού τόπου <http://iekteachers.sch.gr/Login>, μέσω του οποίου καθηγητές υπέβαλαν αιτήσεις για απασχόληση σε Δημόσια ΙΕΚ. Ειδικότερα, με βάση την καταγγελία, τα δεδομένα που αποστέλλονται στον ανωτέρω διαδικτυακό τόπο, όπως ο Αριθμός Φορολογικού Μητρώου και ο Αριθμός Μητρώου Κοινωνικής Ασφάλισης, δεν είναι κρυπτογραφημένα.

Ο υπεύθυνος επεξεργασίας, μετά τις έγγραφες απόψεις του που υπέβαλε στην Αρχή επί των ανωτέρω ζητημάτων, κλήθηκε νομίμως σε ακρόαση ενώπιον της Αρχής στη συνεδρίαση της 26-03-2014 για να δώσει περαιτέρω διευκρινίσεις και να εκθέσει διεξοδικά τις απόψεις του. Ακολούθως, υπέβαλε εκ νέου υπομνήματα αλλά και συμπληρωματικά έγγραφα επί των καταγγελλομένων.

Η Αρχή, μετά την εξέταση του συνόλου των στοιχείων, έκρινε ότι πρέπει να επιβληθεί στον υπεύθυνο επεξεργασίας η προβλεπόμενη στο άρθρο 21 παρ. 1 στοιχ. α' του ν. 2472/1997 κύρωση της προειδοποίησης για παραβίαση του άρθρου 4 παρ. 1 στοιχ. γ' του ν. 2472/1997 (ακρίβεια των δεδομένων), αναφορικά με το διαδικτυακό τόπο της απογραφής των υπαλλήλων. Επίσης, η ίδια κύρωση πρέπει να επιβληθεί στον υπεύθυνο επεξεργασίας και για την μη λήψη των ενδεδειγμένων μέτρων ασφαλείας κατά την επεξεργασία προσωπικών δεδομένων μέσω των διαδικτυακών του εφαρμογών (άρθρο 10 του ν. 2472).

Ειδικότερα, κάλεσε τον υπεύθυνο επεξεργασίας, για οποιαδήποτε διαδικτυακή εφαρμογή απαιτείται η σύνδεση χρηστών μέσω διακριτικών αυθεντικοποίησης, να διασφαλίσει ότι πληρούνται τα κάτωθι:

α) Ως προς τους μηχανισμούς αυθεντικοποίησης των χρηστών, θα πρέπει να ακολουθούνται τα όσα ρητώς επισημαίνονται στο Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης. Επισημαίνεται ιδιαίτερα ότι σε καμία περίπτωση δεν επιτρέπεται να βασίζεται η αυθεντικοποίηση των χρηστών των διαδικτυακών εφαρμογών μόνο σε αναγνωριστικά τα οποία δύνανται να είναι εις γνώσιν άλλων (όπως είναι, για παράδειγμα, ο Αριθμός Φορολογικού Μητρώου), ακόμα και εάν επίκειται υποβολή εγγράφων αποδεικτικών των υποβληθέντων στοιχείων.

β) Αναφορικά με την απόδοση διαπιστευτηρίων στους χρήστες (ήτοι την εγγραφή τους στις ηλεκτρονικές υπηρεσίες), θα πρέπει να ακολουθούνται τα όσα ρητώς επισημαίνονται στο Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης. Επισημαίνεται ιδιαίτερα ότι, εφόσον πραγματοποιείται επεξεργασία ευαίσθητων προσωπικών δεδομένων μέσω διαδικτυακής εφαρμογής, ο χρήστης θα πρέπει να παραλαμβάνει τα διακριτικά αυθεντικοποίησής του με φυσική του παρουσία στην αρμόδια Υπηρεσία, σύμφωνα με τα όσα αναφέρονται στο Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης.

γ) Η σύνδεση των χρηστών με τη διαδικτυακή εφαρμογή θα πρέπει να είναι κρυπτογραφημένη με χρήση του πρωτοκόλλου HTTPS, το οποίο να βασίζεται στη χρήση πιστοποιητικών που χαρακτηρίζονται ως ασφαλή από τα προγράμματα πλοήγησης στο Διαδίκτυο (φυλλομετρητές).