ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 26-05-2014

Αριθ. Πρωτ.: Γ/ΕΞ/3286/26-05-2014

Α Π Ο Φ Α Σ Η ΑΡ. 57/2014

(Τμήμα)

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνεδρίασε σε σύνθεση Τμήματος στην έδρα της την 06-05-2014 και ώρα 10:00 μετά από πρόσκληση του Προέδρου της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν ο Πέτρος Χριστόφορος, Πρόεδρος της Αρχής και τα αναπληρωματικά μέλη Σπυρίδων Βλαχόπουλος, Γρηγόριος Λαζαράκος, ως εισηγητής, και Χαράλαμπος Ανθόπουλος, σε αντικατάσταση των τακτικών μελών Λεωνίδα Κοτσαλή, Αναστάσιου – Ιωάννη Μεταξά και Δημήτριο Μπριόλα, αντίστοιχα, οι οποίοι, αν και εκλήθησαν νομίμως εγγράφως, δεν παρέστησαν λόγω κωλύματος. Παρόντες χωρίς δικαίωμα ψήφου ήταν ο Κωνσταντίνος Λιμνιώτης, πληροφορικός ελεγκτής, ως βοηθός εισηγητή και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών και οικονομικών υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Υποβλήθηκε στην Αρχή η υπ' αριθμ. πρωτ. Γ/ΕΙΣ/7242/14-11-2013 καταγγελία του Α, αναφορικά με δυνατότητα διαρροής προσωπικών δεδομένων μέσω της διαδικτυακής υπηρεσίας που παρέχει στους ασφαλισμένους του ο Οργανισμός Ασφάλισης Ελεύθερων Επαγγελματιών - ΟΑΕΕ (εφεξής, υπεύθυνος επεξεργασίας). Η Αρχή ενημέρωσε τον καταγγέλλοντα με το υπ' αριθμ. πρωτ. Γ/ΕΞ/7242-1/02-12-2013 ότι, από τις 19-11-2013

που εξέτασε την καταγγελία, δεν υπήρξε η δυνατότητα διαπίστωσης των καταγγελλομένων, ενώ ακολούθως ο καταγγέλλων απάντησε με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/8004/17-12-2013 έγγραφο, στο οποίο αναφέρει ότι το κενό ασφαλείας είχε επιλυθεί την επομένη ημέρα της καταγγελίας του (την οποία καταγγελία είχε αποστείλει και στον υπεύθυνο επεξεργασίας), αλλά ωστόσο επισημαίνει ότι δεν υπήρξε από τον οργανισμό ενημέρωση των ασφαλισμένων του που έχουν ηλεκτρονικό λογαριασμό στις διαδικτυακές του υπηρεσίες περί της πιθανότητας να έχει υπάρξει διαρροή προσωπικών τους δεδομένων.

Ακολούθως η Αρχή απέστειλε στον υπεύθυνο επεξεργασίας το υπ' αριθμ. πρωτ. Γ/ΕΞ/7242-2/19-12-2013 έγγραφο, με το οποίο ζητούσε διευκρινίσεις και απόψεις επί των καταγγελλομένων. Ο υπεύθυνος επεξεργασίας απάντησε με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/231/16-01-2014 έγγραφο. Η Αρχή στη συνέχεια, κατόπιν και συμπληρωματικών στοιχείων που υπέβαλε ο καταγγέλλων με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/1037/17-02-2014 έγγραφο, ζήτησε από τον υπεύθυνο επεξεργασίες συμπληρωματικές διευκρινίσεις με το υπ' αριθμ. πρωτ. Γ/ΕΞ/1058/17-02-2014 έγγραφό της, στο οποίο ο υπεύθυνος επεξεργασίας απάντησε με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/1199/20-02-2014 έγγραφο.

Τόσο στα ως άνω έγγραφα του καταγγέλλοντα, όσο και στις ως απαντήσεις του υπεύθυνου επεξεργασίας, σημειώνονται τα κάτωθι όσον αφορά τη φύση του περιστατικού ασφαλείας:

α) Στις 13-11-2013, ένας επισκέπτης του διαδικτυακού τόπου του υπευθύνου επεξεργασίας[1] μπορούσε, πληκτρολογώντας απλά το όνομα χρήστη (login name) της σχετικής υπηρεσίας και αφήνοντας κενό το συνθηματικό, να δει στην οθόνη το συνθηματικό του χρήστη αυτού για την εν λόγω υπηρεσία – οπότε, ακολούθως, είχε τη δυνατότητα να συνδεθεί στο σύστημα με τα στοιχεία αυτού του χρήστη.

β) Πραγματοποιώντας κάποιος σύνδεση με τα στοιχεία τρίτου, αποκτούσε πρόσβαση στις βεβαιώσεις αποδοχών αυτού, σε ενημερωτικά σημειώματα συντάξεων και σε βεβαιώσεις εισφορών. Τα προσωπικά δεδομένα που εμπεριέχονται στα ως άνω έγγραφα είναι, μεταξύ άλλων: ονοματεπώνυμο, πατρώνυμο, τόπος κατοικίας, Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ), Αριθμός Φορολογικού Μητρώου (ΑΦΜ), Αρ. ταυτότητας, είδος αποδοχών, ακαθάριστο ποσό αλλά και καθαρό φορολογητέο ποσό, ειδική εισφορά (ν. 3986/2011), ασφαλιστικές αλλά και λοιπές κρατήσεις, μηνιαία σύνταξη, εξιδρωματικό επίδομα, επίδομα απολύτου αναπηρίας, επίδομα αεροθεραπείας, οικονομική ενίσχυση, ΕΚΑΣ, κατασχέσεις και λοιπές οφειλές.

[1] Ο διαδικτυακός αυτός τόπος είναι ο https://www.oaee.gr/login.asp.

γ) Την επόμενη ημέρα, στις 14-11-2013, το ως άνω πρόβλημα έπαψε να υφίσταται (ήδη ο υπεύθυνος επεξεργασίας είχε λάβει την καταγγελία από τον καταγγέλλοντα).

δ) Δεν υπήρχε η δυνατότητα, κατά τη διάρκεια του ανωτέρω προβλήματος, μαζικής μεταφόρτωσης αρχείων από τη βάση δεδομένων του υπευθύνου επεξεργασίας (και άρα διαρροής ολόκληρης της βάσης των προσωπικών δεδομένων των ασφαλισμένων). Για να αποκτήσει κάποιος τρίτος πρόσβαση σε προσωπικά δεδομένα ασφαλισμένων του οργανισμού, θα έπρεπε να μαντέψει σωστά το όνομα που έχει ένας ασφαλισμένος ως χρήστης της υπηρεσίας (δηλ. το όνομα χρήστη) - οπότε και, ακολούθως, μπορούσε να δει το συνθηματικό του και, κατ' επέκταση, να εισέλθει στην εφαρμογή με τα στοιχεία αυτά. Σημειώνεται ωστόσο ότι υπήρχαν χρήστες με εύκολα προβλέψιμο όνομα χρήστη (ήδη ο καταγγέλλων μάντεψε σωστά περισσότερα από είκοσι (20) ονόματα χρηστών – κατονομάζει κάποια εξ αυτών στα έγγραφά του, ενώ επισημαίνει ότι αυτό έγινε εύκολα, σε πολύ μικρό χρονικό διάστημα).

ε) Ο οργανισμός προέβη σε προληπτικό «κλείδωμα» όλων των λογαριασμών των χρηστών της υπηρεσίας, καθώς και στην ανάρτηση μηνύματος, κατά τη σύνδεση, για υποχρεωτική αλλαγή του συνθηματικού: η αλλαγή αυτή μπορούσε να γίνει μόνο με χρήση κλειδάριθμου ενεργοποίησης που έχει ο κάθε χρήστης και τον γνωρίζει μόνο αυτός, ο οποίος δεν μπορεί να υποκλαπεί από τον ως άνω διαδικτυακό τόπο. Ωστόσο, με βάση τα έγγραφα του καταγγέλλοντα, οι ανωτέρω ενέργειες του υπευθύνου επεξεργασίας δεν έλαβαν χώρα αμέσως μετά τη γνωστοποίηση του προβλήματος (φαίνεται ότι έγιναν μετά την αποστολή του πρώτου εγγράφου της Αρχής προς τον υπεύθυνο επεξεργασίας).

Περαιτέρω, ως προς τις επιμέρους λεπτομέρειες για τα χαρακτηριστικά του εν λόγω προβλήματος, το μέγεθος της διαρροής δεδομένων, αλλά και τις ενέργειες αποκατάστασής του, ο υπεύθυνος επεξεργασίας στα έγγραφά του επισημαίνει τα εξής:

α) Κατά το χρονικό διάστημα από 13-11-2013 (και ώρα 18:00) μέχρι και 14-11-2013 (πρώτες πρωινές ώρες), στο πλαίσιο εργασιών συντήρησης και διαφόρων αλλαγών που πραγματοποιούντο στον κώδικα της ιστοσελίδας του υπευθύνου επεξεργασίας, ενεργοποιήθηκε εκ παραδρομής μία δοκιμαστική σελίδα (test page) η οποία βρέθηκε σε κοινή θέα - η οποία σελίδα, αν κάποιος εισήγαγε ένα όνομα χρήστη και ένα οποιοδήποτε συνθηματικό, θα επέστρεφε το πραγματικό συνθηματικό του χρήστη. Εφόσον λοιπόν κάποιος τρίτος χρησιμοποιούσε το όνομα ενός χρήστη και το συνθηματικό του, θα πραγματοποιούσε επιτυχή σύνδεση στη διαδικτυακή υπηρεσία του υπευθύνου επεξεργασίας, αλλά όμως σε περιβάλλον που θα επέτρεπε μόνο ανάγνωση και καμία μεταβολή στοιχείων: ακόμα και αν τροποποιούσε στοιχεία πληκτρολογώντας νέα στις

εμφανιζόμενες φόρμες εισαγωγής στοιχείων, δεν γινόταν καμία καταχώρηση στη βάση δεδομένων – συνεπώς, ο κακόβουλος χρήστης θα είχε απλά την αίσθηση[2] πως θα μπορούσε να αλλοιώσει τα στοιχεία επικοινωνίας του χρήστη, χωρίς αυτό να γίνεται πραγματικά, για το λόγο ότι, όπως ο υπεύθυνος επεξεργασίας επισημαίνει, τα στοιχεία επικοινωνίας που δηλώνουν οι χρήστες καταχωρούνται σε διαφορετική βάση δεδομένων και σε διαφορετικό σύστημα από αυτό που περιέχει τα ασφαλιστικά-συνταξιοδοτικά προσωπικά στοιχεία, χωρίς να υπάρχει διασύνδεση μεταξύ τους.

β) Όταν το ανωτέρω λάθος έγινε αντιληπτό από τον προγραμματιστή της εταιρείας συντήρησης (WEB INTELLIGENCE), το πρόβλημα αποκαταστάθηκε με την επαναφορά του παραγωγικού περιβάλλοντος λειτουργίας.

γ) Η εταιρεία συντήρησης απέστειλε στις 08-01-2014 γραπτή απάντηση στον υπεύθυνο επεξεργασίας (την οποία ο τελευταίος κοινοποίησε στην Αρχή με το τελευταίο έγγραφό του), όπου - πέραν του χρονικού διαστήματος στο οποίο εμφανιζόταν το πρόβλημα και της μη δυνατότητας τροποποίησης στοιχείων - επισημαίνει ότι δεν υπάρχουν στοιχεία καταγραφής εισόδου στο σύστημα διότι η παροχή αυτής της υπηρεσίας δεν είχε ζητηθεί. Αναφέρει επίσης ότι, πλέον, ανά τακτά χρονικά διαστήματα το σύστημα δεν επιτρέπει στους χρήστες του να το προσπελάσουν εάν δεν κάνουν ενεργοποίηση του λογαριασμού τους μέσω του «ειδικού κωδικού» που έχουν λάβει από τα αντίστοιχα τμήματα του οργανισμού κατά την υποχρεωτική τους – για την αρχική ενεργοποίηση του λογαριασμού – επίσκεψη σε αυτά.

δ) Το πλήθος των ενεργοποιημένων χρηστών της εν λόγω διαδικτυακής υπηρεσίας είναι 1293 (επί συνόλου 800.000 ασφαλισμένων και 300.000 συνταξιούχων του οργανισμού).

Η Αρχή, αφού άκουσε τον εισηγητή και το βοηθό εισηγητή, ο οποίος στη συνέχεια αποχώρησε, 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

[2] Τη δυνατότητα αλλαγής στοιχείων την επισήμανε και ο καταγγέλλων στα έγγραφά του προς την Αρχή.

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 η 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».

Περαιτέρω, 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, ενώ ως εκτελών την επεξεργασία ορίζεται οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου επεξεργασίας (φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός).

2. Όπως ορίζεται στο άρθρο 4, παρ. 1, εδ. α' του ν. 2472/1997 τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών.

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. Οι υποχρεώσεις του άρθρου αυτού βαρύνουν επίσης και τον εκτελούντα την επεξεργασία.

Εξάλλου, αναφορικά με τις υπηρεσίες ηλεκτρονικής διακυβέρνησης, στο άρθρο 7 του ν. 3979/2011 επισημαίνεται μεταξύ άλλων ότι κατά το σχεδιασμό, διαμόρφωση και προμήθεια πληροφοριακών συστημάτων και υπηρεσιών ηλεκτρονικής διακυβέρνησης πρέπει να γίνεται αξιολόγηση των επιπτώσεών τους στην ιδιωτικότητα και στην προστασία των δεδομένων προσωπικού χαρακτήρα.

3α. Ειδικότερα, 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) και, ειδικότερα, στο Παράρτημα ΙΙΙ αυτού. Όπως επισημαίνεται στο εν λόγω Πλαίσιο (εφεξής, ΠΠΥΗΔ), οι διαδικασίες εγγραφής και αυθεντικοποίησης των χρηστών καθορίζονται από το επίπεδο εμπιστοσύνης στο οποίο εντάσσονται οι παρεχόμενες ηλεκτρονικές υπηρεσίες. Ειδικότερα, τα επίπεδα εμπιστοσύνης είναι τέσσερα, και αριθμούνται από 0 (το χαμηλότερο) έως 3 (το υψηλότερο). Σημειώνεται ότι υπηρεσίες που απαιτούν ανταλλαγή ευαίσθητων προσωπικών δεδομένων εντάσσονται στο επίπεδο εμπιστοσύνης 3. Περαιτέρω, στο ΠΠΥΗΔ επισημαίνονται ως υποχρεωτικοί κανόνες, 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. 297 στο Παράρτημα ΙΙΙ του ΠΠΥΗΔ), καθώς επίσης και ακολούθως το επίπεδο εμπιστοσύνης στο οποίο εντάσσεται η συγκεκριμένη υπηρεσία (βλ. Κ.Υ. 298 στο Παράρτημα ΙΙΙ του ΠΠΥΗΔ).

ii) Υπηρεσίες που έχουν ενταχθεί στο επίπεδο εμπιστοσύνης 3 πρέπει να υιοθετήσουν επίπεδο εγγραφής 2 και επίπεδο αυθεντικοποίησης τουλάχιστον 1, ενώ συνιστάται επίπεδο αυθεντικοποίησης 2 (βλ. Κ.Υ. 302 στο Παράρτημα ΙΙΙ του ΠΠΥΗΔ).

iii) Υπηρεσίες που έχουν υιοθετήσει το επίπεδο αυθεντικοποίησης 1 πρέπει να αξιοποιήσουν ως μηχανισμό αυθεντικοποίησης κατ' ελάχιστο τα συνθηματικά (βλ. Κ.Υ. 303 στο Παράρτημα ΙΙΙ του ΠΠΥΗΔ).

Σημειώνεται ότι τα επίπεδα εγγραφής περιγράφονται επίσης στο ΠΠΥΗΔ: ιδιαίτερα επισημαίνεται ότι, για την περίπτωση του επιπέδου εγγραφής 3, ο χρήστης τελικά 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.

4. Η Αρχή είχε ήδη ενημερώσει τον υπεύθυνο επεξεργασίας, κατόπιν σχετικού έγγραφου ερωτήματος του τελευταίου, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/102/10-01-2013 έγγραφό της, για τις διαδικασίες ασφαλούς εγγραφής και αυθεντικοποίησης των χρηστών των διαδικτυακών του υπηρεσιών οι οποίες πρέπει να υλοποιηθούν, καθώς επίσης και για λοιπά μέτρα ασφάλειας που πρέπει να ληφθούν. Ειδικότερα, στο ως άνω έγγραφο είχε επισημάνει ότι οι παρεχόμενες διαδικτυακές υπηρεσίες κρίνεται σκόπιμο να ενταχθούν στο υψηλότερο επίπεδο εμπιστοσύνης που ορίζεται στο ΠΠΥΗΔ – ήτοι, στο επίπεδο 3 – αφού μέσω αυτών δύναται να πραγματοποιηθεί και επεξεργασία ευαίσθητων δεδομένων. Κατά συνέπεια, θα έπρεπε να έχει υλοποιηθεί και μηχανισμός αυθεντικοποίησης που να αντιστοιχεί στα υψηλότερα επίπεδα αυθεντικοποίησης, δηλ. στα επίπεδα 1 ή 2 όπως αυτά ορίζονται στο ΠΠΥΗΔ, ενώ επίσης και το επίπεδο εγγραφής πρέπει να είναι υψηλό (ήτοι 3, όπως αυτό ορίζεται επίσης στο Πλαίσιο).

Περαιτέρω, η Αρχή στο ως άνω έγγραφό της ενημέρωσε τον υπεύθυνο επεξεργασίας ότι θα πρέπει να ληφθούν και περαιτέρω τεχνικά μέτρα προκειμένου να διασφαλίζεται η ασφάλεια και το απόρρητο της επεξεργασίας (όπως άλλωστε επιτάσσει και το άρθρο 10 του ν. 2472/1997), στα οποία πρέπει να συγκαταλέγονται τα κάτωθι: α) χρήση κρυπτογράφησης κατά τη μετάδοση και ανταλλαγή δεδομένων (πρωτόκολλα SSL και HTTPS), β) ο διαδικτυακός τόπος του υπεύθυνου επεξεργασίας πρέπει να έχει ένα έγκυρο και αναγνωρισμένο ψηφιακό πιστοποιητικό, γ) τα συνθηματικά των χρηστών δεν πρέπει να τηρούνται σε πρωτογενή μορφή αλλά σε μη αναγνώσιμη (με χρήση αλγόριθμου κατακερματισμού - hash), ούτε επίσης να αποστέλλονται στους χρήστες τους μέσω ηλεκτρονικού ταχυδρομείου. Τα παραπάνω θα έπρεπε να έχουν υλοποιηθεί στο πλαίσιο μίας γενικότερης πολιτικής ασφαλείας που πρέπει να υιοθετήσει και εφαρμόσει ο υπεύθυνος επεξεργασίας για την προστασία των προσωπικών δεδομένων των ασφαλισμένων.

5. Ως περιστατικό παραβίασης προσωπικών δεδομένων θεωρείται κάθε περίπτωση παραβίασης της ασφάλειας των δεδομένων όπως τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη διάδοση ή προσπέλαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που διαβιβάσθηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατά οποιονδήποτε άλλον τρόπο σε επεξεργασία στο πλαίσιο του χρησιμοποιούμενου συστήματος επεξεργασίας (βλ. επίσης και άρθρο 2 του ν. 3471/2006 για την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, όπως τροποποιήθηκε με το ν. 4070/2012).

Το συγκεκριμένο περιστατικό αφορά στη διαρροή προσωπικών δεδομένων ορισμένων χρηστών (ασφαλισμένων) της διαδικτυακής υπηρεσίας του υπεύθυνου επεξεργασίας σε τρίτους (ήτοι σε άλλους χρήστες της ίδιας εφαρμογής, αλλά επίσης - με μικρότερη πιθανότητα - και σε άλλους απλούς επισκέπτες του συγκεκριμένου διαδικτυακού τόπου, εφόσον οι τελευταίοι επιχειρούσαν προσπάθεια παράνομης πρόσβασης). Ως εκ τούτου αποτελεί περιστατικό παραβίασης των προσωπικών δεδομένων των εν λόγω χρηστών, καθώς τα προσωπικά δεδομένα τους διέρρευσαν σε μη εξουσιοδοτημένα πρόσωπα.

6. Από την εξέταση του φακέλου της υπόθεσης, προκύπτει ότι το εν λόγω περιστατικό οφείλεται σε αβλεψία της εταιρείας συντήρησης (εκτελούντος την επεξεργασία), η οποία ενεργοποίησε αθέλητα μία διαδικτυακή δοκιμαστική σελίδα στην οποία δεν θα έπρεπε να έχει πρόσβαση το ευρύ κοινό. Το μέγεθος της διαρροής δεδομένων, ήτοι το πλήθος και ακριβές είδος των δεδομένων που διέρρευσαν, καθώς και το πλήθος μη εξουσιοδοτημένων χρηστών που απέκτησαν πρόσβαση σε αυτά, δεν μπορεί να αποσαφηνιστεί, λόγω του ότι δεν είχε υλοποιηθεί η κατάλληλη υπηρεσία καταγραφής όλων των προσβάσεων των χρηστών. Ωστόσο, από το γεγονός ότι οι εγγεγραμμένοι χρήστες στην εν λόγω υπηρεσία ήταν 1293, που αντιστοιχούν σε χαμηλό ποσοστό επί του συνολικού πλήθους των ασφαλισμένων και συνταξιούχων, σε συνδυασμό με το ότι δεν ήταν εφικτή η μαζική μεταφόρτωση των δεδομένων των εγγεγραμμένων χρηστών - αλλά υπό προϋποθέσεις μπορούσε κανείς να προσπελαύνει τα δεδομένα μεμονωμένα για κάθε χρήστη - αλλά και από το ότι η εν λόγω σελίδα – που αποτέλεσε πηγή της διαρροής – φαίνεται ότι ήταν δημόσια προσβάσιμη για χρονικό διάστημα μικρότερο των 12 ωρών, προκύπτει ότι, πιθανότατα, δεν υπήρξε ευρεία διάδοση μεγάλου όγκου δεδομένων σε μεγάλο πλήθος ατόμων. Παρόλα αυτά, το είδος των δεδομένων που ενδεχομένως διέρρευσαν - έστω και αν αφορά μικρό πλήθος υποκειμένων των δεδομένων - είναι ιδιαίτερα κρίσιμο, όπως περιγράφεται στο ιστορικό της παρούσας, ενώ επίσης ήταν δυνατό να είχε συμπεριλάβει μέχρι και ευαίσθητα δεδομένα. Περαιτέρω, η διαρροή του συνθηματικού ενός χρήστη μπορεί να οδηγήσει και σε περαιτέρω δυσμενείς συνέπειες για τον ίδιο, εάν χρησιμοποιεί το ίδιο συνθηματικό και σε άλλες υπηρεσίες.

Σημειώνεται ότι ο υπεύθυνος επεξεργασίας είχε ήδη υλοποιήσει πλήθος μέτρων ασφάλειας για την επεξεργασία, συμμορφούμενος σε μεγάλο βαθμό και με τις προτάσεις που του είχε ήδη απευθύνει η Αρχή με το από 10-01-2013 έγγραφό της αλλά και με τα όσα προδιαγράφονται στο ΠΠΥΗΔ. Συγκεκριμένα, με βάση τα όσα επισημαίνει στο υπ’ αριθμ. πρωτ. Γ/ΕΙΣ/231/16-01-2014 έγγραφό του, για την αρχική εγγραφή των χρηστών της υπηρεσίας και την απόδοση διαπιστευτηρίων απαιτείται η φυσική τους παρουσία σε

κάποιο τμήμα του Οργανισμού, προσκομίζοντας στοιχεία που αποδεικνύουν την ταυτότητά τους[3], ενώ επίσης οι παρεχόμενες διαδικτυακές υπηρεσίες είναι κρυπτογραφημένες με χρήση του πρωτοκόλλου SSL[4]. Στο ίδιο έγγραφο επισημαίνεται ότι ο εν λόγω διαδικτυακός τόπος φιλοξενείται στην ΟΤΕΝΕΤ, από την οποία εφαρμόζονται όλες οι πολιτικές για την ασφάλεια των συστημάτων και δεδομένων. Ωστόσο, ο υπεύθυνος επεξεργασίας δεν είχε υλοποιήσει την πρόταση της Αρχής περί αποθήκευσης των συνθηματικών κατά τρόπο τέτοιο ώστε να είναι μη αναγνώσιμα (βλ. σκέψη 4)· όπως δε αναφέρει στο υπ' αριθμ. πρωτ. Γ/ΕΙΣ/1199/20-02-2014 έγγραφό του, η υλοποίηση αυτής τη πρότασης ήταν σε εξέλιξη το συγκεκριμένο χρονικό διάστημα που έλαβε χώρα το περιστατικό παραβίασης δεδομένων. Σημειώνεται ιδιαίτερα ότι, εάν είχε υλοποιηθεί η πρόταση της Αρχής, το συγκεκριμένο περιστατικό θα είχε αποτραπεί, αφού δεν θα υπήρχε η δυνατότητα εμφάνισης στην οθόνη του συνθηματικού κανενός χρήστη, ακόμα και αν λανθασμένα ενεργοποιούταν - όπως έγινε - η εν λόγω δοκιμαστική ιστοσελίδα.

Όπως στο ιστορικό αναφέρεται, ο υπεύθυνος επεξεργασίας, μόλις έλαβε γνώση του περιστατικού, έλαβε μέτρα για την αντιμετώπισή του όσον αφορά στην αποκατάσταση της διαδικτυακής υπηρεσίας. Παρόλα αυτά, δεν φαίνεται να υπήρξε άμεση ενημέρωση των χρηστών της ως προς το συμβάν, ενώ επίσης οι τελευταίοι δεν υποχρεώθηκαν αμέσως να αλλάξουν το συνθηματικό που χρησιμοποιούσαν για την πρόσβαση σε αυτή.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή Προστασίας Δεδομένων, λαμβάνοντας υπόψη τη φύση του περιστατικού, την αντίδραση του υπεύθυνου επεξεργασίας όταν έλαβε γνώση αυτού, καθώς επίσης και τα μέτρα ασφαλείας που ήδη είχε θέσει σε εφαρμογή ο υπεύθυνος επεξεργασίας, απευθύνει με βάση το άρθρο 21 παρ. 1 στοιχ. α' του ν. 2472/1997 αυστηρή προειδοποίηση στον Οργανισμό Ασφάλισης Ελεύθερων Επαγγελματιών, ως υπεύθυνο επεξεργασίας, να προβεί στις ακόλουθες ενέργειες, καθώς επίσης και να ενημερώσει σχετικά την Αρχή εντός τριών (3) μηνών από την κοινοποίηση της παρούσας Απόφασης, αναφορικά με την εκπλήρωση των υποχρεώσεων που απορρέουν από το άρθρο 10 του ν. 2472/1997:

[3] Τα στοιχεία αυτά είναι η αστυνομική ταυτότητα, το εκκαθαριστικό σημείωμα και η βεβαίωση ΑΜΚΑ.
[4] Με χρήση αναγνωρισμένου και έγκυρου ψηφιακού πιστοποιητικού για την ιστοσελίδα, όπως διαπιστώθηκε μετά την εξέταση αυτής.

α) Να ενημερώσει άμεσα, με πρόσφορο τρόπο, όλους τους χρήστες της διαδικτυακής του υπηρεσίας περί της πιθανότητας διαρροής του συνθηματικού τους που ήταν σε ισχύ την επίμαχη ημερομηνία (13-14 Νοεμβρίου 2013), προτρέποντάς τους να το μεταβάλλουν και σε όποια άλλη διαδικτυακή υπηρεσία τυχόν το χρησιμοποιούν.

β) Να ληφθεί μέριμνα ώστε όλα τα συνθηματικά των χρηστών της διαδικτυακής του υπηρεσίας να αποθηκεύονται στη σχετική βάση δεδομένων σε μη αναγνώσιμη μορφή (για παράδειγμα, με χρήση ασφαλούς συνάρτησης κατακερματισμού - hash), κατά τρόπο τέτοιο ώστε ακόμα και αν προσπελαθούν από κάποιον τρίτο να είναι πρακτικά αδύνατον να τα ανακτήσει. Επίσης, θα πρέπει να υιοθετηθεί συγκεκριμένη πολιτική διαχείρισης των συνθηματικών ως προς το ελάχιστο μήκος αυτών αλλά και ως προς την υποχρεωτική χρήση μη αλφαριθμητικών χαρακτήρων, έτσι ώστε αυτά να καθίστανται μη προβλέψιμα.

γ) Να ληφθεί μέριμνα ώστε το γεγονός και οι λεπτομέρειες (ταυτότητα χρήστη, είδος πρόσβασης κτλ.) κάθε πρόσβασης χρηστών στη διαδικτυακή υπηρεσία να μπορούν να ελεγχθούν αποτελεσματικά εκ των υστέρων (μέσω της λειτουργίας κατάλληλων αρχείων καταγραφής - log files). Περαιτέρω, να πραγματοποιούνται ανά τακτά χρονικά διαστήματα έλεγχοι (π.χ. επίβλεψη των σχετικών αρχείων καταγραφής) για ανίχνευση τυχόν αθέμιτων ενεργειών.

δ) Να καταγραφεί συγκεκριμένη διαδικασία για την αντιμετώπιση περιστατικών παραβίασης προσωπικών δεδομένων, η οποία θα πρέπει να κοινοποιηθεί σε όλο το προσωπικό και να είναι δεσμευτική. Κατ' ελάχιστο η διαδικασία πρέπει να ορίζει τις περιπτώσεις που θεωρούνται περιστατικά παραβίασης προσωπικών δεδομένων και να περιγράφει τον τρόπο αναφοράς των περιστατικών, καθώς και τον τρόπο λήψης μέτρων για την αντιμετώπισή τους (συμπεριλαμβανομένων της σχετικής ενημέρωσης των υποκειμένων των δεδομένων). Μέρος της διαδικασίας θα πρέπει να αποτελεί και η καταχώρηση των περιστατικών σε ειδικό αρχείο (έντυπο ή ηλεκτρονικό), το οποίο θα πρέπει να περιέχει τα βασικά χαρακτηριστικά του περιστατικού, καθώς και τον τρόπο με τον οποίο αντιμετωπίστηκε.

ε) Να οριστεί διαδικασία για τη διαχείριση αλλαγών σε συστήματα επεξεργασίας προσωπικών δεδομένων. Ειδικότερα επισημαίνεται ότι, στις περιπτώσεις που πραγματοποιείται ανάπτυξη λογισμικού, αυτή θα πρέπει να γίνεται σε περιβάλλον δοκιμών, το οποίο πρέπει να είναι απομονωμένο από το παραγωγικό σύστημα.

στ) Να διασφαλίζεται ότι οι εκτελούντες την επεξεργασία εφαρμόζουν τα απαραίτητα μέτρα για την ασφάλεια της επεξεργασίας, στο μέτρο που αυτά τους αφορούν – όπως είναι,

για παράδειγμα, ο διαχωρισμός του περιβάλλοντος δοκιμών από το παραγωγικό περιβάλλον και η διαχείριση περιστατικών ασφαλείας.

Ο Πρόεδρος	**Η γραμματέας**
Πέτρος Χριστόφορος	**Ειρήνη Παπαγεωργοπούλου**