ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Αθήνα, 15-07-2026
Αριθ. Πρωτ.: 3164

ΑΠΟΦΑΣΗ 14/2026

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (εφεξής Αρχή), συνήλθε, μετά από πρόσκληση του ασκούντος καθήκοντα Προέδρου Αναπληρωτή Προέδρου της, Γεωργίου Μπατζαλέξη, σε συνεδρίαση μέσω τηλεδιάσκεψης στις 04-11-2025, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Στη συνεδρίαση παρέστησαν ο Αναπληρωτής Πρόεδρος της Αρχής, Γεώργιος Μπατζαλέξης, τα τακτικά μέλη Σπυρίδων Βλαχόπουλος, Κωνσταντίνος Λαμπρινουδάκης, Χαράλαμπος Ανθόπουλος, Χρήστος Καλλονιάτης, και Κατερίνα Ηλιάδου, καθώς και τα αναπληρωματικά μέλη Δημοσθένης Βουγιούκας, ως εισηγητής, και Μαρία Ψάλλα, αντικαθιστώντας το τακτικό μέλος Γρηγόρη Τσόλια, ο οποίος αν και εκλήθη νομίμως εγγράφως, δεν παρέστη λόγω κωλύματος. Παρόντες, με εντολή του Αν. Προέδρου, χωρίς δικαίωμα ψήφου, ήταν η Γεωργία Παναγοπούλου και ο Ιωάννης Λυκοτραφίτης, ειδικοί επιστήμονες-πληροφορικοί, ως βοηθοί εισηγητή και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών υποθέσεων της Αρχής, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα κατωτέρω:

Το Ελληνικό Ανοικτό Πανεπιστήμιο (εφεξής ΕΑΠ) υπέβαλε στην Αρχή, με βάση τον Κανονισμό (ΕΕ) 2016/679 (Γενικός Κανονισμός Προστασίας Δεδομένων – εφεξής ΓΚΠΔ), την υπ’ αρ. πρωτ. Γ/ΕΙΣ/8375/31-10-2024 αρχική γνωστοποίηση περιστατικού παραβίασης προσωπικών δεδομένων, την οποία, στη συνέχεια, συμπλήρωσε με την υπ’ αρ. πρωτ. Γ/ΕΙΣ/8569/07-11-2024 συμπληρωματική γνωστοποίηση.

Το περιστατικό συνίσταται, σύμφωνα με την γνωστοποίηση, σε παραβίαση της εμπιστευτικότητας και διαθεσιμότητας των προσωπικών δεδομένων του ΕΑΠ, ως συνέπεια κακόβουλης εξωτερικής ενέργειας ransomware στα πληροφοριακά του συστήματα. Η διαρροή αφορά σε περίπου 30.000 υποκείμενα, φοιτητές, απόφοιτους, καθηγητές, διοικητικό προσωπικό και προμηθευτές του ΕΑΠ, τα οποία το ΕΑΠ δηλώνει ότι λόγω της μεγάλης σοβαρότητας των πιθανών συνεπειών του περιστατικού ενημερώθηκαν σχετικά. Ειδικότερα, αναφέρεται ότι αυτό έγινε αφενός μέσω ανακοίνωσης στην κεντρική ιστοσελίδα (www.eap.gr) για την ακαδημαϊκή κοινότητα και ενδιαφερόμενα μέρη (φοιτητές, απόφοιτοι, καθηγητές, διοικητικό προσωπικό, προμηθευτές), και αφετέρου με ανακοινώσεις και ηλεκτρονικά μηνύματα για καθηγητές και διοικητικό προσωπικό. Στη συμπληρωματική γνωστοποίηση επισυνάπτονται αντίγραφα των σχετικών ενημερώσεων/ανακοινώσεων. Τέλος, το ΕΑΠ σημειώνει ότι καθώς πρόκειται για επίθεση μέσω ransomware, από την Ομάδα κυβερνοεκβιασμού RansomHub, είναι αναγκαία η διεξοδική έρευνα ώστε να διαπιστωθεί πλήρως η φύση της παραβίασης και ο βαθμός στον οποίο δεδομένα προσωπικού χαρακτήρα έχουν τεθεί σε κίνδυνο.

Η Αρχή, αφού εξέτασε την αρχική και τη συμπληρωματική γνωστοποίηση, απέστειλε το υπ' αρ. πρωτ. Γ/ΕΞΕ/3339/26-11-2024 έγγραφο στο ΕΑΠ, καλώντας τον να υποβάλει εντός εύλογου χρονικού διαστήματος νέα συμπληρωματική ή την πλήρη/τελική γνωστοποίηση στην οποία να διευκρινίζονται σημεία όπως: η φύση της παραβίασης και ο βαθμός στον οποίο δεδομένα προσωπικού χαρακτήρα έχουν τεθεί σε κίνδυνο, τα μέτρα ασφάλειας πριν και μετά το περιστατικό, καθώς και τα αποτελέσματα της διερεύνησής του, μαζί με τα ανάλογα τεκμήρια. Επίσης, η Αρχή με το ίδιο έγγραφο κάλεσε το ΕΑΠ να προσδιορίσει αν υπήρξε νεότερη παροχή συγκεκριμένων πληροφοριών προς τα επηρεαζόμενα υποκείμενα σχετικά με τις ενέργειες στις οποίες θα πρέπει να προβούν τα ίδια για να προστατευτούν.

Καθώς το ΕΑΠ δεν είχε υποβάλει κάποια νέα συμπληρωματική ή πλήρη/τελική γνωστοποίηση ή κάποια άλλη έγγραφη ενημέρωση, η Αρχή, με το υπ' αρ. πρωτ. Γ/ΕΞΕ/536/07-02-2025 έγγραφο, κάλεσε εκ νέου το ΕΑΠ να παράσχει τις ανωτέρω ζητηθείσες πληροφορίες, ή άλλη σχετική έγγραφη ενημέρωση για τους

λόγους καθυστέρησης ανταπόκρισης στο έγγραφό της.

Κατόπιν αυτού, το ΕΑΠ υπέβαλε την υπ' αρ. πρωτ. Γ/ΕΙΣ/1364/14-02-2025 δεύτερη συμπληρωματική γνωστοποίηση περιστατικού παραβίασης προσωπικών δεδομένων, ενημερώνοντας την Αρχή, μεταξύ άλλων, ότι η διερεύνηση του περιστατικού βρίσκεται σε εξέλιξη και ότι φέρεται να έχει διαρρεύσει αρχείο μεγέθους 813GB, το οποίο έχει αναρτηθεί σε πλατφόρμα του dark web, χωρίς να έχει καταστεί δυνατή η πλήρης πρόσβαση στο περιεχόμενό του. Για το λόγο αυτό, σημειώνει το ΕΑΠ, δεν έχει ακόμα προβεί σε ειδική ενημέρωση των υποκειμένων, διότι επιθυμεί πρώτα να προσδιορίσει τα υποκείμενα των οποίων τα προσωπικά δεδομένα περιέχονται στο αρχείο αυτό.

Η Αρχή, στη συνέχεια, με το υπ' αρ. πρωτ. Γ/ΕΞΕ/766/06-03-2025 έγγραφο, έδωσε εντολή στο ΕΑΠ να προβεί αμελλητί στην ανακοίνωση της παραβίασης δεδομένων προσωπικού χαρακτήρα σε όλα τα πιθανά υποκείμενα των δεδομένων, σύμφωνα με το άρθρο 34 παρ. 4 του ΓΚΠΔ. Στο έγγραφο αυτό, η Αρχή σημειώνει, μεταξύ άλλων, ότι ακόμα και αν δεν είναι σε θέση το ΕΑΠ να προσδιορίσει με ακρίβεια ποια υποκείμενα έχουν επηρεαστεί από την παραβίαση, λόγω του όγκου του αρχείου που είναι διαθέσιμο στο διαδίκτυο για κάθε ενδιαφερόμενο, είναι ασφαλέστερο για τα δικαιώματα και τις ελευθερίες των υποκειμένων να θεωρηθεί ότι έχουν επηρεαστεί τα δεδομένα όλων των υποκειμένων που τηρούνταν στα αρχεία του ΕΑΠ. Η δημόσια ανακοίνωση, στην εξεταζόμενη περίπτωση αυτή, δεν θεωρείται ενδεδειγμένος τρόπος με τον οποίο τα υποκείμενα ενημερώνονται αποτελεσματικά. Η μη ενημέρωση, έστω κι ενός υποκειμένου του οποίου τα δεδομένα (μεταξύ αυτών ενδεχομένως στοιχεία ταυτότητας, στοιχεία πληρωμών μέσω τραπεζικής κάρτας) ενδέχεται να έχουν διαρρεύσει, σε συνδυασμό με τις κατά πάσα πιθανότητα κακόβουλες προθέσεις των υπευθύνων για τη παραβίαση, μπορεί να έχει αντίκτυπο σε αυτό ή ακόμα και σοβαρή ζημιά. Επίσης, η ανακοίνωση της παραβίασης απευθείας στα υποκείμενα επιτρέπει να παρασχεθεί ειδική ενημέρωση, προσαρμοσμένη στα τηρούμενα προσωπικά δεδομένα ανά κατηγορία υποκειμένων, σχετικά με τους κινδύνους που εγκυμονεί η παραβίαση και τις

ενέργειες στις οποίες μπορούν να προβούν αυτά τα υποκείμενα προκειμένου να προστατευθούν από τις πιθανές αρνητικές συνέπειες της παραβίασης.

Το ΕΑΠ απάντησε στην ανωτέρω εντολή που εξέδωσε η Αρχή με το υπ' αρ. πρωτ. Γ/ΕΙΣ/6684/16-07-2025 έγγραφο, στο οποίο επισυνάπτεται η από 28-03-2025 δημόσια αναλυτική ανακοίνωση ενημέρωσης των υποκειμένων[1], σε εφαρμογή της σχετικής εντολής της Αρχής, για τις συνθήκες και τα πραγματικά περιστατικά της παραβίασης, τα μέτρα προστασίας και οι οδηγίες για τις αναγκαίες προληπτικές ενέργειες από πλευράς κάθε υποκειμένου, καθώς και η τελική αναφορά από τη διερεύνηση του περιστατικού. Αναφέρονται στα ανωτέρω, μεταξύ άλλων, τα ακόλουθα:

Όσον αφορά τον τρόπο επίθεσης, αυτός περιγράφεται στο Εμπιστευτικό Παράρτημα Β, Σημείο 1. Στο ανωτέρω έγγραφο του ΕΑΠ αναφέρεται, επίσης, ότι: *«Πριν το περιστατικό το ΕΑΠ είχε προσχωρήσει σε προμήθεια μέσω διαγωνιστικών διαδικασιών εξειδικευμένων λογισμικών ασφάλειας πληροφοριών, τα οποία κατά την περίοδο εγκατάστασης και εφαρμογής τους, αναγνωρίζονταν ως κορυφαία εργαλεία στον τομέα για τον οποίο προμηθεύτηκαν. Το ΕΑΠ είχε προχωρήσει σε συνεχή ενημέρωση των χρηστών για την ορθή χρήση των πληροφοριακών συστημάτων και των κινδύνων του διαδικτύου. Αν και το ΕΑΠ αντιμετωπίζει επιτυχώς και συχνά επιθέσεις διαφόρων ειδών και σε διαφορετικά επίπεδα των υπηρεσιών του, στην παρούσα επίθεση δεν ήταν εφικτή η πλήρης αποτροπή όλου του εύρους της και των συνεπειών της, καθώς χρησιμοποιήθηκαν τεχνικές επίθεσης που έχουν σαν στόχο την παραπλάνηση των τελικών χρηστών, με σκοπό την μη εξουσιοδοτημένη πρόσβαση σε εσωτερικά συστήματα.»*

Επίσης, αναφορικά με τη διαχείριση του περιστατικού και την ενημέρωση των υποκειμένων σχετικά με το περιστατικό, υπεβλήθησαν στην Αρχή σχετικές αναφορές/καταγγελίες, οι οποίες διαβιβάστηκαν στο ΕΑΠ με αντίστοιχα

[1] https://www.eap.gr/2025/03/28/enimerosi-skhetika-me-entopismeno-peristatiko-kakovoulis-epithesis/

διαβιβαστικά έγγραφα. Τα σχετικά έγγραφα αναφέρονται στο Παράρτημα Α της παρούσης.

Σχετικά, με τον τρόπο που χειρίστηκε και ανταποκρίθηκε το ΕΑΠ στα αιτήματα και ερωτήματα που υποβλήθηκαν σε αυτό από υποκείμενα και νομικούς πληρεξούσιους αυτών, αναφέρει τα εξής: «*Δίνονται προσωπικά σε κάθε υποκείμενο – αποστολέα, απαντήσεις σύμφωνα με τα όσα καθορίστηκαν στην από 6-3-2025 εντολή της Αρχής. Κρίθηκε δε, με την επιφύλαξη αντίθετης νεότερης διευκρίνησης – σύστασης από πλευράς της Αρχής, ότι με δεδομένη την υποχρέωση επίσκεψης όλων των φοιτητών/ριων, διδακτικού προσωπικού κλπ στην ιστοσελίδα του ΕΑΠ για σειρά θεμάτων, η ανάρτηση της συνημμένης αναλυτικής ανακοίνωσης ανταποκρίνεται στο γράμμα και στο πνεύμα του νόμου και της απόφασης της Αρχής, ενώ η απόπειρα έγγραφης κατ' ιδίαν και ατομικής ενημέρωσης του συνόλου των υποκειμένων, τα οποία υπερβαίνουν τις 36.000 πέραν του ότι δημιουργεί αυτονόητο κίνδυνο αδικαιολόγητης αναστάτωσης, αποτελεί, κατά την κρίση μας, και μη επιβεβλημένη μέθοδο η οποία θα απαιτούσε δυσανάλογη προσπάθεια κατ' άρθρο 33 ν. 4624/2019 τόσο από τον διαχειριστή όσο και από πλευράς της Αρχής.»*

Στη συνέχεια, η Αρχή κάλεσε το ΕΑΠ με την υπ' αρ. πρωτ. Γ/ΕΞΕ/3027/01-09-2025 κλήση σε ακρόαση, μέσω τηλεδιάσκεψης. Στην εν λόγω τηλεδιάσκεψη συνδέθηκαν οι Α, Πρύτανης του ΕΑΠ, Β, Αντιπρύτανης Οικονομικών και Υποδομών, Γ, Αντιπρύτανης Έρευνας και Καινοτομίας και οι πληρεξούσιοι δικηγόροι του ΕΑΠ Δημήτριος Κουρκουμέλης, με ΑΜ ΔΣ…, Δ, DPO του ΕΑΠ, Ε, Συνεργάτης του γραφείου Δικτυακών & Πληροφοριακών Υπηρεσιών, και ΣΤ, Συνεργάτης του γραφείου Δικτυακών & Πληροφοριακών Υπηρεσιών του ΕΑΠ.

Ακολούθως, το ΕΑΠ υπέβαλε εμπροθέσμως το υπ' αρ. πρωτ. Γ/ΕΙΣ/9334/26-09-2025 υπόμνημα μετά των σχετικών αυτού εγγράφων. Το ανωτέρω υπόμνημα συμπληρώθηκε με το υπ' αρ. πρωτ. Γ/ΕΙΣ/9674/02-10-2025 έγγραφο, το οποίο περιείχε τις επιστολές που απέστειλε το ΕΑΠ στα πρόσωπα τα οποία προσέφυγαν στην Αρχή (βλ. Παράρτημα Α), καθώς και με το υπ' αρ. πρωτ. Γ/ΕΙΣ/9675/02-10-2025 έγγραφο, που περιείχε αντίγραφο του ηλεκτρονικού μηνύματος που εστάλη στα υποκείμενα που διαθέτουν λογαριασμό ηλεκτρονικού ταχυδρομείου στο ΕΑΠ. Σημειώνεται ότι, ενώ είχε γίνει αναφορά στο με το υπ' αρ. πρωτ. Γ/ΕΙΣ/6684/16-07-

2025 έγγραφο σχετικά με την ειδική ενημέρωση των υποκειμένων μέσω προσωπικών μηνυμάτων ηλεκτρονικού ταχυδρομείου, το περιεχόμενο του εν λόγω ενημερωτικού email υποβλήθηκε στην Αρχή με το συμπληρωματικό με αρ. πρωτ. Γ/ΕΙΣ/9675/02-10-2025 έγγραφο του ΕΑΠ.

Ειδικότερα, στο ανωτέρω υπόμνημά του, το ΕΑΠ αναφέρει συνοπτικά, μεταξύ άλλων, τα ακόλουθα:

Αναφορικά με την ενημέρωση των υποκειμένων, αναφέρεται ότι «*… το ΕΑΠ συμμορφούμενο πλήρως με την εντολή της Αρχής, προχώρησε αφενός μεν σε αναλυτική ανακοίνωση στην ιστοσελίδα του στις 28.3.2025 με εκτενή περιγραφή του περιστατικού, των παραμέτρων προσβολής, των κινδύνων και των συγκεκριμένων ατομικών μέτρων προστασίας που ενδείκνυνται και οφείλει κάθε υποκείμενο να λάβει και, αφετέρου, στην μαζική αποστολή μέσω ηλεκτρονικού ταχυδρομείου, μηνύματος γνωστοποίησης του περιστατικού, η οποία αποστολή πραγματοποιήθηκε την πρώτη εβδομάδα του Απριλίου 2025 μέχρι και τις 13.4.2025, με περαιτέρω οδηγίες προστασίας, στο σύνολο των υποκειμένων που διατηρούσε έως τότε ιδρυματικό λογαριασμό με διεύθυνση ηλεκτρονικού ταχυδρομείου, δηλαδή στους φοιτητές, στους αποφοίτους, στους διδάσκοντες, στα μέλη ΔΕΠ και στο διοικητικό προσωπικό του πανεπιστημίου, οι οποίοι υπολογίζονται περίπου σε 108.000*».

Σχετικά με τις αιτίες του περιστατικού, επαναλαμβάνονται τα αναφερόμενα στο Εμπιστευτικό Παράρτημα Β, Σημείο 1. Τα βασικά στοιχεία των σχετικών με το περιστατικό μέτρων ασφάλειας που είχαν ληφθεί πριν το περιστατικό, περιγράφονται στο Εμπιστευτικό Παράρτημα Β, Σημείο 2.

Τα βασικά στοιχεία των μέτρων ασφάλειας που ελήφθησαν μετά το περιστατικό περιγράφονται στο Εμπιστευτικό Παράρτημα Β, Σημείο 3.

Η Αρχή, μετά από εξέταση των στοιχείων του φακέλου, αφού άκουσε τον εισηγητή και τις διευκρινίσεις από τους βοηθούς εισηγητή, οι οποίοι παρέστησαν χωρίς δικαίωμα ψήφου, κατόπιν διεξοδικής συζητήσεως,

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Από τις διατάξεις των άρθρων 51 και 55 του ΓΚΠΔ και του άρθρου 9 του νόμου 4624/2019 (ΦΕΚ Α΄ 137) προκύπτει ότι η Αρχή έχει αρμοδιότητα να εποπτεύει την εφαρμογή των διατάξεων του ΓΚΠΔ, του νόμου αυτού και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων.
2. Σύμφωνα με το σημείο 12 του άρθρου 4 του ΓΚΠΔ, ως *«παραβίαση δεδομένων προσωπικού χαρακτήρα νοείται η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία».*
3. Σύμφωνα με το άρθρο 4 στοιχ. 1 του ΓΚΠΔ δεδομένα προσωπικού χαρακτήρα είναι «*κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου*».
4. Στο άρθρο 5 παρ. 1 του ΓΚΠΔ ορίζονται οι αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Σε αυτές περιλαμβάνεται η αρχή της ακεραιότητας και εμπιστευτικότητας (εδαφ. στ'), σύμφωνα με την οποία τα δεδομένα υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων.
5. Σύμφωνα δε με την αρχή της λογοδοσίας που εισάγεται με τη δεύτερη παράγραφο του αυτού ως άνω άρθρου 5, ορίζεται ρητώς ότι ο υπεύθυνος επεξεργασίας «φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 («λογοδοσία»)». Η αρχή αυτή, η οποία συνιστά ακρογωνιαίο λίθο του ΓΚΠΔ, συνεπάγεται την υποχρέωση του υπευθύνου επεξεργασίας να

σχεδιάζει, εφαρμόζει και εν γένει λαμβάνει τα αναγκαία μέτρα και πολιτικές, προκειμένου η επεξεργασία των δεδομένων να είναι σύμφωνη με τις σχετικές νομοθετικές προβλέψεις και, επιπλέον, να είναι σε θέση να αποδεικνύει ο ίδιος και ανά πάσα στιγμή τη συμμόρφωσή του με τις αρχές του άρθρου 5 παρ. 1 ΓΚΠΔ.

6. Σύμφωνα με τους ορισμούς του άρθρου 25 του ΓΚΠΔ: «*1. Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία, ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.»*

7. Στο άρθρο 32 παρ. 1 και 2 του ΓΚΠΔ ορίζεται ότι: «*1. Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων (…) 2. Κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας λαμβάνονται ιδίως υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία*».

8. Σύμφωνα το άρθρο 33 του ΓΚΠΔ: «*1. Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και,*

αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή που είναι αρμόδια σύμφωνα με το άρθρο 55, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση. (...) 3. Η γνωστοποίηση που αναφέρεται στην παράγραφο 1 κατ' ελάχιστο: α) περιγράφει τη φύση της παραβίασης δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων, όπου είναι δυνατό, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων των δεδομένων, καθώς και των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων δεδομένων προσωπικού χαρακτήρα, β)ανακοινώνει το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες, γ) περιγράφει τις ενδεχόμενες συνέπειες της παραβίασης των δεδομένων προσωπικού χαρακτήρα, δ) περιγράφει τα ληφθέντα ή τα προτεινόμενα προς λήψη μέτρα από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της. 4. Σε περίπτωση που και εφόσον δεν είναι δυνατόν να παρασχεθούν οι πληροφορίες ταυτόχρονα, μπορούν να παρέχονται σταδιακά χωρίς αδικαιολόγητη καθυστέρηση. 5. Ο υπεύθυνος επεξεργασίας τεκμηριώνει κάθε παραβίαση δεδομένων προσωπικού χαρακτήρα, που συνίστανται στα πραγματικά περιστατικά που αφορούν την παραβίαση δεδομένων προσωπικού χαρακτήρα, τις συνέπειες και τα ληφθέντα διορθωτικά μέτρα. Η εν λόγω τεκμηρίωση επιτρέπει στην εποπτική αρχή να επαληθεύει τη συμμόρφωση προς το παρόν άρθρο. »

9. Σύμφωνα με το άρθρο 34 του ΓΚΠΔ: «*1. Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο*

των δεδομένων. 2. Στην ανακοίνωση στο υποκείμενο των δεδομένων η οποία αναφέρεται στην παράγραφο 1 του παρόντος άρθρου περιγράφεται με σαφήνεια η φύση της παραβίασης των δεδομένων προσωπικού χαρακτήρα και περιέχονται τουλάχιστον οι πληροφορίες και τα μέτρα που αναφέρονται στο άρθρο 33 παράγραφος 3 στοιχεία β), γ) και δ). 3. Η ανακοίνωση στο υποκείμενο των δεδομένων η οποία αναφέρεται στην παράγραφο 1 δεν απαιτείται, εάν πληρείται οποιαδήποτε από τις ακόλουθες προϋποθέσεις: α) ο υπεύθυνος επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, και τα μέτρα αυτά εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση δεδομένα προσωπικού χαρακτήρα, κυρίως μέτρα που καθιστούν μη κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, όπως η κρυπτογράφηση, β) ο υπεύθυνος επεξεργασίας έλαβε στη συνέχεια μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει ο αναφερόμενος στην παράγραφο 1 υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, γ) προϋποθέτει δυσανάλογες προσπάθειες. Στην περίπτωση αυτή, γίνεται αντ' αυτής δημόσια ανακοίνωση ή υπάρχει παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο. 4. Εάν ο υπεύθυνος επεξεργασίας δεν έχει ήδη ανακοινώσει την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, η εποπτική αρχή μπορεί, έχοντας εξετάσει την πιθανότητα επέλευσης υψηλού κινδύνου από την παραβίαση των δεδομένων προσωπικού χαρακτήρα, να του ζητήσει να το πράξει ή μπορεί να αποφασίσει ότι πληρούνται οποιαδήποτε από τις προϋποθέσεις που αναφέρονται στην παράγραφο 3.»

10. Η υποχρέωση ασφάλειας που προβλέπεται στο άρθρο 32 του ΓΚΠΔ συνιστά υποχρέωση «μέσων» και όχι «αποτελέσματος» και επιβάλλει στον υπεύθυνο επεξεργασίας την υποχρέωση λήψης κατάλληλων τεχνικών και οργανωτικών μέτρων, τα οποία, λαμβανομένων υπόψη των χαρακτηριστικών της συγκεκριμένης επεξεργασίας, αποσκοπούν τόσο στη μείωση της πιθανότητας επέλευσης παραβίασης δεδομένων προσωπικού χαρακτήρα όσο και, στον περιορισμό της σοβαρότητάς της, όταν ένας κίνδυνος υλοποιηθεί. Ως εκ τούτου,

δεν απαιτείται τα μέτρα ασφάλειας να εξαλείφουν κάθε μορφή κινδύνου και η απλή επέλευση παραβίασης δεδομένων προσωπικού χαρακτήρα δεν συνιστά, αυτή καθαυτή, παράβαση του άρθρου 32 του ΓΚΠΔ. Η ανωτέρω ερμηνεία έχει επιβεβαιωθεί από το Δικαστήριο της Ευρωπαϊκής Ένωσης με την απόφασή του στην υπόθεση C-340/21[2] (βλ. σκέψεις 29-31), με την οποία κρίθηκε ότι η αναφορά, στο άρθρο 32 παρ. 1 και 2 ΓΚΠΔ, σε «επίπεδο ασφάλειας κατάλληλο προς τον κίνδυνο» και σε «κατάλληλο επίπεδο ασφάλειας» καταδεικνύει ότι ο ΓΚΠΔ θεσπίζει καθεστώς διαχείρισης κινδύνων και δεν αποσκοπεί στην εξάλειψη των κινδύνων παραβίασης δεδομένων προσωπικού χαρακτήρα. Από τη διατύπωση των άρθρων 24 και 32 ΓΚΠΔ προκύπτει ότι οι διατάξεις αυτές επιβάλλουν στον υπεύθυνο επεξεργασίας την υποχρέωση υιοθέτησης τεχνικών και οργανωτικών μέτρων με σκοπό την αποτροπή, στο μέτρο του δυνατού, παραβιάσεων δεδομένων προσωπικού χαρακτήρα. Η καταλληλότητα των μέτρων αυτών πρέπει να αξιολογείται κατά περίπτωση, λαμβανομένων υπόψη των κριτηρίων που προβλέπονται στα ανωτέρω άρθρα, καθώς και των ειδικών αναγκών προστασίας των δεδομένων και των κινδύνων που απορρέουν από τη συγκεκριμένη επεξεργασία. Συνεπώς, τα άρθρα 24 και 32 ΓΚΠΔ δεν μπορούν να ερμηνευθούν υπό την έννοια ότι η μη εξουσιοδοτημένη γνωστοποίηση ή πρόσβαση τρίτου σε δεδομένα προσωπικού χαρακτήρα αρκεί αφ' εαυτής για να συναχθεί ότι τα ληφθέντα μέτρα ασφάλειας δεν ήταν κατάλληλα, χωρίς να παρέχεται στον υπεύθυνο επεξεργασίας η δυνατότητα ανταπόδειξης. Περαιτέρω, το Δικαστήριο υπενθύμισε ότι η ερμηνεία αυτή επιβεβαιώνεται από τη συνδυασμένη ανάγνωση των άρθρων 24 και 32 ΓΚΠΔ με το άρθρο 5 παρ. 2 και το άρθρο 82 του ίδιου κανονισμού, υπό το φως των αιτιολογικών σκέψεων 74, 76 και 83 αυτού, από τα οποία προκύπτει ιδίως ότι ο υπεύθυνος επεξεργασίας υποχρεούται να μετριάζει τους κινδύνους παραβίασης δεδομένων προσωπικού χαρακτήρα και όχι να αποτρέπει κάθε παραβίαση (25.1.2024, C-687/21, σκέψη 39). Κατά συνέπεια, παράβαση της υποχρέωσης ασφάλειας του άρθρου 32 ΓΚΠΔ

[2] (Case C-340/21, Natsionalna agentsia za prihodite) - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CA0340

δύναται να διαπιστωθεί ανεξαρτήτως της ύπαρξης παραβίασης δεδομένων προσωπικού χαρακτήρα.

11. Επομένως, η Αρχή δύναται να επιβάλει κύρωση όχι για την επέλευση παραβίασης δεδομένων προσωπικού χαρακτήρα αυτή καθαυτή, αλλά για το γεγονός ότι η εν λόγω παραβίαση κατέστη δυνατή ή διευκολύνθηκε λόγω απουσίας ή ανεπάρκειας των εφαρμοσθέντων μέτρων ασφάλειας από τον υπεύθυνο επεξεργασίας, λαμβανομένης υπόψη των σύγχρονων τεχνολογικών δυνατοτήτων και των πρακτικών ασφάλειας που θεωρούνται σήμερα βέλτιστες (state-of the art).

12. Ως προς την εκτίμηση της υποχρέωσης μέσων που βαρύνει τον υπεύθυνο επεξεργασίας, το Δικαστήριο έχει κρίνει ότι η καταλληλότητα των τεχνικών και οργανωτικών μέτρων πρέπει να αξιολογείται σε δύο στάδια: αφενός, με τον εντοπισμό των κινδύνων παραβίασης δεδομένων προσωπικού χαρακτήρα που συνεπάγεται η συγκεκριμένη επεξεργασία και των ενδεχόμενων συνεπειών τους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, λαμβανομένων υπόψη της πιθανότητας και της σοβαρότητάς τους, και αφετέρου, με την εξέταση του κατά πόσον τα μέτρα που έλαβε ο υπεύθυνος επεξεργασίας είναι προσαρμοσμένα στους κινδύνους αυτούς, λαμβανομένων υπόψη της κατάστασης των γνώσεων, του κόστους εφαρμογής, καθώς και της φύσης, της έκτασης, του πλαισίου και των σκοπών της επεξεργασίας (14.12.2023, C-340/21, σκέψη 42).

13. Κατά συνέπεια, η Αρχή δεν εξετάζει την παραβίαση δεδομένων προσωπικού χαρακτήρα αυτή καθαυτή, αλλά κρίνει εάν, λαμβανομένων υπόψη της κατάστασης των γνώσεων, των χαρακτηριστικών της επεξεργασίας, της πιθανότητας και της σοβαρότητας των κινδύνων, καθώς και της έκτασης της υποχρέωσης ασφάλειας, το ΕΑΠ συμμορφώνεται με τις υποχρεώσεις που υπέχει από το άρθρο 32 του ΓΚΠΔ, έχοντας θέσει σε εφαρμογή κατάλληλα τεχνικά και οργανωτικά μέτρα.

14. Στην προκειμένη περίπτωση, από τα στοιχεία του φακέλου της υπόθεσης προκύπτει ότι ο υπεύθυνος επεξεργασίας συμμορφώθηκε με τις υποχρεώσεις των υπευθύνων επεξεργασίας οι οποίες απορρέουν από τα προαναφερθέντα

άρθρα 33 και 34 του ΓΚΠΔ αναφορικά με τη διαχείριση περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα, δεδομένου ότι:

α) υπέβαλε τη σχετική γνωστοποίηση στην Αρχή, εντός εβδομήντα δύο (72) ωρών από τη στιγμή που έλαβε γνώση του περιστατικού,

β) η γνωστοποίηση συνολικά, όπως αυτή συμπληρώθηκε, παρέχει όλες τις πληροφορίες που απαιτούνται βάσει του άρ. 33 του ΓΚΠΔ,

γ) προέβη σε αξιολόγηση των κινδύνων για τα επηρεαζόμενα υποκείμενα των δεδομένων λόγω του περιστατικού και πραγματοποίησε ενημέρωση αυτών, σύμφωνα με τα όσα προβλέπονται σχετικώς στο άρ. 34 του ΓΚΠΔ, κατόπιν της σχετικής εντολής της Αρχής (αρ. πρωτ. Γ/ΕΞΕ/766/06-03-2025). Επισημαίνεται ότι τα περιστατικά που οδήγησαν στην εντολή της Αρχής δεν εξετάζονται εκ νέου, καθώς αποτέλεσαν ήδη αντικείμενο της εν λόγω πράξης της Αρχής. Συνεπώς, με την παρούσα δεν εξετάζεται τυχόν παράβαση του άρθρου 34, ενώ μετά την υλοποίηση της εν λόγω εντολής, δεν παρίσταται πλέον ανάγκη εξέτασης της εν λόγω διάταξης.

δ) Σχετικά με τα αίτια του περιστατικού, και την συμμόρφωση με το άρ. 32 του ΓΚΠΔ: Η διανομή του κακόβουλου λογισμικού έγινε δυνατή εξαιτίας ενός ανθρώπινου λάθους, το οποίο θα μπορούσε να αποφευχθεί μέσω ακόμη πιο στοχευμένης εκπαίδευσης αλλά και βελτίωσης των μέτρων αυθεντικοποίησης για τους χρήστες με δικαιώματα διαχείρισης των συστημάτων. Το γεγονός ότι το κακόβουλο λογισμικό είχε τη δυνατότητα να σκανάρει το δίκτυο και να εκμεταλλευτεί κενά ασφαλείας, υποδηλώνει ότι παρά την εφαρμογή ισχυρών πρακτικών ασφάλειας, η διαμόρφωση του εσωτερικού δικτύου δεν λειτούργησε αποτελεσματικά, ώστε να αποτρέψει τον συγκεκριμένο τρόπο παρείσφρησης και διάδοσης. Ειδικά, ως προς την ανεπαρκή απομόνωση του εσωτερικού δικτύου προ του περιστατικού, αυτό τεκμαίρεται και από το γεγονός ότι ένα από τα μέτρα ασφάλειας που το ΕΑΠ αποφάσισε να λάβει μετά το περιστατικό περιλαμβάνουν και η επαναξιολόγηση και ανασχεδιασμό της αρχιτεκτονικής του εσωτερικού του δικτύου, όπως περιγράφεται στο Σημείο 3 του Παραρτήματος Β.

15. Ο χειρισμός του περιστατικού κρίνεται ως επαρκής, λαμβάνοντας υπόψη τις ενέργειες στις οποίες προέβη το ΕΑΠ, τόσο για την ανάκτηση των κρυπτογραφημένων δεδομένων, έστω κι αν αυτή δεν ήταν επιτυχής, για την

αποκατάσταση της λειτουργίας των συστημάτων του και για τη λήψη κατάλληλων μέτρων για να αποτραπεί αντίστοιχη επιτυχής εγκατάσταση κακόβουλου λογισμικού στο μέλλον. Δηλαδή, το ΕΑΠ, μετά το συμβάν προχώρησε σε όλες τις δυνατές διορθωτικές ενέργειες ως προς τα μέτρα ασφαλείας, για την αποτροπή μελλοντικού περιστατικού ασφαλείας, αλλά και τις ενέργειες προς το μετριασμό της τυχόν ζημιάς στα επηρεαζόμενα υποκείμενα (όπως ενημέρωση τόσο μέσω της ιστοσελίδας του όσο και απευθείας με ηλεκτρονικό ταχυδρομείο).

16. Επίσης απάντησε πλήρως σε κάθε μία από τις αναφερόμενες στο Παράρτημα Α αναφορές/καταγγελίες.

17. Η Αρχή, λαμβάνοντας υπόψη τα παραπάνω, και συνυπολογίζοντας αφενός μεν τον μεγάλο αριθμό των επηρεαζόμενων υποκειμένων, αφετέρου ότι ο υπεύθυνος επεξεργασίας προέβη σε επαρκείς ενέργειες για την αντιμετώπιση του περιστατικού και για αποτροπή παρόμοιου μελλοντικού περιστατικού, συνεκτιμώντας και το κόστος λήψης των μέτρων αυτών, κρίνει ότι η αρμόζουσα διορθωτική εξουσία είναι η εντολή κατ’ άρθρο 58 παρ. 2 β΄ του ΓΚΠΔ.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή, με βάση το άρθρο 58 παρ. 2 εδ. δ’ του ΓΚΠΔ, δίνει εντολή στο Ελληνικό Ανοικτό Πανεπιστήμιο να προβεί σε στοχευμένες δράσεις εκπαίδευσης των διαχειριστών, καθώς και στην πλήρη υλοποίηση του συνόλου των μέτρων που αναφέρονται στην Σκέψη 14, παρ. δ), τα οποία έχει ήδη προγραμματίσει, εντός αποκλειστικής προθεσμίας έξι (6) μηνών από τη λήψη της παρούσας και να ενημερώσει σχετικά την Αρχή προσκομίζοντας την κατάλληλη τεκμηρίωση.

Ο εκτελών χρέη Προέδρου

Αναπληρωτής Πρόεδρος

Η Γραμματέας

Γεώργιος Μπατζαλέξης

Ειρήνη Παπαγεωργοπούλου