ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Αποστολή: Ηλεκτρονικό ταχυδρομείο

Αθήνα, 28-02-2024

Αριθ. Πρωτ.: 667

Απόφαση 10/2024

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνήλθε μετά από πρόσκληση του Προέδρου της σε συνεδρίαση δια ζώσης την 26.09.2023 και ώρα 10:00, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Κωνσταντίνος Μενουδάκος, Πρόεδρος της Αρχής, Χρήστος Καλλονιάτης ως εισηγητής, Σπυρίδων Βλαχόπουλος, Κωνσταντίνος Λαμπρινουδάκης, Αικατερίνη Ηλιάδου, και Γρηγόριος Τσόλιας ως τακτικά μέλη και Νικόλαος Λίβος αναπληρωματικό μέλος του Χαράλαμπου Ανθόπουλου, ο οποίος παρόλο που εκλήθη νομίμως εγγράφως δεν παρέστη, λόγω κωλύματος. Στη συνεδρίαση παρέστησαν, με εντολή του Προέδρου χωρίς δικαίωμα ψήφου, οι Παναγιώτης Τσόπελας, Λεωνίδας Ρούσος, ειδικοί επιστήμονες – ελεγκτές ως βοηθοί εισηγητή και η Ειρήνη Παπαγεωργοπούλου υπάλληλος του Τμήματος Διοικητικών Υποθέσεων της Αρχής.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Η εταιρία «ΕΛΛΗΝΙΚΑ ΤΑΧΥΔΡΟΜΕΙΑ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ», (εφεξής ΕΛΤΑ) υπέβαλε στην Αρχή, με βάση τον Κανονισμό (ΕΕ) 2016/679 (Γενικός Κανονισμός Προστασίας Δεδομένων – εφεξής ΓΚΠΔ), τις με αρ. πρωτ. Γ/ΕΙΣ/5033/23-03-2022 και με αρ. πρωτ. Γ/ΕΙΣ/9170/27-07-2022 γνωστοποιήσεις περιστατικών παραβίασης που αφορούν κρυπτογράφηση λογισμικού στο σύστημα της εταιρίας, ως αποτέλεσμα κακόβουλης επίθεσης από τρίτους, και διαρροή προσωπικών δεδομένων τα οποία, σε επόμενη φάση, δημοσιεύτηκαν στο σκοτεινό ιστό (Dark Web). Από την περαιτέρω ανάλυση της κυβερνοεπίθεσης προκύπτει ότι έλαβαν χώρα, στο πλαίσιο της παραβίασης του συστήματος του υπευθύνου επεξεργασίας, ενέργειες μη εξουσιοδοτημένης απομακρυσμένης πρόσβασης σε σταθμούς εργασίας και σε αρχεία, εύρεση εκ μέρους του επιτιθέμενου των

κωδικών πρόσβασης των λογαριασμών διαχείρισης του τομέα του δικτύου, μη εξουσιοδοτημένη πρόσβαση σε αρχεία και φακέλους και εγκατάσταση κακόβουλων διεργασιών.

Η Αρχή, αφού εξέτασε την αρχική γνωστοποίηση, απέστειλε το έγγραφο με το υπ' αρ. πρωτ. Γ/ΕΞΕ/1208/19-05-2022 στα ΕΛΤΑ, ζητώντας την περιγραφή των ενεργειών που έχουν λάβει χώρα στο πλαίσιο διερεύνησης/αντιμετώπισης του εν λόγω περιστατικού και κάθε σχετική πληροφορία και αναφορά (π.χ. αναφορές προς/από άλλες αρμόδιες αρχές ή τρίτες εταιρείες), καθώς και τις ενέργειες στις οποίες τα ΕΛΤΑ έχουν προβεί σε σχέση με την ενημέρωση των επηρεαζόμενων υποκειμένων των δεδομένων και τυχόν τρίτων μερών.

Τα ΕΛΤΑ απάντησαν με τα υπ' αρ πρωτ. Γ/ΕΙΣ/7610/01-06-2022 και Γ/ΕΙΣ/7660/02-06-2022 ηλεκτρονικά μηνύματα, στα οποία περιλαμβάνονταν τεχνική έκθεση περιστατικού Κυβερνοασφάλειας, τα κεντρικά σημεία της οποίας περιγράφονται αναλυτικά στο παράρτημα Α της απόφασης και αναφέρονταν τα ακόλουθα:

1. Πραγματοποιήθηκαν ανακοινώσεις του υπευθύνου επεξεργασίας προς το κοινό για ενημέρωση σχετικά με την παραβίαση (21.03.2022 και 23.03.2022), καθώς και για τις ενέργειες μετά την παραβίαση (24.03.2022 και 07.04.2022).
2. Υπήρξε εσωτερική ανακοίνωση υπευθύνου επεξεργασίας στην οποία προσδιορίζονταν οι ενέργειες επαναφοράς του συστήματος.
3. Έγινε ενημέρωση διεθνών φορέων International Post Corporation, PostEurop, και Universal Postal Union που επηρεάζονται από το περιστατικό (22.03.2022 και 23.03.2022).
4. Έγινε ενημέρωση της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (24.03.2022), της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (22.03.2022) και της Εθνικής Αρχής Κυβερνοασφάλειας (30.3.2022) .
5. Έγινε ενημέρωση της Εταιρίας Δικτύου Ύδρευσης και Αποχέτευσης Πρωτευούσης. Για το περιστατικό έχει υποβάλλει και η εν λόγω εταιρία αρχική αναφορά γνωστοποίησης με αρ. πρωτ. Γ/ΕΙΣ/5224/25-03-2022 και οριστική με αρ. πρωτ. Γ/ΕΙΣ/8266/24-06-2022.
6. Υποβλήθηκε συμπληρωματική γνωστοποίηση παραβίασης, με τα νέα δεδομένα που προέκυψαν κατά τη διερεύνηση του περιστατικού.

Στη συνέχεια, η Αρχή, αφού εξέτασε την ανωτέρω απάντηση, ζήτησε με το υπ' αρ. Γ/ΕΞΕ/1499/21-06-2022 έγγραφο τις πολιτικές και διαδικασίες πληροφορικής και ασφάλειας πληροφοριών του φορέα αλλά και τον τρόπο εφαρμογής των εν λόγω πολιτικών και διαδικασιών στο πλαίσιο της αντιμετώπισης του εν λόγω περιστατικού παραβίασης. Τα ΕΛΤΑ, απάντησαν με το υπ' αρ. πρωτ. Γ/ΕΙΣ/8566/06-07-2022 έγγραφο υποβάλλοντας τα ακόλουθα:

I. Την πολιτική ασφάλειας συστημάτων & δεδομένων, όπως έχει εγκριθεί κατά την 1753/01.06.2018 συνεδρίαση του διοικητικού συμβουλίου της εταιρίας, τα κεντρικά σημεία της οποίας περιγράφονται αναλυτικά στο παράρτημα Α της απόφασης.
II. Την πολιτική προστασίας της ιδιωτικότητας από τον σχεδιασμό και εξ ορισμού (privacy by default and by design), όπως έχει εγκριθεί κατά την 1868/29.12.2021 (θέμα 2ο) Συνεδρίαση του Διοικητικού Συμβουλίου στην οποία, μεταξύ άλλων, αναφέρονται τα εξής:

    α. Η εταιρία εφαρμόζει από σχεδιασμό την προστασία των δεδομένων με την εφαρμογή κατάλληλων τεχνικών μέτρων ανά περίπτωση και ανά επιδιωκόμενο σκοπό σε σχέση πάντα με τον ενδεχόμενο κίνδυνο.
    β. Η εταιρία διασφαλίζει εξ ορισμού ότι η πρόσβαση στα δεδομένα προσωπικού χαρακτήρα περιορίζεται μόνο σε εξουσιοδοτημένα άτομα.
    γ. Η εταιρία στο πλαίσιο της προστασίας της ιδιωτικότητας ως προεπιλογή διασφαλίζει ότι τα προσωπικά δεδομένα προστατεύονται αυτόματα.

Στη συνέχεια, τα ΕΛΤΑ υπέβαλαν τη με υπ' αρ. πρωτ. Γ/ΕΙΣ/9170/27-07-2022 γνωστοποίηση περιστατικού παραβίασης, η οποία συμπληρώθηκε με την Γ/ΕΙΣ/12894/29-12-2022 γνωστοποίηση. Αναφέρεται ότι, ως επακόλουθη δράση του ανωτέρω περιστατικού, οι δράστες δημοσιοποίησαν στον σκοτεινό ιστό του Διαδικτύου (Dark Web) προσωπικά δεδομένα που υπέκλεψαν κατά την παραβίαση του συστήματος του υπευθύνου επεξεργασίας. Η Αρχή, αφού εξέτασε τη σχετική γνωστοποίηση, απέστειλε το έγγραφο με το υπ' αρ. πρωτ. Γ/ΕΞΕ/231/26-01-2023 στα ΕΛΤΑ, ζητώντας τους onion υπερσυνδέσμους της ομάδας Vice Society, στους οποίους βρίσκονται αναρτημένα τα προσωπικά δεδομένα που

σχετίζονται με την εν λόγω υπόθεση, καθώς και οποιαδήποτε συμπληρωματική έκθεση είναι διαθέσιμη αναφορικά με το ζήτημα αυτό. Τα ΕΛΤΑ απάντησαν με το υπ' αρ πρωτ. Γ/ΕΙΣ/1308/21-02-2023 έγγραφο, με το οποίο υποβλήθηκαν τα ακόλουθα:

1. Ο υπερσύνδεσμος της ομάδας στο σκοτεινό ιστό μέσω του οποίου υπάρχει πρόσβαση στα δεδομένα[1].
2. Αναφορά διερεύνησης της εταιρίας Netbull με την οποία διαπιστώνεται ότι το συσχετιζόμενο με την επίθεση της 20ης Μαρτίου 2022, Ransomware Group «Vice Society» έχει αναρτήσει, στις 04 Μαΐου 2022, στην ιστοσελίδα που διατηρεί στο DarkWeb (Hacker Forum), δεδομένα τα οποία σχετίζονται με την επίθεση. Στην αναφορά περιλαμβάνονται τα περιεχόμενα του δέντρου υποκαταλόγων και αρχείων που αναρτήθηκαν στην ιστοσελίδα.
3. Λεπτομερής ανάλυση των αρχείων που αναρτήθηκαν στον ιστότοπο στην οποία περιλαμβάνεται όνομα υποφακέλου, όνομα αρχείου, κατηγορία αρχείου, κατηγορία υποκειμένων δεδομένων, είδη προσωπικών δεδομένων και περιγραφή.

Τα ΕΛΤΑ κλήθηκαν σε ακρόαση στις 29.11.2022, με το υπ' αριθμ. πρωτ. Γ/ΕΞΕ/2888/15-11-2022 έγγραφο της Αρχής. Τα ΕΛΤΑ υπέβαλαν αίτημα αναβολής της συνεδρίασης με την αιτιολογία ότι βρίσκεται σε εξέλιξη διαδικασία ενδελεχούς ελέγχου των αρχείων που έχουν διαρρεύσει στο σκοτεινό ιστό, το οποίο έγινε δεκτό. Η Αρχή υπέβαλε εκ νέου κλήση σε ακρόαση στις 09.05.2023 με το υπ' αριθμ. πρωτ. Γ/ΕΞΕ/1091/02-05-2023 έγγραφο, για το οποίο τα ΕΛΤΑ υπέβαλαν, με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/3260/04-05-2023, αίτημα αναβολής της συνεδρίασης με αιτιολογία την αλλαγή του νομικού συμβούλου της διοίκησης. Τα αίτημα έγινε δεκτό και η ακρόαση αναβλήθηκε για τις 06.06.2023.

Στην συνεδρίαση της 06.06.2023 παρέστησαν εκ μέρους του υπευθύνου επεξεργασίας οι Ιωάννης Γιαννακάκης με ΑΜΔΣΑ …, ο Α από τη Γενική Διεύθυνση …, ο Β, Προϊστάμενος …, η Χαρά Ζέρβα με ΑΜΔΣΑ … και ο Στέργιος Κωνσταντίνου με ΑΜΔΣΑ …, οι οποίοι υπεστήριξαν τα εξής:

1. Κατά το χρόνο εκδήλωσης της κυβερνοεπίθεσης ο οργανισμός αντιμετώπιζε

[1] http://vsociet***.onion/

σοβαρές οικονομικές δυσκολίες. Τα μέτρα ασφάλειας δεν λειτουργούσαν εξαιτίας του εν λόγω οικονομικού περιορισμού.

2. Η κυβερνοεπίθεση ξεκίνησε στις 1:30π.μ. και έγινε αντιληπτή στις 6:30π.μ. Μετά την επιβεβαίωση της ύπαρξης απειλής το σύστημα τέθηκε εκτός λειτουργίας και ξεκίνησε διαδικασία έρευνας, καταγραφής, κατηγοριοποίησης, ταξινόμησης και ενημέρωσης των εμπλεκόμενων μερών.
3. Με στόχο την καλύτερη διαχείριση περιστατικών παραβίασης, έχουν ξεκινήσει προγράμματα εκπαίδευσης του προσωπικού.
4. Διατέθηκαν, μετά το περιστατικό, σημαντικοί πόροι για την θωράκιση της ασφάλειας του συστήματος. Οι ενέργειες μετά το περιστατικό αφορούν την ενίσχυση των τεχνικών και των οργανωτικών ευπαθειών του συστήματος και όχι στην μεταβολή του κανονιστικού πλαισίου λειτουργίας της εταιρίας.
5. Δεν υπήρξαν alerts από την δραστηριότητα των διεργασιών του εργαλείου Windows Management Instrumentation Command (WMIC) εξαιτίας διακοπής της δικτυακής σύνδεσης.

Τέλος, τα ΕΛΤΑ, υπέβαλαν, το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/4815/28-06-2023 υπόμνημα στο οποίο αναφέρονται τα ακόλουθα:

1. Επιπλέον τεχνικές διευκρινίσεις αναφορικά με την κυβερνοεπίθεση, τα βασικά σημεία των οποίων περιγράφονται στο παράρτημα Α της απόφασης.
2. Η μεγάλη πλειονότητα των συστημάτων ανακτήθηκαν από αντίγραφα ασφαλείας (μαγνητικές ταινίες) τα οποία δεν είχαν κρυπτογραφηθεί και από αντίγραφα ασφαλείας τα οποία βρισκόντουσαν εκτός της υποδομής που δέχτηκε την επίθεση. Κάποια συστήματα που κρυπτογραφήθηκαν δεν κατέστη δυνατό να ανακτηθούν, όμως φιλοξενούσαν ιστορικά δεδομένα παλαιών εφαρμογών.
3. Από τη στιγμή που έγινε αντιληπτό το περιστατικό κυβερνοεπίθεσης, τα ΕΛΤΑ προχώρησαν στην άμεση ενημέρωση όλων των εταιρικών πελατών, οι οποίοι στο πλαίσιο των συνεργασιών με τα ΕΛΤΑ δύναται (ανάλογα με το είδος των παρεχόμενων προς αυτούς υπηρεσιών) να ενεργούν είτε ως υπεύθυνοι είτε ως εκτελούντες την επεξεργασία. Ειδικότερα, σχετικά με την συνεργασία των ΕΛΤΑ με την ΕΤΑΙΡΙΑ ΥΔΡΕΥΣΕΩΣ ΚΑΙ ΑΠΟΧΕΤΕΥΣΕΩΣ ΠΡΩΤΕΥΟΥΣΗΣ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ

(εφεξής ΕΥΔΑΠ), η εταιρεία προχώρησε σε ενδελεχή ενημέρωση της αντισυμβαλλομένης τόσο για το περιστατικό περιορισμού της διαθεσιμότητας όσο και για το περιστατικό περιορισμού της εμπιστευτικότητας. Ειδικότερα, τα ΕΛΤΑ ενημέρωσαν σχετικά και την ΕΥΔΑΠ, ότι ενεργούν ως εκτελών την επεξεργασία για λογαριασμό της μόνο ως προς τις υπηρεσίες του άρθρου 1 υποπαρ. (ε) της οικείας μεταξύ τους σύμβασης: «Διαδικασία Ενημέρωσης ΕΥΔΑΠ Α.Ε.», ενώ για τις λοιπές επεξεργασίες τις οποίες εκτελούν τα ΕΛΤΑ, ήτοι την εκπλήρωση της καθολικής υπηρεσίας ταχυδρομικών υπηρεσιών, τα ΕΛΤΑ ενεργούν ως αυτοτελώς υπεύθυνος επεξεργασίας.

4. Όπως προκύπτει από τους ισολογισμούς των ετών 2020, 2021 και 2022, τα ΕΛΤΑ είχαν ζημίες τα τελευταία 3 τελευταία έτη. Συγκεκριμένα: Ο κύκλος εργασιών το 2019 ανήλθε στα 355.647.000. Το 2020, ο κύκλος εργασιών ανήλθε στα 318.467.000, ήτοι σημείωσε μείωση της τάξεως του 10.5%. Το 2021 ο κύκλος εργασιών ανήλθε στα 299.514, ήτοι σημείωσε μείωση της τάξεως του 6% και το 1ο εξάμηνο του 2022 ο κύκλος εργασιών ανήλθε στα 140.051.000, ήτοι σημείωσε μείωση της τάξεως του 5.4% σε σχέση με το αντίστοιχο του 2021

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Σύμφωνα με την παράγραφο 1 στοιχ. στ' του άρθρου 5 του ΓΚΠΔ, τα δεδομένα προσωπικού χαρακτήρα *«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 («ακεραιότητα και εμπιστευτικότητα»).»*

2. Σύμφωνα με το άρθρο 32 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, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:

α) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα,
β) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,
γ) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος,
δ) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

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.
(…)
4. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία λαμβάνουν μέτρα ώστε να διασφαλίζεται ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα τα επεξεργάζεται μόνο κατ' εντολή του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους.»

3. Στην εξεταζόμενη υπόθεση, από την εξέταση της τεχνικής έκθεση περιστατικού κυβερνοασφάλειας προκύπτει ότι τα ΕΛΤΑ δεν τηρούσαν επαρκή τεχνικά μέτρα ασφαλείας στο σύστημα, όπως περιγράφεται αναλυτικά στα παραρτήματα Δ και Ε της απόφασης, κατά παράβαση του άρθρου 32 του ΓΚΠΔ.
4. Επιπροσθέτως, από την εξέταση της πολιτικής ασφαλείας διαπιστώνεται η μη ορθή εφαρμογή πολιτικών όπως περιγράφεται αναλυτικά στο παράρτημα ΣΤ της απόφασης, κατά παράβαση του άρθρου 32 του ΓΚΠΔ.
5. Περαιτέρω, από την με αρ. πρωτ. Γ/ΕΙΣ/9170/27-07-2022 γνωστοποίηση περιστατικού παραβίασης προκύπτει ότι δεν διασφαλίστηκε ο περιορισμός της πρόσβασης μόνο σε εξουσιοδοτημένα άτομα, όπως περιγράφεται αναλυτικά στα παραρτήματα Δ και Ε της απόφασης, κατά παράβαση του 5 παρ. 1 στοιχ. στ'.
6. Εξάλλου, από την εξέταση της τεχνικής έκθεση περιστατικού κυβερνοασφάλειας προκύπτει ότι δεν έγιναν αντιληπτές και δεν αποτράπηκαν οι δραστηριότητες ιχνηλάτισης και αναγνώρισης εκ μέρους του δράστη και η απενεργοποίηση των μηχανισμών ασφαλείας ως συνέπεια της εκτέλεσης διεργασιών του κακόβουλου λογισμικού, όπως περιγράφεται αναλυτικά στα παραρτήματα Δ και Ε της απόφασης, κατά παράβαση του άρθρου 32 του ΓΚΠΔ.
7. Ειδικότερα, σε σχέση με τις παραβάσεις που αναφέρονται στις προηγούμενες σκέψεις 3-6, από το σύνολο των στοιχείων του φακέλου και την ακροαματική διαδικασία, προκύπτει ότι τα ΕΛΤΑ:

    α. Δεν διασφάλισαν, με την εφαρμογή των απαιτούμενων τεχνικών και οργανωτικών μέτρων, την προστασία των προσωπικών δεδομένων από μη εξουσιοδοτημένη ή παράνομη επεξεργασία με αποτέλεσμα να λάβει χώρα απώλεια της κατά το άρθρο 5 παρ. 1 στοιχ. στ' του ΓΚΠΔ επιβαλλόμενης εμπιστευτικότητας.

    β. Δεν εφάρμοσαν, τις κατάλληλες πολιτικές για την προστασία των δεδομένων ώστε να διασφαλιστεί ότι είναι σε θέση να αποδείξουν ότι πραγματοποίησαν επεξεργασία σύμφωνα με τους ορισμούς του άρθρου 32 του ΓΚΠΔ.

    γ. Δεν διασφάλισαν το απόρρητο, την διαθεσιμότητα και την αξιοπιστία των

συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση και την ακεραιότητα των διαδικασιών για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για την ασφάλεια της επεξεργασίας, ούτως ώστε διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, για τα δικαιώματα των υποκειμένων, κατά το άρθρο 32 παρ. 1 στοιχ. β' του ΓΚΠΔ.

8. Με βάση τα ανωτέρω, η Αρχή κρίνει ότι έλαβαν χώρα παραβάσεις των κατά άρθρα 5 παρ. 1 στοιχ. στ' και 32 ΓΚΠΔ υποχρεώσεων του υπευθύνου επεξεργασίας. Για τις παραβιάσεις των άρθρων αυτών, που συνιστούν αυτοτελείς παραβάσεις, συντρέχει περίπτωση άσκησης των διορθωτικών εξουσιών της Αρχής με την επιβολή, κατ' εφαρμογή του άρθρου 58 παρ. 2 στοιχ. θ' του ΓΚΠΔ, με βάση τις περιστάσεις που διαπιστώθηκαν, αποτελεσματικού, αναλογικού και αποτρεπτικού διοικητικού προστίμου κατ' άρθρο 83 του ΓΚΠΔ.

9. Για την επιμέτρηση του προστίμου λαμβάνονται υπόψη τα εξής κριτήρια σύμφωνα με τις κατευθυντήριες γραμμές 4/2022 του ΕΣΠΔ για τον υπολογισμό των διοικητικών προστίμων:[2]

   I. Τα δεδομένα κύκλων εργασιών και συγκεκριμένα:

      a. Τελευταίος διαθέσιμος κύκλος εργασιών: **140.051.000**[3] € (01/01/2022-30/06/2022).

      b. Τελευταίος διαθέσιμος ετήσιος κύκλος εργασιών 2021: **299.514.000**[4] € (01/01/2021-31/12/2021).

      c. Μείωση του κύκλου εργασιών της τάξεως του 5.4% μεταξύ των εξαμήνων 01/01/2021-30/06/2021 και 01/01/2022-30/06/2022.[5]

   II. Το ότι η βαρύτητα των διαπιστωμένων παραβάσεων κρίνεται σε όλες τις περιπτώσεις ως μεγάλη, λαμβάνοντας υπόψη:

[2] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_en - έκδοση 2.0, μετά τη διαβούλευση.
[3] Γ/ΕΙΣ/4815/28-06-2023
[4] Γ/ΕΙΣ/4815/28-06-2023, https://publicity.businessportal.gr/company/1092101000
[5] Γ/ΕΙΣ/4815/28-06-2023

α. το μεγάλο εύρος των επηρεαζόμενων προσώπων ήτοι 4.000.000-5.000.000, μεταξύ των οποίων υπάλληλοι ΕΛΤΑ, στελέχη, μέλη Δ.Σ., εκμισθωτές, πελάτες, εξωτερικοί συνεργάτες, διανομείς, αντισυμβαλλόμενοι, συνταξιούχοι, ταχυδρομικοί πράκτορες, δανειολήπτες, εγγυητές και

β. Το υψηλό ύψος της ζημίας, ήτοι εκτεταμένη διαρροή δεδομένων που αφορά προσωπικά στοιχεία, οικονομικά δεδομένα κλπ. και η απώλεια διαθεσιμότητας υπηρεσιών.

γ. Το ότι έλαβε χώρα παραβίαση του συστήματος του υπευθύνου επεξεργασίας, μη εξουσιοδοτημένη πρόσβαση σε πόρους, εγκατάσταση κακόβουλων λογισμικών και δημοσιοποίηση δεδομένων στο σκοτεινό ιστό, όπως περιγράφεται αναλυτικά στα παραρτήματα Γ, Δ, Ε και ΣΤ.

δ. Το ότι υπήρξαν παραλείψεις εφαρμογής της πολιτικής ασφαλείας, αδυναμία διασφάλισης της πρόσβασης σε δεδομένα από μη εξουσιοδοτημένους χρήστες, μη επαρκής τεχνική τεκμηρίωση σχετικά με τα ζητήματα της συλλογής των κωδικών πρόσβασης τομέα και της μη αξιοποίησης των μηνυμάτων προειδοποίησης ασυνήθιστης δραστηριότητας από τους μηχανισμούς προστασίας, όπως περιγράφεται αναλυτικά στα παραρτήματα Δ και Ε.

ε. Το ότι επηρεάστηκαν ιδιαίτερης σημασίας κατηγορίες προσωπικών δεδομένων, όπως οικονομικά στοιχεία υπευθύνου επεξεργασίας και επηρεαζόμενων εταιριών/φορέων, στοιχεία εργαζομένων, αλληλογραφία, διαγωνισμοί, πρακτικά ΔΣ, φωτογραφίες προσωπικού αρχείου και πελατών, στοιχεία κλήσης μαρτύρων, έκθεση κατάθεσης μάρτυρα, έκθεση καθολικής επιθεώρησης, εγγραφές βάσεων δεδομένων, κατάλογος συνταξιούχων ΟΓΑ, στοιχεία πελατών/προμηθευτών, υπεύθυνες δηλώσεις/εξουσιοδοτήσεις.

στ. Το ότι δεν ανακτήθηκαν ιστορικά δεδομένα εφαρμογών. Δεν πάρθηκαν μέτρα περιορισμού της ανάρτησης των δεδομένων στο σκοτεινό ιστό.

III. Η Αρχή λαμβάνει υπόψη ως ελαφρυντικά στοιχεία τα εξής:

α. Κατόπιν του περιστατικού, ενισχύθηκε η ασφάλεια του συστήματος με τη λήψη τόσο τεχνικών όσο και οργανωτικών μέτρων.

β. Δεν υπήρξε διαρροή ευαίσθητων προσωπικών δεδομένων.

γ. Ο υπεύθυνος επεξεργασίας ανέθεσε σε τρίτη εταιρία τη διεξαγωγή πρότυπης διαδικασίας διαχείρισης και ανταπόκρισης σε περιστατικά και εφάρμοσε όλα τα στάδια αυτής.

δ. Υπήρξε επαναφορά σημαντικού μέρους του όγκου των δεδομένων από αντίγραφα ασφαλείας. Υπήρξε επαναφορά διαθεσιμότητας υπηρεσιών.

ε. Ο υπεύθυνος επεξεργασίας υπέβαλε πρόσθετη γνωστοποίηση περιστατικού παραβίασης στο οποίο περιλαμβάνονται αναλυτικά στοιχεία για την διαρροή δεδομένων στο σκοτεινό ιστό.

στ. Κατά την εκδήλωση της επίθεσης ο υπεύθυνος επεξεργασίας ήταν σε δυσχερή οικονομική κατάσταση. Η εταιρία εμφάνιζε ζημιές στον κύκλο εργασιών της μέχρι τις 30/6/2022.

10. Κατόπιν συνεκτίμησης των ανωτέρω επιβαρυντικών και ελαφρυντικών κριτηρίων (σκέψη 9 σημεία ii) και iii) ανωτέρω), καθώς και των δεδομένων του κύκλου εργασιών του ΥΕ (σκέψη 9 σημείο i) ανωτέρω), η Αρχή κρίνει ότι πρέπει να επιβληθεί στην εταιρία με την επωνυμία «ΕΛΛΗΝΙΚΑ ΤΑΧΥΔΡΟΜΕΙΑ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ» πρόστιμο κοντά στα χαμηλά του στατικού εύρους που ορίζουν οι κατευθυντήριες γραμμές 4/2022 του ΕΣΠΔ για το είδος των παραβάσεων με μεγάλη σοβαρότητα και ίσο με το 1% του τελευταίου διαθεσίμου ετησίου κύκλου εργασιών του ΥΕ.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή

Ασκώντας τις διορθωτικές εξουσίες με βάση το άρθρο 58 παρ. 2 στοιχ. θ) του ΓΚΠΔ, επιβάλλει πρόστιμο ύψους δύο εκατομμυρίων εννιακόσιων ενενήντα πέντε χιλιάδων εκατόν

σαράντα ευρώ (2.995.140) στην εταιρία με την επωνυμία «ΕΛΛΗΝΙΚΑ ΤΑΧΥΔΡΟΜΕΙΑ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ», για τους λόγους που εκτενώς αναφέρονται στο σκεπτικό.

Ο Πρόεδρος	**Η Γραμματέας**
Κωνσταντίνος Μενουδάκος	**Ειρήνη Παπαγεωργοπούλου**