ΑΠΔΠΧ 10/2024 ΕΠΙΒΟΛΗ ΠΡΟΣΤΙΜΟΥ 2.995.140 ΕΥΡΩ ΣΤΑ ΕΛΤΑ ΓΙΑ ΤΗΝ ΠΑΡΑΒΙΑΣΗ ΤΩΝ ΑΡΧΩΝ ΤΗΣ ΑΚΕΡΑΙΟΤΗΤΑΣ ΚΑΙ ΤΗΣ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ ΚΑΙ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Σουζάνα Παπακωνσταντίνου
Δικηγόρος,
Υπ. Δρ Συνταγματικού Δικαίου
Τμ. Δημόσιας Διοίκησης, Πάντειο Πανεπιστήμιο
Μ.Δ.Ε. Κοινωνικής Προστασίας (Δίκαιο Κοιν. Ασφάλισης – Δημ. Δ. Υγείας) Νομική Σχολή ΕΚΠΑ

Ι. ΙΣΤΟΡΙΚΟ

Η εταιρία «ΕΛΛΗΝΙΚΑ ΤΑΧΥΔΡΟΜΕΙΑ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ», εφεξής ΕΛΤΑ, υπέβαλε στην Αρχή γνωστοποιήσεις περιστατικών παραβίασης που αφορούσαν στην κρυπτογράφηση λογισμικού στο σύστημα της εταιρείας, ως αποτέλεσμα κακόβουλης επίθεσης από τρίτους και στη διαρροή δεδομένων προσωπικού χαρακτήρα, τα οποία σε δεύτερο χρόνο δημοσιεύθηκαν στον σκοτεινό ιστό (Dark Web). Στη συνέχεια, η Αρχή ζήτησε την περιγραφή των ενεργειών που έλαβαν χώρα στο πλαίσιο διερεύνησης/αντιμετώπισης του εν λόγω περιστατικού, κάθε σχετική πληροφορία και αναφορά προς άλλες εταιρείες ή τρίτους, καθώς και κάθε ενέργεια σε σχέση με την ενημέρωση των υποκειμένων των δεδομένων και τυχόν τρίτων μερών. Τα ΕΛΤΑ απάντησαν υποβάλλοντας τεχνική έκθεση περιστατικού κυβερνοασφάλειας σχετικά με τις διαδικασίες ενημέρωσης των ΕΛΤΑ για το εν λόγω περιστατικό. Ακολούθως, η Αρχή ζήτησε από τα ΕΛΤΑ τις πολιτικές και τις 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 κατά την απάντησή τους υπέβαλαν τα ζητούμενα, ενώ στη συνέχεια υπέβαλαν επιπλέον γνωστοποίηση παραβίασης και συμπληρωματική αυτής σχετικά με την επακόλουθη δημοσιοποίηση δεδομένων προσωπικού χαρακτήρα που είχαν υποκλαπεί κατά την παραβίαση του συστήματος υπεύθυνου επεξεργασίας στον σκοτεινό ιστό (Dark Web). Η

Αρχή εξετάζοντας τα ανωτέρω ζήτησε από τα ΕΛΤΑ τους onion υπερσυνδέσμους, στους οποίους βρίσκονταν αναρτημένα τα σχετικά με την υπόθεση δεδομένα προσωπικού χαρακτήρα, καθώς και οποιαδήποτε διαθέσιμη συμπληρωματική έκθεση σχετικά με το ζήτημα. Τα ΕΛΤΑ απάντησαν παρέχοντας τις σχετικές πληροφορίες και στη συνέχεια κλήθηκαν σε ακρόαση από την Αρχή. Η συνεδρίαση, έπειτα από δύο αναβολές που είχαν ζητήσει τα ΕΛΤΑ, έλαβε χώρα στις 06.06.2023.

Πιο αναλυτικά, τα ΕΛΤΑ υπέβαλαν στην Αρχή τις υπ' αρ. πρωτ. Γ/ΕΙΣ/5033/23.03.2022 και Γ/ΕΙΣ/9170/27.07.2022 γνωστοποιήσεις περιστατικών παραβίασης που αφορούσαν στην κρυπτογράφηση λογισμικού στο σύστημα της εταιρείας, ως αποτέλεσμα κακόβουλης επίθεσης από τρίτους, και διαρροή δεδομένων προσωπικού χαρακτήρα τα οποία σε επόμενη φάση δημοσιεύθηκαν στον σκοτεινό ιστό (Dark Web). Επιπλέον, από την ανάλυση της κυβερνοεπίθεσης προέκυψε ότι έλαβαν χώρα, στο πλαίσιο της παραβίασης του συστήματος του υπεύθυνου επεξεργασίας, ενέργειες μη εξουσιοδοτημένης απομακρυσμένης πρόσβασης σε σταθμούς εργασίας και σε αρχεία, εύρεση των κωδικών πρόσβασης των λογαριασμών διαχείρισης του τομέα του δικτύου, καθώς και μη εξουσιοδοτημένη πρόσβαση σε αρχεία και φακέλους και εγκατάσταση κακόβουλων διεργασιών.

Στη συνέχεια η Αρχή, αφού εξέτασε τη γνωστοποίηση των ΕΛΤΑ, ζήτησε με το υπ' αρ. πρωτ. Γ/ΕΞΕ/1208/19.05.2022 από τα ΕΛΤΑ την περιγραφή των ενεργειών που έλαβαν χώρα στο πλαίσιο διερεύνησης/αντιμετώπισης του εν λόγω περιστατικού, κάθε σχετική πληροφορία και αναφορά προς άλλες εταιρείες ή τρίτους, καθώς και κάθε ενέργεια σε σχέση με την ενημέρωση των 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 συμπεριλαμβανόταν τεχνική έκθεση περιστατικού κυβερνοασφάλειας, τα κεντρικά σημεία της οποίας ήταν τα εξής:

- Έλαβε χώρα ενημέρωση προς το κοινό, εκ μέρους του υπεύθυνου επεξεργασίας, σχετικά με την παραβίαση αλλά και σχετικά με τις ενέργειες κατόπιν της παραβίασης.
- Υπήρξε εσωτερική ανακοίνωση υπευθύνου επεξεργασίας στην οποία προσδιορίζονταν οι ενέργειες επαναφοράς του συστήματος.
- Ενημερώθηκαν οι διεθνείς φορείς που επηρεάζονταν από το περιστατικό.
- Ενημερώθηκε η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων και η Εθνική Αρχή Κυβερνοασφάλειας.
- Ενημερώθηκε η Εταιρία Δικτύου Ύδρευσης και Αποχέτευσης Πρωτευούσης, η οποία είχε υποβάλλει και η ίδια αρχική αναφορά γνωστοποίησης με αρ. πρωτ. Γ/ΕΙΣ/5224/25.03.2022 και οριστική με αρ. πρωτ. Γ/ΕΙΣ/8266/24.06.2022.
- Υποβλήθηκε συμπληρωματική γνωστοποίηση παραβίασης, με τα νέα δεδομένα που προέκυψαν κατά τη διερεύνηση του περιστατικού.

Στη συνέχεια, η Αρχή ζήτησε με το υπ' αρ. πρωτ. Γ/ΕΞΕ/1499/21.06.2022 έγγραφό της τις πολιτικές και τις διαδικασίες πληροφορικής και ασφάλειας πληροφοριών του φορέα, καθώς 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 την

πολιτική ασφάλειας συστημάτων και δεδομένων και την πολιτική προστασίας της ιδιωτικότητας εξ ορισμού και από τον σχεδιασμό (privacy by default and by design), στην οποία αναφερόταν ότι:

- Η εταιρεία προστάτευε τα δεδομένα προσωπικού χαρακτήρα εφαρμόζοντας τα κατάλληλα τεχνικά και οργανωτικά μέτρα από τον σχεδιασμό, ανά περίπτωση και ανά επιδιωκόμενο σκοπό, σε σχέση με τον ενδεχόμενο κίνδυνο.
- Η εταιρεία εξασφάλιζε εξ ορισμού τον περιορισμό της πρόσβασης στα δεδομένα προσωπικού χαρακτήρα μόνον σε εξουσιοδοτημένα άτομα.
- Η εταιρεία, στο πλαίσιο της προστασίας της ιδιωτικότητας, εξασφάλιζε εξ ορισμού ότι τα δεδομένα προσωπικού χαρακτήρα προστατεύονται αυτόματα.

Επιπλέον, τα ΕΛΤΑ υπέβαλαν την υπ' αρ. πρωτ. Γ/ΕΙΣ/9170/27.07.2022 γνωστοποίηση και τη συμπληρωματική αυτής, υπ' αρ. πρωτ. Γ/ΕΙΣ/12894/29.12.2022 γνωστοποίηση, στις οποίες αναφερόταν ως επακόλουθη δράση του περιστατικού η δημοσιοποίηση στον σκοτεινό ιστό (Dark Web) εκ μέρους των δραστών των προσωπικών δεδομένων που είχαν υποκλέψει κατά την παραβίαση του συστήματος.

Η Αρχή, ακολούθως, ζήτησε από τα ΕΛΤΑ με το υπ' αρ. πρωτ. Γ/ΕΞΕ/231/26.01.2023 έγγραφό της τους onion υπερσυνδέσμους της Ομάδας Vice Society, στους οποίους είχαν αναρτηθεί τα προσωπικά δεδομένα που είχαν υποκλαπεί, καθώς και οποιαδήποτε συμπληρωματική έκθεση σχετικά με το εν λόγω ζήτημα.

Τα ΕΛΤΑ απάντησαν με το υπ' αρ. πρωτ. Γ/ΕΙΣ/1308/21.02.2023 έγγραφο, το οποίο συμπεριλάμβανε τα εξής:

- Τον σχετικό υπερσύνδεσμο στον σκοτεινό ιστό.
- Αναφορά διερεύνησης της εταιρείας Netbull, με την οποία επιβεβαιωνόταν ότι το συσχετιζόμενο με την επίθεση στις 20.03.2022 Ransomware Group ''Vice Society'' είχε αναρτήσει στις 04.05.2022 στην ιστοσελίδα που διατηρούσε στο Dark Web δεδομένα σχετικά με την επίθεση.
- Λεπτομερή ανάλυση των αρχείων που αναρτήθηκαν στον ιστότοπο αυτό, όπως π.χ. κατηγορία υποκειμένων δεδομένων, είδη δεδομένων προσωπικού χαρακτήρα κ.λπ.

Η Αρχή κάλεσε τα ΕΛΤΑ σε ακρόαση στις 29.11.2022 κι έπειτα από δύο αναβολές εκ μέρους των ΕΛΤΑ η συνεδρίαση πραγματοποιήθηκε στις 06.06.2023.

Κατά τη συνεδρίαση τα ΕΛΤΑ υποστήριξαν τα εξής:

- Την περίοδο που εκδηλώθηκε η κυβερνοεπίθεση, αντιμετώπιζαν σοβαρές οικονομικές δυσκολίες και εξαιτίας αυτών τα μέτρα ασφαλείας δεν λειτουργούσαν.
- Η κυβερνοεπίθεση έγινε αντιληπτή έπειτα από πέντε (5) ώρες, όταν το σύστημα τέθηκε εκτός λειτουργίας, και ξεκίνησαν οι διαδικασίες έρευνας του περιστατικού και ενημέρωσης των εμπλεκόμενων μερών.
- Με στόχο την καλύτερη διαχείριση παρόμοιων περιστατικών έχουν ξεκινήσει προγράμματα εκπαίδευσης του προσωπικού.
- Κατόπιν του περιστατικού διατέθηκαν σημαντικοί πόροι προκειμένου να αυξηθεί η ασφάλεια του συστήματος, όπως η ενίσχυση των τεχνικών και οργανωτικών μέτρων κ.ά.
- Δεν υπήρξαν alerts από τη δραστηριότητα των διεργασιών του εργαλείου Windows

Management Instrumentation Command (WMIC), εξαιτίας της διακοπής της διαδικτυακής σύνδεσης.

Επιπλέον, τα ΕΛΤΑ υπέβαλαν το υπ' αρ. πρωτ. Γ/ΕΙΣ/4815/28.06.2023 υπόμνημα, στο οποίο αναφέρονταν, συν τοις άλλοις, τα εξής:

- Τα περισσότερα από τα συστήματα ανακτήθηκαν από αντίγραφα ασφαλείας (μαγνητικές ταινίες), τα οποία δεν είχαν κρυπτογραφηθεί και από αντίγραφα τα οποία βρίσκονταν εκτός της υποδομής που δέχθηκε την επίθεση. Ωστόσο, δεν κατέστη εφικτό να ανακτηθούν ιστορικά αρχεία εφαρμογών.
- Ενημερώθηκαν άμεσα όλοι οι εταιρικοί πελάτες για τους οποίους τα ΕΛΤΑ, στο πλαίσιο συνεργασίας τους, λειτουργούσαν είτε ως υπεύθυνοι επεξεργασίας είτε ως εκτελούντες την επεξεργασία, μεταξύ των οποίων και η «ΕΤΑΙΡΕΙΑ ΥΔΡΕΥΣΕΩΣ ΚΑΙ ΑΠΟΧΕΤΕΥΣΕΩΣ ΠΡΩΤΕΥΟΥΣΗΣ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ» (ΕΥΔΑΠ).
- Σύμφωνα με τους ισολογισμούς των ετών 2020-2022, τα ΕΛΤΑ παρουσίαζαν ζημία τα τελευταία έτη.

II. ΝΟΜΟΘΕΣΙΑ – ΝΟΜΟΛΟΓΙΑ

ΑΡΘΡΟ 4 ΓΚΠΔ

Σύμφωνα με το στοιχείο 7 του άρθρου 4 ΓΚΠΔ, ως «*υπεύθυνος επεξεργασίας*» νοείται «*το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους*».

ΑΡΘΡΟ 5 ΓΚΠΔ

Στο άρθρο 5 του ΓΚΠΔ ορίζονται οι αρχές που διέπουν την επεξεργασία δεδομένων χαρακτήρα. Σύμφωνα με την παρ. 1 στοιχ. στ΄, τα δεδομένα προσωπικού χαρακτήρα «*υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων και την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών και οργανωτικών μέτρων ("ακεραιότητα και εμπιστευτικότητα")*».

Στο Προοίμιο του ΓΚΠΔ και συγκεκριμένα στην Αιτιολογική Σκέψη 39 ορίζεται ότι «*τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να υφίστανται επεξεργασία κατά τρόπο που να διασφαλίζει την ενδεδειγμένη προστασία και εμπιστευτικότητα των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων και για να αποτρέπεται κάθε ανεξουσιοδότητη πρόσβαση σε αυτά τα δεδομένα προσωπικού χαρακτήρα και στον εξοπλισμό που χρησιμοποιείται για την επεξεργασία τους ή τη χρήση αυτών των δεδομένων προσωπικού χαρακτήρα και του εν λόγω εξοπλισμού*».

Επιπλέον, στην παράγραφο 2 του άρθρου 5 του ΓΚΔΠ εισάγεται η θεμελιώδης «*αρχή της λο-*

γοδοσίας», που συνιστά *«ακρογωνιαίο λίθο του ΓΚΠΔ*[1]» και η οποία ορίζει ρητώς ότι ο υπεύθυνος επεξεργασίας *«φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 ("λογοδοσία")»*.

ΑΡΘΡΟ 25 ΓΚΠΔ

Σύμφωνα με το άρθρο 25 παρ. 1 ΓΚΠΔ, σχετικά με την προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, *«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»*.

ΑΡΘΡΟ 32 ΓΚΠΔ

Σύμφωνα με την παράγραφο 1 του άρθρου 32 ΓΚΠΔ, *«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»*.

Επιπλέον, σύμφωνα με την παράγραφο 2 του άρθρου 32 του ΓΚΠΔ, *«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»*.

Επίσης, κατά την παράγραφο 4 του άρθρου 32 του ΓΚΠΔ, *«ο υπεύθυνος επεξεργασίας και*

[1] ΑΠΔΠΧ 35/2022, σκ. 7, σελ. 10.

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».

ΑΡΘΡΟ 33 ΓΚΠΔ

Σύμφωνα με το άρθρο 33 παρ. 1 ΓΚΠΔ *«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».*

Επιπλέον, σύμφωνα με τις από 06.02.2018 Κατευθυντήριες Γραμμές της Ομάδας Εργασίας του Άρθρου 29 της Οδηγίας 95/46/ΕΚ (νυν Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων – EDPB) για τη Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα[2], ανάμεσα στους τύπους σύμφωνα με τους οποίους κατηγοριοποιούνται οι παραβιάσεις προσωπικών δεδομένων είναι αυτός που γίνεται με βάση την «αρχή της εμπιστευτικότητας», όταν διαπιστώνεται πρόσβαση άνευ δικαιώματος σε προσωπικά δεδομένα (''confidentiality breach'').

Επίσης, σύμφωνα με τις Αιτιολογικές Σκέψεις 85 και 75 του ΓΚΠΔ, η παραβίαση δεδομένων προσωπικού χαρακτήρα μπορεί, εάν δεν αντιμετωπιστεί κατάλληλα και έγκαιρα, να έχει ως αποτέλεσμα σωματική, υλική ή ηθική βλάβη, όπως για παράδειγμα απώλεια του ελέγχου επί των δεδομένων προσωπικού χαρακτήρα, περιορισμό δικαιωμάτων, διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια, παράνομη άρση της ψευδωνυμοποίησης, κ.ά.[3].

Κατά την παράγραφο 5 του άρθρου 33 ΓΚΠΔ, *«ο υπεύθυνος επεξεργασίας τεκμηριώνει κάθε παραβίαση δεδομένων προσωπικού χαρακτήρα, που συνίστανται στα πραγματικά περιστατικά που αφορούν τη 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».*

ΑΡΘΡΟ 34 ΓΚΠΔ

Σύμφωνα με το άρθρο 34 παρ. 1 ΓΚΠΔ *«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] *Guidelines on Personal data breach notification under Regulation 2016/679,* WP 250 rev. 1.

[3] ΑΠΔΠΧ 6/2022, σελ. 10.

Επίσης, κατά την παράγραφο 2 του άρθρου 34 ΓΚΠΔ, *«στην ανακοίνωση στο υποκείμενο των δεδομένων (...) 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)».*

III. ΤΟ ΣΚΕΠΤΙΚΟ ΤΗΣ ΑΡΧΗΣ, ΟΙ ΠΑΡΑΒΑΣΕΙΣ ΤΟΥ ΓΚΠΔ ΚΑΙ ΤΑ ΠΡΑΓΜΑΤΙΚΑ ΠΕΡΙΣΤΑΤΙΚΑ ΠΟΥ ΣΥΝΕΤΕΛΕΣΑΝ ΣΤΗΝ ΑΠΟΦΑΣΗ

Η Αρχή εντόπισε τις εξής παραβάσεις:

- Δεν είχαν ληφθεί και δεν εφαρμόζονταν επαρκή τεχνικά και οργανωτικά μέτρα ασφαλείας, σύμφωνα με όσα ορίζονται στο άρθρο 32 του ΓΚΠΔ.
- Δεν υπήρχε ορθή εφαρμογή της πολιτικής ασφαλείας που είχαν υιοθετήσει τα ΕΛΤΑ, κατά παράβαση του άρθρου 32 του ΓΚΠΔ.
- Δεν διασφαλίστηκε ο περιορισμός της πρόσβασης στο σύστημα μόνο σε εξουσιοδοτημένα άτομα, κατά παράβαση του άρθρου 5 παρ. 1 στοιχ. στ΄ του ΓΚΠΔ και της αρχής εμπιστευτικότητας.
- Κατά παράβαση των άρθρων 5 παρ. 1 στοιχ. στ΄ και 32 ΓΚΠΔ, δεν διασφαλίστηκε η αξιοπιστία των συστημάτων και η ακεραιότητα των διαδικασιών, ούτε και η αποτελεσματικότητα των τεχνικών και οργανωτικών μέτρων για την ασφάλεια της επεξεργασίας, με αποτέλεσμα να μην διασφαλίζεται επαρκές επίπεδο ασφαλείας έναντι των πιθανών κινδύνων για τα υποκείμενα των δεδομένων.

Έτσι, η Αρχή έκρινε ότι σύμφωνα με τα ανωτέρω έλαβαν χώρα οι παραβάσεις των άρθρων 5 παρ. 1 στοιχ. στ΄ του ΓΚΠΔ (αρχή ακεραιότητας και εμπιστευτικότητας) και 32 παρ. 1, 2 και 4 του ΓΚΠΔ (ασφάλεια επεξεργασίας), οι οποίες μάλιστα είναι και αυτοτελείς[4]. Για αυτές τις παραβάσεις, συντρέχει η περίπτωση του άρθρου 58 παρ. 2 στοιχ. θ΄ του ΓΚΠΔ, σύμφωνα με το οποίο η Αρχή ασκεί τις διορθωτικές της εξουσίες, επιβάλλοντας αποτελεσματικό, αναλογικό και αποτρεπτικό πρόστιμο, σύμφωνα με τα οριζόμενα στο άρθρο 83 του ΓΚΠΔ.

Η Αρχή για την επιμέτρηση του προστίμου έλαβε υπ' όψιν τους εξής παράγοντες[5]:

- Τα δεδομένα των κύκλων εργασιών των ΕΛΤΑ και συγκεκριμένα τη σταδιακή μείωση αυτών μεταξύ των ετών 2021 και 2022.
- Την αυξημένη βαρύτητα των παραβάσεων που διαπιστώθηκαν. Πιο αναλυτικά, πολύ σημαντικοί παράμετροι επιβάρυνσης των παραβάσεων ήταν οι εξής:

– Το μεγάλο εύρος των επηρεαζόμενων προσώπων (έως και 5.000.000 πρόσωπα).
– Το ύψος της ζημίας λόγω της εκτεταμένης διαρροής δεδομένων, του είδους των δεδομένων και της απώλειας διαθεσιμότητας των υπηρεσιών.
– Η παραβίαση του συστήματος του υπεύθυνου επεξεργασίας και η μη εξουσιοδοτημένη πρόσβαση σε αυτό, καθώς και η εγκατάσταση κακόβουλου λογισμικού και η διαρροή δεδομένων στον σκοτεινό ιστό (Dark Web).

[4] ΑΠΔΠΧ 10/2024, σκ. 8, σελ. 9.
[5] ΑΠΔΠΧ 10/2024, σκ. 9, σελ. 9.

- Ο εντοπισμός παραλείψεων εφαρμογής της πολιτικής ασφαλείας, αδυναμίας διασφάλισης της πρόσβασης σε δεδομένα από μη εξουσιοδοτημένους χρήστες, μη επαρκούς τεχνικής τεκμηρίωσης σχετικά με τα ζητήματα της συλλογής των κωδικών πρόσβασης τομέα και η μη αξιοποίηση των μηνυμάτων προειδοποίησης (alerts) ασυνήθιστης δραστηριότητας από τους μηχανισμούς προστασίας.
- Το γεγονός ότι επηρεάστηκαν ιδιαίτερης σημασίας κατηγορίες προσωπικών δεδομένων, όπως π.χ. οικονομικά στοιχεία υπεύθυνου επεξεργασίας και επηρεαζόμενων εταιρειών/φορέων, στοιχεία εργαζομένων, πελατών, προμηθευτών κ.ά.
- Η μη ανάκτηση ιστορικών δεδομένων εφαρμογών και η μη λήψη μέτρων περιορισμού της ανάρτησης δεδομένων στον σκοτεινό ιστό (Dark Web).

Επιπλέον, η Αρχή έλαβε υπόψιν της τα εξής ελαφρυντικά στοιχεία:

- Κατόπιν του περιστατικού, ελήφθησαν τεχνικά και οργανωτικά μέτρα, με σκοπό την ενίσχυση της ασφάλειας του συστήματος, ενώ ανατέθηκε σε τρίτη εταιρεία η διεξαγωγή πρότυπης διαδικασίας διαχείρισης και ανταπόκρισης σε αντίστοιχα περιστατικά.
- Δεν διέρρευσαν δεδομένα προσωπικού χαρακτήρα ειδικών κατηγοριών («ευαίσθητα» δεδομένα).
- Τα περισσότερα από τα δεδομένα ανακτήθηκαν από αντίγραφα ασφαλείας και οι υπηρεσίες κατεστάθησαν διαθέσιμες.
- Υπεβλήθη από τον υπεύθυνο επεξεργασίας επιπλέον αναλυτική γνωστοποίηση περιστατικού παραβίασης περί διαρροής δεδομένων στον σκοτεινό ιστό (Dark Web).
- Κατά την εκδήλωση της επίθεσης, τα ΕΛΤΑ (υπεύθυνος επεξεργασίας) βρίσκονταν σε δυσχερή οικονομική κατάσταση, εμφανίζοντας ζημία στους κύκλους εργασιών τους.

IV. Η ΑΠΟΦΑΣΗ ΤΗΣ ΑΡΧΗΣ

Η Αρχή, λαμβάνοντας υπόψη όλα τα ανωτέρω, με βάση το άρθρο 58 παρ. 2 εδ. θ΄ του ΓΚΠΔ, αλλά και όσα ορίζουν οι Κατευθυντήριες Γραμμές 4/2022[6] του ΕΣΠΔ σχετικά με τον υπολογισμό των διοικητικών προστίμων για παραβάσεις με μεγάλη σοβαρότητα, επέβαλε στα ΕΛΤΑ πρόστιμο συνολικού ύψους 2.995.140 ευρώ, για τις παραβάσεις των άρθρων 5 παρ. 1 στοιχ. στ΄ και 32 παρ. 1, 2 και 4 του ΓΚΠΔ.

V. ΣΚΕΨΕΙΣ – ΠΑΡΑΤΗΡΗΣΕΙΣ

Η απόφαση 10/2024 της Αρχής είναι σπουδαίας σημασίας, καθώς οφείλουμε να συγκρατήσουμε τα εξής:

Επεβλήθη στα ΕΛΤΑ από την ΑΠΔΠΧ ένα από τα υψηλότερα πρόστιμα που έχουν επιβληθεί ιστορικά σε ελληνική επιχείρηση, καθώς έλαβε χώρα παραβίαση και διαρροή δεδομένων προσωπικού χαρακτήρα μέσω κυβερνοεπίθεσης και σε δεύτερο χρόνο δημοσίευση αυτών των δεδομένων στον σκοτεινό ιστό (Dark web). Οι λόγοι για τους οποίους συνέβησαν αυτές οι παραβάσεις ήταν

[6] EDPB, *Guidelines 04/2022 on the calculation of administrative fines under the GDPR,* διαθέσιμο στο link.

οι εξής: Πρώτον, ο υπεύθυνος επεξεργασίας δεν είχε λάβει τα κατάλληλα τεχνικά και οργανωτικά μέτρα, τα οποία θα μπορούσαν να προφυλάξουν τα λειτουργικά συστήματα από τον κίνδυνο της διαρροής των δεδομένων προσωπικού χαρακτήρα. Δεύτερον, φάνηκε πως η πολιτική ασφαλείας της επεξεργασίας δεδομένων που είχε υιοθετήσει ο υπεύθυνος επεξεργασίας δεν εφαρμόστηκε στην πράξη, καθώς, εκ του αποτελέσματος, παραβιάσθηκε το σύστημα και πραγματοποιήθηκε πρόσβαση στα δεδομένα προσωπικού χαρακτήρα από μη εξουσιοδοτημένα άτομα. Τρίτον, δεν ελήφθησαν τα κατάλληλα μέτρα ούτε έγιναν οι απαραίτητες ενέργειες μετά από την κυβερνοεπίθεση και την παραβίαση, με αποτέλεσμα, σε δεύτερο χρόνο, να διαρρεύσουν στον σκοτεινό ιστό (Dark Web) τα δεδομένα προσωπικού χαρακτήρα που είχαν αντληθεί.

Συνεπώς, οι ανωτέρω παραβιάσεις των αρχών της ακεραιότητας, της εμπιστευτικότητας[7] και της ασφάλειας της επεξεργασίας[8] συνιστούν γενικότερα παραβίαση της θεμελιώδους αρχής του ΓΚΠΔ, της αρχής της νομιμότητας[9] της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Τονίζεται η σημασία της προστασίας των υποκειμένων των δεδομένων προσωπικού χαρακτήρα, εξ ορισμού και από τον σχεδιασμό, από τους πιθανούς κινδύνους επεξεργασίας: Συγκεκριμένα, οι πιο «τεχνικές» διατάξεις του ΓΚΠΔ που αφορούν σε «τακτικές» προστασίας των δεδομένων από τον σχεδιασμό, όπως η διενέργεια εκτίμησης αντικτύπου πιθανών κινδύνων από την επεξεργασία δεδομένων, η τήρηση αρχείου δραστηριοτήτων επεξεργασίας ή η ορθή αντιστοίχιση νομικών βάσεων επεξεργασίας και αντίστοιχων σκοπών επεξεργασίας εκ των προτέρων, στοχεύουν στην τήρηση της νομιμότητας της επεξεργασίας των δεδομένων, στη διαφάνεια, στην ορθή ενημέρωση των υποκειμένων των δεδομένων, στην ελαχιστοποίηση των δεδομένων κ.ά. Ωστόσο, απώτερος σκοπός, προϋπόθεση και απόρροια της νομιμότητας κάθε επεξεργασίας είναι η ενδελεχής προστασία των δικαιωμάτων των υποκειμένων των δεδομένων.

Αναδεικνύονται ο εξαιρετικά σημαντικός ρόλος και η ευθύνη του υπεύθυνου επεξεργασίας[10] στον ΓΚΠΔ, ο οποίος οφείλει να τηρεί την αρχή της νομιμότητας πριν, κατά τη διάρκεια και μετά την επεξεργασία των δεδομένων και να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας τους. Περαιτέρω, ο υπεύθυνος επεξεργασίας φέρει το βάρος της αποδείξεως της νομιμότητας της επεξεργασίας των δεδομένων, την οποία οφείλει να είναι σε θέση να αποδεικνύει ανά πάσα στιγμή, σύμφωνα με τη θεμελιώδη αρχή της λογοδοσίας.

Διαφαίνεται η σημασία της θεμελιώδους αρχής της λογοδοσίας του υπεύθυνου επεξεργασίας στον ΓΚΠΔ[11], στην οποία ερείδονται όλες οι διατάξεις που αφορούν στην ευθύνη του να προβαίνει στις απαραίτητες ενέργειες και να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα, τόσο για να προλαμβάνει όσο και για να αντιμετωπίζει τυχόν παραβίαση δεδομένων προσωπικού χαρακτήρα. Η αρχή της λογοδοσίας λειτουργεί σαν «μηχανισμός εγγύησης» της τήρησης των αρχών που πρέπει να διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Επίσης, μέσω της θε-

[7] ΑΠΔΠΧ 35/2023, 4/2023, 36/2022 και 6/2022.
[8] 16/2024, 60/2022, 36/2022, 23/2022, 27/2022 και 4/2022.
[9] ΑΠΔΠΧ 50/2021· ΑΠΔΠΧ 61/2022.
[10] Σ. Παπακωνσταντίνου, *ΑΠΔΠΧ 30/2023. Επιβολή προστίμου 50.000 ευρώ στον ΟΑΣΑ για παράνομη επεξεργασία δεδομένων στο πλαίσιο του ηλεκτρονικού εισιτηρίου,* e-ΠΟΛΙΤΕΙΑ 9/2024, σελ. 171.
[11] Ibidem, σελ. 171.

σμοθέτησης της αρχής αυτής, αναδεικνύεται η επιλογή του Ευρωπαίου νομοθέτη για μετακύλιση της ευθύνης της εφαρμογής του ΓΚΠΔ από τις εποπτικές αρχές στους υπεύθυνους επεξεργασίας, ώστε η προστασία δεδομένων *«να γίνει κτήμα καθενός που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα*[12]».

Συνεπώς, κρίνεται απαραίτητο, οι επιχειρήσεις να υποστηρίζουν ουσιαστικά και πρακτικά τη λήψη τέτοιων μέτρων και ενεργειών, τόσο προληπτικών, όσο και αμυντικών. Έτσι, θα πρέπει να επιδιώκουν να επενδύουν στη «θωράκιση» της ασφάλειας των δεδομένων προσωπικού χαρακτήρα και κατ' επέκταση στην προστασία των υποκειμένων των δεδομένων.

Τέλος, φαίνεται πως μέσω των σχετικών με την ασφάλεια των δεδομένων διατάξεών του (λήψη τεχνικών και οργανωτικών μέτρων, μελέτη εκτίμησης αντικτύπου, τήρηση αρχείου δραστηριοτήτων, αρχή της λογοδοσίας κ.λπ.), ο ΓΚΠΔ εισάγει ένα καθεστώς *«οιονεί αυτορρυθμίσεως*[13]», με το οποίο *μετακυλίεται* το βάρος λήψης αποφάσεων από τις εποπτικές αρχές στους υπεύθυνους επεξεργασίας.

Έτσι, αναδεικνύεται η «εργονομία»[14] του εργαλείου του ΓΚΠΔ, ο οποίος έχει διαμορφωθεί και έχει συνταχθεί με τέτοιο τρόπο ώστε τα υποκείμενα των δεδομένων να μπορούν να αισθάνονται ασφαλή, χάρη στις θεμελιώδεις αρχές και στα δικαιώματα που τα προστατεύουν, τόσο προληπτικά, όσο και αμυντικά.

VI. ΕΠΙΛΟΓΟΣ

Στην κριθείσα υπόθεση, το σύστημα ασφαλείας που εφάρμοζαν τα ΕΛΤΑ στάθηκε ανεπαρκές, τόσο κατά τη διάρκεια της κυβερνοεπίθεσης, όσο και κατόπιν αυτής. Επιπλέον, οι οικονομικές δυσκολίες που αντιμετώπιζαν φαίνεται πως είχαν άμεσο αντίκτυπο στην ασφάλεια των δεδομένων προσωπικού χαρακτήρα, καθώς δεν χρηματοδοτούνταν επαρκώς ενέργειες ενίσχυσης των τεχνικών και οργανωτικών μέτρων ασφαλείας. Έτσι, φαίνεται πως υπάρχει άμεση σύνδεση μεταξύ των περιορισμένων οικονομικών και της μη επάρκειας των εφαρμοζόμενων μέτρων ασφαλείας από τα ΕΛΤΑ. Συνεπώς, κρίνεται απαραίτητο να ενισχύονται οικονομικά οι ενέργειες διασφάλισης της ακεραιότητας και της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα, πόσω μάλλον δε όταν διακυβεύονται και κινδυνεύουν η ασφάλεια, η μυστικότητα και η ακεραιότητα των δεδομένων εκατομμυρίων προσώπων και ο υπεύθυνος επεξεργασίας είναι εταιρεία «κοινής ωφέλειας».

Συνοψίζοντας, θα πρέπει γενικότερα οι υπεύθυνοι επεξεργασίας να λαμβάνουν κάθε εύλογο και δυνατό μέτρο, ώστε να προστατεύονται πάση θυσία τα δικαιώματα των υποκειμένων των δεδομένων που υφίστανται επεξεργασία. Σε αυτό στοχεύει άλλωστε –μέσω της επικείμενης συμμόρφωσης– το πρόστιμο που επεβλήθη από την Αρχή.

Τέλος, η Απόφαση 10/2024 της Αρχής αναδεικνύει, συν τοις άλλοις, την αναγκαιότητα ορθής

---

[12] Ι. Ιγγλεζάκη, *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων*, 3η έκδ., 2020, σελ. 77.

[13] Φ. Παναγοπούλου-Κουτνατζή, *Συνταγματικές προεκτάσεις των μηχανισμών διευρύνσεως της προστασίας δεδομένων προσωπικού χαρακτήρα πέραν της Ε.Ε.: Εξωεδαφική εφαρμογή του ΓΚΠΔ και διασυνοριακή διαβίβαση δεδομένων*, ΔiΜΕΕ 4/2019, σελ. 518.

[14] Σ. Παπακωνσταντίνου, *ΑΠΔΠΧ 35/2022. Επιβολή προστίμου 20.000.000 ευρώ στην εταιρία Clearview AI, Inc. για παράβαση των αρχών της νομιμότητας και της διαφάνειας*, e-ΠΟΛΙΤΕΙΑ 6/2023, σελ. 278.

εφαρμογής του Κανονισμού, ο οποίος παρά τις όποιες εγγενείς αδυναμίες του αποτελεί αδιαμφισβήτητα ένα πολύ σημαντικό θεσμικό εργαλείο που ως στόχο του έχει τη διαφύλαξη και την εξασφάλιση των θεμελιωδών δικαιωμάτων του ανθρώπου, που ως εγγυητικοί πυλώνες υποστηρίζουν την κοινωνική ευημερία και την προόδου και τη διάρκεια αυτών των αξιών στο μέλλον. ❑