ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Αθήνα, 5 Ιουλίου 2024

Αριθμ. Πρωτ. 1828

ΑΠΟΦΑΣΗ 18/2024

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνήλθε μετά από πρόσκληση του Προέδρου της μέσω διάσκεψης, την 23/01/2024, εξ αναβολής των από 05/12/2023 και 19/12/2023 συνεδριάσεων, προκειμένου να εξετάσει την υπόθεση, που αναφέρεται κατωτέρω στο ιστορικό της παρούσας απόφασης. Παρέστησαν ο Πρόεδρος της Αρχής, Κωνσταντίνος Μενουδάκος και τα τακτικά μέλη της Αρχής Κωνσταντίνος Λαμπρινουδάκης ως εισηγητής, Σπυρίδων Βλαχόπουλος, Χαράλαμπος Ανθόπουλος, Χρήστος Καλλονιάτης, Αικατερίνη Ηλιάδου και Γρηγόριος Τσόλιας. Παρόντες χωρίς δικαίωμα ψήφου ήταν ο Κωνσταντίνος Λιμνιώτης και η Αικατερίνη Χατζηδιάκου, πληροφορικοί ελεγκτές, ως βοηθοί εισηγητή και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα κάτωθι:

Με την υπ' αριθ. πρωτ. Γ/ΕΙΣ/4615/20-06-2023 καταγγελία, ο Α (εφεξής «καταγγέλλων») κατήγγειλε στην Αρχή περιστατικό παραβίασης δεδομένων που αφορά στην μη εξουσιοδοτημένη πρόσβαση από χρήστες του διαδικτύου σε ευχερώς προσπελάσιμα αρχεία με προσωπικά δεδομένα πολιτών του Δήμου Αλίμου. Συγκεκριμένα, σύμφωνα με την καταγγελία, αρχεία με προσωπικά δεδομένα πολιτών του Δήμου Αλίμου ήταν ευχερώς προσπελάσιμα από οποιονδήποτε χρήστη μέσω του ιστότοπου «…», με αλλαγή του τελευταίου πενταψήφιου αριθμού που εμφανίζεται στη σχετική ηλεκτρονική (URL) διεύθυνση. Η Αρχή διαπίστωσε ότι η ανωτέρω καταγγελία είναι βάσιμη και προς επιβεβαίωση ελεγκτές της Αρχής, στο πλαίσιο διερεύνησης της καταγγελίας, «κατέβασαν» ένα μεγάλο αριθμό αρχείων με προσωπικά δεδομένα πολιτών του Δήμου Αλίμου από τον

ανωτέρω σύνδεσμο.

Η Αρχή ενημέρωσε στις 21-06-2023 μέσω ηλεκτρονικού ταχυδρομείου τον Δήμο Αλίμου (εφεξής «υπεύθυνος επεξεργασίας») για το ως άνω περιστατικό παραβίασης και στη συνέχεια ο υπεύθυνος επεξεργασίας υπέβαλε στην Αρχή, με βάση τον Κανονισμό (ΕΕ) 2016/679 (Γενικός Κανονισμός Προστασίας Δεδομένων – εφεξής ΓΚΠΔ), την υπ' αριθ. πρωτ. Γ/ΕΙΣ/4715/23-06-2023 γνωστοποίηση περιστατικού παραβίασης και την υπ' αριθ. πρωτ. Γ/ΕΙΣ/4749/26-06-2023 απάντησή του επί του περιστατικού.

Η Αρχή, αφού εξέτασε την ανωτέρω σχετική γνωστοποίηση και το σχετικό απαντητικό έγγραφο, απέστειλε το υπ' αριθ. πρωτ. Γ/ΕΞΕ/1649/27-06-2023 έγγραφο στον υπεύθυνο επεξεργασίας, ζητώντας αναλυτικότερη περιγραφή του περιστατικού παραβίασης με κάθε σχετική πληροφορία που αφορά στις ενέργειες στις οποίες προέβη από τη στιγμή της γνωστοποίησης και εφεξής, τα μέτρα ασφαλείας, την τυχόν κοινοποίηση του περιστατικού στα επηρεαζόμενα υποκείμενα των δεδομένων, το χρονικό διάστημα για το οποίο υπήρχε αυτή η ευπάθεια στο σύστημα, καθώς επίσης και την αξιολόγηση των κινδύνων από την πλευρά του υπευθύνου επεξεργασίας. Με το ανωτέρω έγγραφο η Αρχή ζήτησε από τον υπεύθυνο επεξεργασίας, όπως αποστείλει την πλήρη σύμβαση με την εταιρεία «ΤΕΣΤ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ Ο.Ε.» (εφεξής «εκτελών την επεξεργασία») με την οποία ο υπεύθυνος επεξεργασίας είχε συμβληθεί για την υλοποίηση και υποστήριξη των σχετικών διαδικτυακών υπηρεσιών.

Στις 03-07-2023, και ενώ ο υπεύθυνος επεξεργασίας είχε ήδη ενημερώσει την Αρχή ότι είχε προβεί σε διορθωτικές ενέργειες και επομένως τα αρχεία του υπεύθυνου επεξεργασίας δεν ήταν πλέον ευχερώς προσπελάσιμα από μη εξουσιοδοτημένους χρήστες (κάτι το οποίο εξάλλου είχε διαπιστώσει και η Αρχή), ο καταγγέλλων ενημέρωσε την Αρχή, με το υπ' αριθ. πρωτ. Γ/ΕΙΣ/4916/03-07-2023 έγγραφο, ότι η ευπάθεια συνέχιζε να υφίσταται και ουσιαστικά επανεμφανίστηκε το ίδιο πρόβλημα, παρόλο που αρχικώς φαινόταν ότι είχε αντιμετωπιστεί. Λόγω αυτού, η Αρχή επικοινώνησε αμέσως, μέσω τηλεφώνου, με τον υπεύθυνο επεξεργασίας, τον οποίο και ενημέρωσε σχετικά ώστε να προβεί σε άμεσες ενέργειες για την αντιμετώπιση του περιστατικού παραβίασης (όπως και έγινε, αφού κατέστησαν αμέσως ανενεργές οι σχετικές διαδικτυακές ιστοσελίδες από τις οποίες ήταν εφικτή η μη εξουσιοδοτημένη πρόσβαση στα δεδομένα).

Ακολούθως, ο υπεύθυνος επεξεργασίας απάντησε με το υπ' αρ πρωτ. Γ/ΕΙΣ/5144/12-

07-2023 έγγραφο στο οποίο περιλαμβάνονται τα ακόλουθα:

- Η εφαρμογή στην οποία εντοπίστηκε η ευπάθεια στεγάζεται στην ηλεκτρονική διεύθυνση (url) «…», ενώ η πρόσβαση στα αρχεία δημοτών του Δήμου Αλίμου γίνεται μέσω της ηλεκτρονικής διεύθυνσης (url) «…». Λόγω αναβάθμισης της εφαρμογής σε νέα έκδοση του λογισμικού, το οποίο είχε τεθεί σε δοκιμαστική λειτουργία στο παραγωγικό περιβάλλον, δημιουργήθηκε κενό ασφαλείας το οποίο αποτέλεσε την αιτία του εν λόγω περιστατικού.
- Όπως φαίνεται και από το αρχείο καταγραφής των προσβάσεων σε αρχεία του Δήμου Αλίμου («…»), διαπιστώθηκε αυξημένη πρόσβαση στα αρχεία του Δήμου Αλίμου από δυο συγκεκριμένες IP διευθύνσεις[1] οπότε και έκλεισε η εφαρμογή.
- Μέσω ελέγχου στο ανωτέρω αρχείο καταγραφής, διαπιστώθηκε ότι αποκτήθηκε πρόσβαση σε 1200 αρχεία από τα συνολικά 45000 που είναι διαθέσιμα στην εφαρμογή.
- Πραγματοποιήθηκαν συνολικά περίπου 3800 προσπάθειες μη εξουσιοδοτημένης πρόσβασης, οι περισσότερες των οποίων υπήρξαν αποτυχημένες ή αφορούσαν το ίδιο αρχείο.
- Η ευπάθεια υπήρχε για το διάστημα από τις 12-06-2023 οπότε και ετέθη σε εφαρμογή η δοκιμαστική λειτουργία της νέας έκδοσης της εφαρμογής μέχρι και τις 21-06-2023, ημέρα της γνωστοποίησης του περιστατικού παραβίασης δεδομένων.
- Μετά από διάφορες τεχνικές υλοποιήσεις ώστε η εφαρμογή να είναι λειτουργική και ασφαλής, ο υπεύθυνος επεξεργασίας τελικά κατέληξε στη χρήση tokens. Μέσω αυτής της διαδικασίας ένας χρήστης για να μπορέσει να έχει πρόσβαση ή / και να «κατεβάσει» ένα αρχείο θα πρέπει είτε να είναι δικό του και επομένως να το έχει ανεβάσει ο ίδιος στην εφαρμογή, είτε να είναι χρήστης της εφαρμογής από την πλευρά του Δήμου Αλίμου. Μέσω του token που ελέγχεται από την εφαρμογή, γίνεται ταυτοποίηση του χρήστη και έλεγχος των ρόλων που του έχουν ανατεθεί.

[1] Η μία εκ των δυο IP διευθύνσεων που φαίνεται να απέκτησαν εκτεταμένη μη εξουσιοδοτημένη πρόσβαση στα αρχεία των δημοτών του Δήμου Αλίμου αντιστοιχεί σε υπολογιστή που χρησιμοποιήθηκε από ελεγκτή της Αρχής στα πλαίσια διερεύνησης της ανωτέρω καταγγελίας

- Δεν προέβη σε κοινοποίηση του περιστατικού παραβίασης δεδομένων στα επηρεαζόμενα πρόσωπα, λαμβάνοντας υπόψη τα παρακάτω κριτήρια:
    - Η εφαρμογή βρισκόταν σε δοκιμαστική λειτουργία μετά την αναβάθμιση.
    - Το χρονικό διάστημα που εντοπίστηκε η ευπάθεια ήταν μικρό.
    - Ο αριθμός των αρχείων που επηρεάστηκαν ήταν μικρός.
    - Τα δεδομένα των αρχείων που φιλοξενούνται στη συγκεκριμένη εφαρμογή θεωρούνται απλής φύσεως.
    - Έγινε λήψη άμεσων διορθωτικών μέτρων.
    - Οι κίνδυνοι που προκύπτουν από το συγκεκριμένο περιστατικό παραβίασης χαρακτηρίζονται ως μικροί.

Επίσης, ο υπεύθυνος επεξεργασίας υπέβαλε σύμβαση μεταξύ αυτού και του εκτελούντος την επεξεργασία, στο άρθρο 11 της οποίας γίνεται αναφορά στις υποχρεώσεις των συμβαλλόμενων μερών προκειμένου να τηρούν την ισχύουσα νομοθεσία και σχετικές αποφάσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα σε σχέση με την προστασία προσωπικών δεδομένων, ενώ στο άρθρο 5 αυτής αναφέρεται ότι ο εκτελών την επεξεργασία λαμβάνει τα κατάλληλα μέτρα για να διαφυλάξει την εμπιστευτικότητα των πληροφοριών που έχουν χαρακτηρισθεί ως τέτοιες.

Στη συνέχεια, η Αρχή, αφού εξέτασε την ανωτέρω απάντηση, ζήτησε με το υπ' αριθ. πρωτ. Γ/ΕΞΕ/1783/13-07-2023 έγγραφο επιπλέον διευκρινίσεις και αναλυτικότερη περιγραφή σχετικά με το κενό ασφαλείας που δημιουργήθηκε, τον τρόπο με τον οποίο προέκυψε το ανωτέρω περιστατικό ασφαλείας, τον τρόπο παρακολούθησης της νεότερης έκδοσης της εφαρμογής κατά την επίμαχη δοκιμαστική περίοδο, την πολιτική, η οποία ακολουθείται εν γένει για την διασφάλιση των αλλαγών που συμβαίνουν στα πληροφοριακά συστήματα, τον λόγο επαναλειτουργίας της εφαρμογής (την οποία υπέδειξε με το δεύτερο έγγραφό του ο καταγγέλλων) χωρίς να έχουν ληφθεί τα αναγκαία μέτρα για την προστασία των προσωπικών δεδομένων, καθώς και περιγραφή του τρόπου διερεύνησης του εν λόγω περιστατικού παραβίασης. Επιπλέον, η Αρχή με το ως άνω έγγραφο ζήτησε διευκρινίσεις σχετικά με το ζήτημα των προσβάσεων που χαρακτηρίστηκαν ως μη εξουσιοδοτημένες, αν η διακοπή της χρήσης της εφαρμογής εγείρει ζητήματα διαθεσιμότητας των αρχείων και σχετικών υπηρεσιών στους πολίτες και, τέλος, αν και πώς επηρεάζονται τα υποκείμενα των

δεδομένων από το εν λόγω περιστατικό παραβίασης και επομένως αν πρέπει να ενημερωθούν.

Επιπροσθέτως, η Αρχή με το υπ' αριθ. πρωτ. Γ/ΕΞΕ/1785/13-07-2023 έγγραφο, ζήτησε διευκρινίσεις από τον εκτελούντα την επεξεργασία σχετικά με την πολιτική που ακολουθείται σε περιπτώσεις αναβάθμισης υπάρχοντος λογισμικού, σε τι περιβάλλον λαμβάνουν χώρα οι αλλαγές, αν το συγκεκριμένο κενό ασφαλείας επηρεάζει και άλλους υπεύθυνους επεξεργασίας στους οποίους ο εκτελών προσφέρει παρόμοιες υπηρεσίες και ποιες είναι οι ενέργειές του σε περίπτωση καταφατικής απάντησης.

Εν συνεχεία, με το υπ' αριθ. πρωτ. Γ/ΕΙΣ/5330/19-07-2023 έγγραφό του, ο καταγγέλλων ενημέρωσε εκ νέου την Αρχή ότι τα αρχεία του Δήμου Αλίμου ήταν και πάλι ευχερώς προσπελάσιμα από μη εξουσιοδοτημένους χρήστες κατά τον ίδιο ακριβώς τρόπο (όπως και διαπίστωσε και η Αρχή). Κατόπιν αυτού, η Αρχή εξέδωσε την υπ' αρ. Απόφαση 28/2023 (Μονοπρόσωπο Όργανο) κατά την οποία επέβαλε με προσωρινή διαταγή όπως ο υπεύθυνος επεξεργασίας προβεί σε κάθε αναγκαία ενέργεια ώστε να περιοριστεί η ελεύθερη πρόσβαση χρηστών του διαδικτύου σε αρχεία της εφαρμογής του υπεύθυνου επεξεργασίας και τα αρχεία με προσωπικά δεδομένα χρηστών της εφαρμογής να είναι διαθέσιμα μόνο σε κατάλληλα εξουσιοδοτημένους χρήστες ή και τα υποκείμενα των δεδομένων χωρίς να είναι ευχερώς προσπελάσιμα από άλλους μη εξουσιοδοτημένους χρήστες. Όπως διαπιστώθηκε από την Αρχή, μετά τη λήψη της προσωρινής διαταγής ο υπεύθυνος επεξεργασίας απενεργοποίησε τη δυνατότητα αθέμιτης πρόσβασης στα προσωπικά δεδομένα (οι σχετικές ιστοσελίδες απενεργοποιήθηκαν).

Ακολούθως, ο υπεύθυνος επεξεργασίας, απάντησε με το υπ' αριθ. πρωτ. Γ/ΕΙΣ/5840/10-08-2023 έγγραφο σε ορισμένες από τις διευκρινίσεις που ζήτησε η Αρχή με το ανωτέρω έγγραφό της ως εξής:

- Το κενό ασφαλείας δημιουργήθηκε από ενεργοποίηση της λανθασμένης έκδοσης της εφαρμογής, το οποίο οφείλεται στις εσωτερικές διαδικασίες παραμετροποίησης (configuration management) του εκτελούντος την επεξεργασία. Συγκεκριμένα είχε διατηρηθεί ο κώδικας της προηγούμενης έκδοσης με στοιχεία του νεότερου λογισμικού που αναπτύχθηκε.
- Η διακοπή της λειτουργίας της εφαρμογής επηρέασε μόνο τις ηλεκτρονικές υπηρεσίες και όχι και την έκδοση των αρχείων που φιλοξενεί η εφαρμογή μέσω αιτήσεων με φυσική παρουσία των δημοτών.

- Σε σχέση με τις υπόλοιπες διευκρινίσεις ο υπεύθυνος επεξεργασίας ανέμενε συνδρομή από τον εκτελούντα την επεξεργασία.

Ακολούθως, μετά και την πάροδο διαστήματος πλέον του μηνός, κατά το οποίο δεν υπήρξε άλλη απάντηση στην Αρχή, η Αρχή απέστειλε τα υπ' αριθ. πρωτ. Γ/ΕΞΕ/2378/21-09-2023 και υπ' αριθ. πρωτ. Γ/ΕΞΕ/2379/21-09-2023 έγγραφα προς υπόμνηση του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία, αντίστοιχα. Κατόπιν αυτών, ο εκτελών την επεξεργασία απάντησε με το υπ' αριθ. πρωτ. Γ/ΕΙΣ/6731/25-09-2023 έγγραφο, στο οποίο αναφέρονται τα εξής:

- Δεν υπάρχει κάποια καταγεγραμμένη πολιτική διαχείρισης αλλαγών για τα λογισμικά που έχει αναπτύξει η εταιρεία.
- Σε περιπτώσεις αλλαγών ακολουθούνται άτυπα τα παρακάτω βήματα:
    - Ενημέρωση του πελάτη για τη διακοπή της λειτουργίας της εφαρμογής (συνήθως σε μη παραγωγικές ώρες)
    - Διακοπή λειτουργίας της εφαρμογής
    - Εγκατάσταση νέα έκδοσης εφαρμογής
    - Λειτουργία νέας εφαρμογής
    - Έλεγχος ορθής λειτουργίας
- Δοκιμές των αλλαγών συνήθως πραγματοποιούνται σε εσωτερικούς διακομιστές, ενώ σε περιπτώσεις πιο σύνθετες που σχετίζονται με ζητήματα ασφαλείας αυτές γίνονται απευθείας σε παραγωγικό περιβάλλον.
- Οι περισσότερες εφαρμογές που έχει αναπτύξει η εταιρεία είναι μεταγενέστερες και ασφαλέστερες της εφαρμογής που χρησιμοποιεί ο υπεύθυνος επεξεργασίας για την αίτηση και έκδοση ψηφιακών πιστοποιητικών. Η συγκεκριμένη εφαρμογή λειτουργεί επιπλέον στο Δήμο Κερατσινίου και στο Δήμο Βούλας – Βάρης – Βουλιαγμένης. Η αναβάθμιση του λογισμικού δεν φαίνεται να έχει επηρεάσει αυτούς τους υπεύθυνους επεξεργασίας. Πέραν τούτου ο χώρος αποθήκευσης των αρχείων και οι ρυθμίσεις της εφαρμογής είναι διαφορετικά σε κάθε περίπτωση. Ο εκτελών την επεξεργασία συνεχίζει να πραγματοποιεί δοκιμές ώστε να διασφαλιστεί ότι οι ανωτέρω Δήμοι δεν έχουν επηρεαστεί.

Τέλος, ο υπεύθυνος επεξεργασίας απάντησε με το υπ' αριθ. πρωτ. Γ/ΕΙΣ/6875/02-10-2023 έγγραφο με το οποίο παρείχε επιπλέον διευκρινίσεις, σχετικά με τον όγκο των

αρχείων στα οποία αποκτήθηκε μη εξουσιοδοτημένη πρόσβαση και από ποιες διαδικτυακές διευθύνσεις έγινε αυτό. Επίσης ο υπεύθυνος επεξεργασίας επαναλαμβάνει ότι η σχετική λειτουργικότητα, η οποία τελικά επέτρεπε τη μη εξουσιοδοτημένη πρόσβαση σε δεδομένα, ενεργοποιήθηκε για τη διενέργεια δοκιμών που έγιναν στο πλαίσιο αναβάθμισης της εφαρμογής, ενώ επίσης επισημαίνει ότι όποιος χρήστης κοιτούσε τον πηγαίο κώδικα της ιστοσελίδας της εφαρμογής θα μπορούσε να υποθέσει τον τρόπο με τον οποίο θα αποκτούσε μη εξουσιοδοτημένη πρόσβαση στα δεδομένα. Επιπλέον, διαπιστώθηκε ότι τελικά από το περιστατικό παραβίασης εκτέθηκαν αρχεία του υπεύθυνου επεξεργασίας, όπως αστυνομικά δελτία ταυτότητας τα οποία μπορούν να χρησιμοποιηθούν εύκολα σε περιστατικά υποκλοπής ταυτότητας σε επιγραμμικά περιβάλλοντα. Τέλος, ο υπεύθυνος επεξεργασίας επαναλαμβάνει τους ισχυρισμούς που είχε διατυπώσει στο υπ' αριθ. πρωτ. Γ/ΕΙΣ/5144/12-07-2023 έγγραφό του αναφορικά με την τεχνική λύση που υιοθετήθηκε για την αντιμετώπιση της επίμαχης ευπάθειας, καθώς επίσης και ότι παρά τις συνεχείς οχλήσεις προς τον εκτελούντα την επεξεργασία δεν είχαν ληφθεί ακόμα όλες οι διευκρινίσεις για το εν λόγω περιστατικό έως τη στιγμή αποστολής του ανωτέρου εγγράφου.

Επισημαίνεται επίσης ότι όλες οι απαντήσεις του υπεύθυνου επεξεργασίας προς την Αρχή, όπως περιγράφονται ανωτέρω, υποβλήθηκαν από τον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ) του Δήμου. Στο τελευταίο δε έγγραφο, αναφέρεται επίσης ότι ο ΥΠΔ συνέστησε στον υπεύθυνο επεξεργασίας να ανακοινώσει το εν λόγω περιστατικό στα υποκείμενα των δεδομένων.

Κατόπιν της εξέτασης των στοιχείων του φακέλου, η Αρχή απέστειλε τις υπ' αριθ. πρωτ. Γ/ΕΞΕ/2554/12-10-2023 και Γ/ΕΞΕ/2553/12-10-2023 κλήσεις προς τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία αντίστοιχα προκειμένου να συζητηθεί η εν λόγω υπόθεση ενώπιον της Ολομέλειας της Αρχής την Τρίτη 24 Οκτωβρίου 2023. Στην εν λόγω συνεδρίαση, η οποία πραγματοποιήθηκε μέσω τηλεδιάσκεψης, ήταν παρόντες εκ μέρους του υπεύθυνου επεξεργασίας, οι Β, Γενικός Γραμματέας του Δήμου, η Μαρία Μαριόλη, δικηγόρος με ΑΜΔΣΑ …, Σύμβουλος Δημάρχου, εκ μέρους της εταιρείας KaPa Data Consulting που εκτελεί καθήκοντα ΥΠΔ του υπεύθυνου επεξεργασίας, η Κωνσταντίνα Ιθακησίου, δικηγόρος, με ΑΜΔΣΑ …, και ο Γ, εξωτερικός συνεργάτης της εταιρείας, και εκ μέρους του εκτελούντα την επεξεργασία οι νόμιμοι εκπρόσωποι της εταιρείας Δ και Ε προκειμένου να παράσχουν διευκρινίσεις επί της εν

λόγω υπόθεσης. Μετά τη συνεδρίαση ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία έλαβαν προθεσμία για υποβολή υπομνήματος. Ακολούθως, ο υπεύθυνος επεξεργασίας υπέβαλε, εντός της ταχθείσας προθεσμίας, το υπ' αριθ. πρωτ. Γ/ΕΙΣ/7936/07-11-2023 υπόμνημα, μετά των συμπληρωματικών υπ' αριθ. πρωτ. Γ/ΕΙΣ/7983/09-11-2023 και Γ/ΕΙΣ/8105/14-11-2023 εγγράφων. Με το υπόμνημά του, ο υπεύθυνος επεξεργασίας επανέλαβε κατ' ουσίαν τους ισχυρισμούς που έθεσε και προηγουμένως ενώπιον της Αρχής. Συγκεκριμένα στο υπόμνημα αναφέρεται ότι έχει συναφθεί, από 12-09-2022, σύμβαση μεταξύ του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία με σκοπό την συντήρηση της διαδικτυακής ψηφιακής πλατφόρμας που αφορά στη διαχείριση των ψηφιακών πιστοποιητικών για τους πολίτες και τις επιχειρήσεις του υπεύθυνου επεξεργασίας, λαμβάνοντας μεταξύ άλλων κατάλληλα τεχνικά μέτρα για την διαφύλαξη της εμπιστευτικότητας των πληροφοριών. Αναφέρεται επιπλέον ότι με τη διαπίστωση της μη εξουσιοδοτημένης πρόσβασης στα αρχεία του υπεύθυνου επεξεργασίας, ξεκίνησε αμέσως η διερεύνηση του περιστατικού. Κατόπιν πλημμελών δοκιμών επαναλειτουργίας της εφαρμογής δόθηκε η εντολή για διακοπή της λειτουργίας της εφαρμογής, η οποία και τελικά επαναλειτούργησε στις 03-11-2023 (ήτοι μετά και την ακρόαση του υπευθύνου επεξεργασίας ενώπιον της Αρχής), αφού ο έλεγχος και οι απαραίτητες διορθώσεις από τη μεριά του εκτελούντος την επεξεργασία είχαν ολοκληρωθεί. Επιπροσθέτως, στο ίδιο υπόμνημα ο υπεύθυνος επεξεργασίας αναφέρει ότι ο εκτελών την επεξεργασία του παρέδωσε τα στοιχεία του ελέγχου που αφορούσαν το σύνολο των υποκειμένων των δεδομένων που είχαν επηρεαστεί από το εν λόγω περιστατικό παραβίασης δεδομένων, με στόχο να ενημερωθούν σε προσωπικό επίπεδο και όχι με γενική ενημέρωση/ανακοίνωση, δίνοντας προτεραιότητα σε υποκείμενα των δεδομένων για τα οποία υπήρξε μη εξουσιοδοτημένη πρόσβαση σε δεδομένα αστυνομικών ταυτοτήτων ή διαβατηρίων. Συγκεκριμένα, ο υπεύθυνος επεξεργασίας απέστειλε μήνυμα ηλεκτρονικού ταχυδρομείου στα θιγόμενα πρόσωπα ενημερώνοντάς τα για το περιστατικό – ενώ το πρότυπο μίας τέτοιας ενημερωτικής επιστολής υποβλήθηκε ακολούθως στην Αρχή με το υπ' αριθ. πρωτ. Γ/ΕΙΣ/7983/09-11-2023 έγγραφο. Όπως προκύπτει από το εν λόγω έγγραφο, ο υπεύθυνος επεξεργασίας ενημέρωνε τα υποκείμενα των δεδομένων για περιστατικό κυβερνοεπίθεσης και παραβίασης της ασφάλειας των πληροφοριακών συστημάτων του Δήμου από μη εξουσιοδοτημένους χρήστες κατά τη διάρκεια της οποίας

έγινε προσπάθεια μαζικής άντλησης τυχαίων αρχείων εκ των οποίων υπήρχαν και αρχεία με προσωπικά τους δεδομένα. Στην παραπάνω ενημέρωση περιλαμβάνεται και η πληροφορία ότι ο υπεύθυνος επεξεργασίας έχει προβεί στις απαραίτητες ενέργειες για τη διόρθωση του ως άνω περιστατικού, καθώς επίσης ότι έχει ενημερώσει και την Αρχή. Περαιτέρω, σύμφωνα με το υπ' αριθ. πρωτ. Γ/ΕΙΣ/8105/14-11-2023 έγγραφο, η μη εξουσιοδοτημένη πρόσβαση σε αρχεία αφορούσε σε περίπου εννιακόσια (900) υποκείμενα δεδομένων – χρήστες των υπηρεσιών του υπεύθυνου επεξεργασίας. Από τα ανωτέρω αρχεία, 150 αφορούσαν ταυτότητες ή διαβατήρια 148 συνολικά υποκειμένων, τα οποία ενημερώθηκαν με επιστολή που τους εστάλη μέσω μηνύματος ηλεκτρονικού ταχυδρομείου στις 03-11-2023 από τον υπεύθυνο επεξεργασίας. Τέλος, στο εν λόγω έγγραφο αναφέρεται ότι η διαδικασία ενημέρωσης και των υπόλοιπων επηρεαζόμενων υποκειμένων βρίσκεται σε εξέλιξη.

Ο εκτελών την επεξεργασία δεν υπέβαλε ιδιαίτερο υπόμνημα μετά την ακρόασή του. Σημειώνεται ωστόσο ότι στο ανωτέρω υπ' αριθ. πρωτ. Γ/ΕΙΣ/7936/07-11-2023 υπόμνημα του υπευθύνου επεξεργασίας, περιγράφονται οι αλλαγές στο λογισμικό που έλαβαν χώρα από τον εκτελούντα την επεξεργασία στην πλατφόρμα για την διασφάλιση και διαφύλαξη των δεδομένων ώστε να μην είναι εφικτό να «κατεβάσει» ένας χρήστης αρχεία έτερου προσώπου.

Η Αρχή, έπειτα από εξέταση των στοιχείων του φακέλου και όσων προέκυψαν από την ενώπιόν της ακροαματική διαδικασία και το υπόμνημα του υπεύθυνου επεξεργασίας, με τα συμπληρωματικά έγγραφα αυτού, 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, ***«παραβίαση δεδομένων***

προσωπικού χαρακτήρα*: 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 5 παρ. 1 περ. στ' 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»).»*
4. Σύμφωνα με τους ορισμούς του άρθρου 24 του ΓΚΠΔ: «1. *Λαμβάνοντας υπόψη 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 εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό. Τα εν λόγω μέτρα επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο. 2. Όταν δικαιολογείται σε σχέση με τις δραστηριότητες επεξεργασίας, τα μέτρα που αναφέρονται στην παράγραφο 1 περιλαμβάνουν την εφαρμογή κατάλληλων πολιτικών για την προστασία των δεδομένων από τον υπεύθυνο επεξεργασίας.»*
5. 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.

6. Σύμφωνα με τους ορισμούς του άρθρου 28 του ΓΚΠΔ: *«1. Όταν η επεξεργασία πρόκειται να διενεργηθεί για λογαριασμό υπευθύνου επεξεργασίας, ο υπεύθυνος επεξεργασίας χρησιμοποιεί μόνο εκτελούντες την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του παρόντος κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων. 2. (…) 3. Η επεξεργασία από τον εκτελούντα την επεξεργασία διέπεται από σύμβαση ή άλλη νομική πράξη υπαγόμενη στο δίκαιο της Ένωσης ή του κράτους μέλους, που δεσμεύει τον εκτελούντα την επεξεργασία σε σχέση με τον υπεύθυνο επεξεργασίας και καθορίζει το αντικείμενο και τη διάρκεια της επεξεργασίας, τη φύση και τον σκοπό της επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα και τις κατηγορίες των υποκειμένων των δεδομένων και τις υποχρεώσεις και τα δικαιώματα του υπευθύνου επεξεργασίας. Η εν λόγω σύμβαση ή άλλη νομική πράξη προβλέπει ειδικότερα ότι ο εκτελών την επεξεργασία: (…) γ) λαμβάνει όλα τα απαιτούμενα μέτρα δυνάμει του άρθρου 32 (…) στ) συνδράμει τον υπεύθυνο επεξεργασίας στη διασφάλιση της συμμόρφωσης προς τις υποχρεώσεις που απορρέουν από τα άρθρα 32 έως 36, λαμβάνοντας υπόψη τη φύση της επεξεργασίας και τις πληροφορίες που διαθέτει ο εκτελών την επεξεργασία (…), η) θέτει στη διάθεση του υπευθύνου επεξεργασίας κάθε απαραίτητη πληροφορία προς απόδειξη της συμμόρφωσης προς τις υποχρεώσεις που θεσπίζονται στο παρόν άρθρο και επιτρέπει και διευκολύνει τους ελέγχους, περιλαμβανομένων των επιθεωρήσεων, που διενεργούνται από τον υπεύθυνο επεξεργασίας ή από άλλον ελεγκτή εντεταλμένο από τον υπεύθυνο επεξεργασίας.*
7. Σύμφωνα με τους ορισμούς του άρθρου 31 του ΓΚΠΔ: «*Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία και, κατά περίπτωση, οι εκπρόσωποί τους συνεργάζονται, κατόπιν αιτήματος, με την εποπτική αρχή για την άσκηση των καθηκόντων της.»*
8. Σύμφωνα με τους ορισμούς του άρθρου 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. 3. (…) 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.»

9. Σύμφωνα με τους ορισμούς του άρθρου 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. 2. Ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας αμελλητί, μόλις αντιληφθεί παραβίαση*

δεδομένων προσωπικού χαρακτήρα. 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.

10. Σύμφωνα με τους ορισμούς του άρθρου 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.»

11. Στην προκειμένη περίπτωση από τα στοιχεία του φακέλου της υπόθεσης προκύπτει ότι για την εν λόγω επεξεργασία δεν λήφθηκαν εξ αρχής από το σχεδιασμό επαρκή μέτρα ασφάλειας σε σχέση με τους αντίστοιχους κινδύνους για τα δικαιώματα και ελευθερίες των φυσικών προσώπων, αλλά ούτε και ήταν σε εφαρμογή διαδικασίες ελέγχου της αποτελεσματικότητας των υφιστάμενων μέτρων ασφάλειας. Συγκεκριμένα:

    - Δεν είχαν τεθεί σε εφαρμογή κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί η εμπιστευτικότητα των προσωπικών δεδομένων τα οποία επηρεάστηκαν με το εν λόγω περιστατικό παραβίασης δεδομένων και τα οποία αφορούν αιτήσεις δημοτών του υπευθύνου επεξεργασίας για διάφορα ζητήματα. Όπως προκύπτει από την περιγραφή του περιστατικού παραβίασης, μη εξουσιοδοτημένοι χρήστες μπορούσαν να αποκτήσουν ή / και απέκτησαν πρόσβαση σε προσωπικά δεδομένα δημοτών του υπεύθυνου επεξεργασίας, στα οποία συμπεριλαμβάνονται, μεταξύ άλλων, αντίγραφα αστυνομικών ταυτοτήτων, υπεύθυνες δηλώσεις φυσικών προσώπων με συμπληρωμένα

όλα τα πεδία με προσωπικά δεδομένα που ζητούνται από έντυπο υπεύθυνης δήλωσης (όπως ονοματεπώνυμα, πατρώνυμα, μητρώνυμα, ημερομηνία γέννησης, ταχυδρομική/ηλεκτρονική διεύθυνση, ΑΦΜ, κτλ.), άδειες οδήγησης κ.α. Όπως επίσης προκύπτει από το ιστορικό της παρούσας, η μη εξουσιοδοτημένη πρόσβαση ήταν αρκετά ευχερής, αφού κάποιος χρήστης με βασικές τεχνικές γνώσεις δημιουργίας ιστοσελίδων θα μπορούσε εύκολα να «αναγνωρίσει» ότι υπάρχει η συγκεκριμένη ευπάθεια.

- Δεν φαίνεται να υπήρχαν επαρκή σημεία ελέγχου, ώστε να ανιχνεύεται έγκαιρα τέτοιου είδους παραβίαση προσωπικών δεδομένων, όπως τακτική παρακολούθηση, αξιολόγηση και εκτίμηση των αρχείων όπου καταγράφονται οι προσβάσεις σε αρχεία με προσωπικά δεδομένα δημοτών της συγκεκριμένης εφαρμογής (logs), προκειμένου να ανιχνευθούν μη «ύποπτες» συμπεριφορές (δηλαδή ενέργειες χρηστών που θα μπορούσαν να ερμηνευθούν ως μη εξουσιοδοτημένες προσβάσεις ή απόπειρες μη εξουσιοδοτημένων προσβάσεων). Αυτό επιβεβαιώνεται και από το γεγονός ότι η παραβίαση προσωπικών δεδομένων δεν έγινε αντιληπτή από τον υπεύθυνο επεξεργασίας, αλλά ούτε και από τον εκτελούντα την επεξεργασία, παρά μόνο όταν ο πρώτος ενημερώθηκε από την Αρχή κατόπιν καταγγελίας. Αυτό μάλιστα συνέβη και στις τρεις (3) διαφορετικές φορές που υπήρξε η σχετική ευπάθεια και, άρα, έλαβε χώρα αντίστοιχο περιστατικό παραβίασης δεδομένων.
- Το ίδιο περιστατικό παραβίασης πραγματοποιήθηκε τρεις (3) φορές, σε κάθε ενεργοποίηση νέας έκδοσης της εφαρμογής. Επομένως δεν υπήρξε αμέσως αποτελεσματική αντιμετώπιση του περιστατικού. Ειδικότερα, η αντιμετώπισή του ήταν προσωρινή, αφού συνίστατο στην πλήρη απενεργοποίηση της σχετικής ιστοσελίδας, γεγονός που δεν επέτρεπε στους δημότες του υπεύθυνου επεξεργασίας να αξιοποιούν την εν λόγω διαδικτυακή υπηρεσία: κάθε νέα ενεργοποίηση όμως της ιστοσελίδας εξακολουθούσε να φέρει την ίδια ευπάθεια – και αυτό συνέβη, όπως προαναφέρθηκε, για άλλες δύο φορές. Περαιτέρω, προκύπτει ότι δεν ήταν σε εφαρμογή αποτελεσματικοί μηχανισμοί διαχείρισης αλλαγών,

ούτε μηχανισμοί αναγνώρισης κενού ασφαλείας που οδηγεί σε περιστατικό παραβίασης δεδομένων.

12. Ο υπεύθυνος επεξεργασίας δεν διαθέτει αποτελεσματικές διαδικασίες για τον έλεγχο και αξιολόγηση του εκτελούντος την επεξεργασία. Κατ' αρχάς, η σύμβαση μεταξύ υπευθύνου και εκτελούντος την επεξεργασία δεν καλύπτει αναλυτικά τις υποχρεώσεις του εκτελούντος την επεξεργασία απέναντι στον υπεύθυνο επεξεργασίας σε σχέση με την πρόσβαση και την επεξεργασία των προσωπικών δεδομένων που διατηρούνται στην εφαρμογή, όπως προδιαγράφονται στο άρθρο 28 του ΓΚΠΔ, αφού στη σύμβαση υπάρχει συναφώς μόνο μία γενική αναφορά στην τήρηση της υφιστάμενης νομοθεσίας, χωρίς να εξειδικεύονται τα στοιχεία που προδιαγράφονται στο άρθρο 28 παρ. 3 του ΓΚΠΔ (βλ. και Σκέψη 6 της παρούσας). Εξάλλου, ο υπεύθυνος επεξεργασίας αναφέρει ότι κατά την αρχική διερεύνηση του περιστατικού ο εκτελών δεν ανταποκρίθηκε πλήρως στα αιτήματά του σχετικά με τη λήψη διευκρινίσεων για το περιστατικό. Περαιτέρω, τα αναλυτικά στοιχεία σχετικά με το περιστατικό φαίνεται ότι δόθηκαν, από τον εκτελούντα προς τον υπεύθυνο επεξεργασίας, τον Οκτώβριο του 2023, ήτοι περίπου τρεις (3) μήνες από την επέλευση του περιστατικού. Σημειώνεται ωστόσο ότι ο υπεύθυνος επεξεργασίας δεν υπέβαλε κάποιο τεκμήριο το οποίο να καταδεικνύει τις ενέργειες στις οποίες προέβη προκειμένου να λάβει όσο γίνεται πιο έγκαιρα τα αναγκαία στοιχεία από τον εκτελούντα την επεξεργασία.

13. Αναφορικά με την ελλιπή εκπλήρωση των όρων του άρθρου 28 παρ. 3 του ΓΚΠΔ ως προς τη σύμβαση μεταξύ υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία, επισημαίνεται ότι, όπως ρητά αναφέρεται και στις Κατευθυντήριες Γραμμές 7/2020[2] του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (εφεξής, ΕΣΠΔ) αναφορικά με τις έννοιες του υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία, «*καθόσον ο Κανονισμός θεσπίζει σαφή υποχρέωση σύναψης γραπτής σύμβασης, εφόσον δεν ισχύει καμία άλλη σχετική νομική πράξη, η έλλειψη σύμβασης συνιστά παράβαση του ΓΚΠΔ. Τόσο ο υπεύθυνος επεξεργασίας όσο και ο εκτελών την επεξεργασία ευθύνονται για τη διασφάλιση της σύναψης σύμβασης ή άλλης νομικής πράξης που διέπει την επεξεργασία. Με την επιφύλαξη των*

[2] Διαθέσιμες στην ιστοσελίδα https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_el

διατάξεων του άρθρου 83 του ΓΚΠΔ, η αρμόδια εποπτική αρχή έχει τη δυνατότητα να επιβάλει διοικητικό πρόστιμο σε βάρος τόσο του υπευθύνου επεξεργασίας όσο και του εκτελούντος την επεξεργασία, λαμβάνοντας υπόψη τις περιστάσεις κάθε συγκεκριμένης περίπτωσης». Συνεπώς, η μη εκπλήρωση των όρων του άρθρου 28 παρ. 3 του ΓΚΠΔ συνιστά παραβίαση τόσο για τον υπεύθυνο επεξεργασίας όσο και για τον εκτελούντα, ενώ δύναται να υπάρξει, κατά την κρίση της Αρχής, επιβολή διοικητικού προστίμου για την εν λόγω παράβαση σε αμφοτέρους.

14. Ο υπεύθυνος επεξεργασίας αξιολόγησε αρχικά ότι δεν απαιτείται η ανακοίνωση του περιστατικού στα υποκείμενα των δεδομένων, σύμφωνα με το άρθρο 34 του ΓΚΠΔ, λαμβάνοντας υπόψη τα παρακάτω κριτήρια:
    - Η εφαρμογή βρισκόταν σε δοκιμαστική λειτουργία μετά την αναβάθμιση
    - Το χρονικό διάστημα που εντοπίστηκε η ευπάθεια ήταν μικρό
    - Ο αριθμός των αρχείων που επηρεάστηκαν ήταν μικρός
    - Τα δεδομένα των αρχείων που φιλοξενούνται στη συγκεκριμένη εφαρμογή θεωρούνται απλής φύσεως
    - Έγινε λήψη άμεσων διορθωτικών μέτρων
    - Οι κίνδυνοι που προκύπτουν από το συγκεκριμένο περιστατικό παραβίασης χαρακτηρίζονται ως μικροί

    Όπως αναφέρεται και παραπάνω στο ιστορικό της παρούσας, ο ΥΠΔ κατόπιν επαναξιολόγησης των κριτηρίων, προέβη τον Ιούλιο του 2023 σε σύσταση προς τον υπεύθυνο επεξεργασίας όπως ενημερώσει τα επηρεαζόμενα υποκείμενα των δεδομένων. Ο υπεύθυνος επεξεργασίας δήλωσε ότι παρέλαβε το σύνολο των λεπτομερών στοιχείων με τα υποκείμενα των δεδομένων που φαίνεται ότι επηρεάστηκαν από το ανωτέρω περιστατικό παραβίασης στις αρχές Οκτωβρίου, οπότε και κινήθηκε η διαδικασία προσωποποιημένης ενημέρωσης των πολιτών, η οποία είναι σε εξέλιξη. Ο ως άνω ισχυρισμός έρχεται καταρχήν σε αντίθεση με την αρχική αξιολόγηση ότι με βάση τα στοιχεία που ο υπεύθυνος επεξεργασίας είχε στη διάθεσή του, τα αρχεία ήταν μικρής σημαντικότητας και επομένως δεν χρειαζόταν ενημέρωση των υποκειμένων, πέρα από το ότι η αρχική αυτή αξιολόγηση δεν ήταν επαρκώς τεκμηριωμένη, αν ληφθούν υπόψη το είδος και το πλήθος των αρχείων με προσωπικά δεδομένα που παραβιάστηκαν. Περαιτέρω, ο

υπεύθυνος επεξεργασίας δεν μνημονεύει κάποια σχετική ενέργειά του κατά το διάστημα Ιουλίου – Οκτωβρίου 2023, δηλαδή από το χρόνο κατά τον οποίο ο ΥΠΔ συνέστησε την κοινοποίηση του περιστατικού στα θιγόμενα πρόσωπα μέχρι τη λήψη των αναλυτικών πληροφοριών τις οποίες του απέστειλε ο εκτελών την επεξεργασία. Με τα δεδομένα αυτά προκύπτει ότι ο υπεύθυνος επεξεργασίας δεν αξιολόγησε έγκαιρα τη σοβαρότητα του περιστατικού ώστε να μεριμνήσει για την αποτελεσματική αντιμετώπισή του, αφού η ορθή αξιολόγηση έγινε τελικώς σχεδόν τρεις (3) μήνες από την επέλευσή του. Εξάλλου, η ενημέρωση που τελικά ο υπεύθυνος επεξεργασίας παρείχε, με καθυστέρηση, στα επηρεαζόμενα πρόσωπα δεν είναι ορθή αφενός διότι αναφέρεται σε κυβερνοεπίθεση, ενώ το περιστατικό δεν σχετίζεται με κυβερνοεπίθεση, με την οποία νοείται οποιαδήποτε κακόβουλη ενέργεια που λαμβάνει μέρος μέσω ηλεκτρονικού υπολογιστή ή δικτύου με σκοπό την τροποποίηση, καταστροφή, κλοπή, υποκλοπή η μη εξουσιοδοτημένη πρόσβαση στις πληροφορίες του κατόχου[3], και αφετέρου διότι δεν παρατίθενται αναλυτικά τα προσωπικά δεδομένα που διέρρευσαν σε άγνωστους τρίτους. Επιπλέον, ο υπεύθυνος επεξεργασίας δεν προέβη στην επικαιροποίηση των στοιχείων της γνωστοποίησης του περιστατικού στην Αρχή, ως όφειλε.

15. Ο εκτελών την επεξεργασία, όπως δήλωσε, δεν διαθέτει επίσημη και καταγεγραμμένη πολιτική διαχείρισης αλλαγών, ώστε να διασφαλίσει ότι οι αλλαγές σε υπάρχουσες εφαρμογές δεν δημιουργούν κενά ασφαλείας. Δεν προέκυψε επίσης ότι ο υπεύθυνος επεξεργασίας είχε θέσει τέτοια απαίτηση στον εκτελούντα την επεξεργασία. Επιπλέον, όπως προκύπτει η υφιστάμενη άτυπη διαδικασία αλλαγών του εκτελούντος την επεξεργασία δεν ακολουθεί την βέλτιστη, από πλευράς ασφάλειας, προσέγγιση ώστε οι αλλαγές, και ιδίως όσες σχετίζονται και με ζητήματα ασφαλείας να πραγματοποιούνται σε περιβάλλον δοκιμών προτού εφαρμοστούν στο παραγωγικό περιβάλλον. Εξάλλου, ως προς το ζήτημα αυτό, δεν προκύπτει ότι ο υπεύθυνος επεξεργασίας είχε θέσει κάποια ειδική απαίτηση στον εκτελούντα την επεξεργασία.
16. Συνεπώς, βάσει των ανωτέρω, η Αρχή διαπιστώνει τις εξής παραβάσεις για τον

[3] Βλ. συναφώς και τον Κανονισμό (ΕΕ) 2019/881 (Πράξη για την Κυβερνοασφάλεια) στον οποίο ο όρος κυβερνοεπίθεση χρησιμοποιείται σε σχέση με «δράστες» που τις πραγματοποιούν

υπεύθυνο επεξεργασίας:

α. Παράβαση του άρθρου 5 παρ. 1 στοιχ. στ’ σε συνδυασμό με το άρθρο 32 παρ. 1 του ΓΚΠΔ αναφορικά με την ασφάλεια της επεξεργασίας (βλ. ανωτέρω Σκέψη 11, Σκέψη 12 ως προς το σκέλος του μη αποτελεσματικού ελέγχου του εκτελούντος την επεξεργασία από τον υπεύθυνο επεξεργασίας, αλλά και Σκέψη 15 ως προς το σκέλος της έλλειψης καθορισμού ελάχιστων απαιτήσεων για την ασφάλεια, από την πλευρά του υπευθύνου επεξεργασίας, για τον εκτελούντα την επεξεργασία.)

β. Παράβαση του άρθρου 25 παρ. 1 του ΓΚΠΔ αναφορικά με την προστασία των δεδομένων ήδη από το σχεδιασμό, αφού δεν είχαν ληφθεί εκ σχεδιασμού μέτρα αντιμετώπισης διαφόρων κινδύνων ως προς τα προσωπικά δεδομένων (βλ. ανωτέρω Σκέψη 11).

γ. Παράβαση του άρθρου 28 παρ. 3 του ΓΚΠΔ αναφορικά με τα στοιχεία που πρέπει να εμπεριέχονται στη σύμβαση μεταξύ υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία (βλ. ανωτέρω Σκέψη 12 και Σκέψη 13).

δ. Παράβαση του άρθρου 33 παρ. 4 του ΓΚΠΔ αφού δεν παρασχέθηκαν στην Αρχή, χωρίς καθυστέρηση, νεότερες πληροφορίες σχετικά με το περιστατικό (βλ. ανωτέρω Σκέψη 14).

ε. Παράβαση του άρθρου 34 παρ. 1 και 2 του ΓΚΠΔ, αφού δεν έγινε με τον δέοντα τρόπο η αξιολόγηση της σοβαρότητας του περιστατικού προκειμένου να ενημερωθούν αμελλητί τα θιγόμενα πρόσωπα, ενώ η ενημέρωση που τελικά παρείχε δεν ήταν απολύτως ορθή σύμφωνα με τα προβλεπόμενα στις εν λόγω διατάξεις (βλ. ανωτέρω Σκέψη 14).

17. Περαιτέρω, βάσει των ανωτέρω, η Αρχή διαπιστώνει τις εξής παραβάσεις για τον εκτελούντα την επεξεργασία:

α. Παράβαση του άρθρου 32 παρ. 1 του ΓΚΠΔ αναφορικά με την ασφάλεια της επεξεργασίας (βλ. ανωτέρω Σκέψη 11 και Σκέψη 15).

β. Παράβαση του άρθρου 28 παρ. 3 του ΓΚΠΔ αναφορικά με τα στοιχεία που πρέπει να εμπεριέχονται στη σύμβαση μεταξύ υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία (βλ. ανωτέρω Σκέψη 12 και Σκέψη 13).

18. Με βάση τα ανωτέρω, η Αρχή κρίνει ότι συντρέχει περίπτωση άσκησης των εκ του άρθρου 58 παρ. 2 ΓΚΠΔ διορθωτικών εξουσιών της και επιβολής σε σχέση με τις

διαπιστωθείσες παραβάσεις.

19. Η Αρχή κρίνει περαιτέρω ότι πρέπει, με βάση τις παραβάσεις που διαπιστώθηκαν, να επιβληθεί, κατ' εφαρμογή της διάταξης του άρθρου 58 παρ. 2 εδ. θ' ΓΚΠΔ, αποτελεσματικό, αναλογικό και αποτρεπτικό διοικητικό χρηματικό πρόστιμο, συμφώνως προς τα άρθρα 83 ΓΚΠΔ και 39 του Ν. 4624/2019, τόσο στον υπεύθυνο επεξεργασίας όσο και στον εκτελούντα την επεξεργασία.
20. Περαιτέρω η Αρχή έλαβε υπόψη τα κριτήρια επιμέτρησης του προστίμου που ορίζονται στο άρθρο 83, παρ. 2 του ΓΚΠΔ, την παράγραφο 4 του άρθρου αυτού που έχει εφαρμογή για τον υπεύθυνο επεξεργασίας για την παράβαση του άρθρου 5 παρ. 1 στοιχ. στ' του ΓΚΠΔ και την παράγραφο 5 του ίδιου άρθρου 83 που έχει εφαρμογή για τις λοιπές παραβάσεις του υπευθύνου επεξεργασίας και για τις παραβάσεις του εκτελούντος την επεξεργασία, το άρθρο 39 παρ. 1 και 2 του ν. 4624/2019 που αφορά την επιβολή διοικητικών κυρώσεων στους φορείς του δημόσιου τομέα και τις Κατευθυντήριες Γραμμές 04/2022 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων[4] για τον υπολογισμό των διοικητικών προστίμων υπό τον ΓΚΠΔ, οι οποίες εγκρίθηκαν στις 24/5/2023, καθώς και τα πραγματικά δεδομένα της εξεταζόμενης υπόθεσης και ιδίως τα εξής:
    i) Η διαπιστωθείσα παράβαση του άρθρου 5 παρ. 1 στοιχ. στ' του ΓΚΠΔ από τον υπεύθυνο επεξεργασίας υπάγεται, σύμφωνα με τις διατάξεις του άρθρου 83 παρ. 5 εδ. β' ΓΚΠΔ, στην ανώτερη προβλεπόμενη κατηγορία του συστήματος διαβάθμισης διοικητικών προστίμων («σημαντικές» παραβάσεις με μέγιστο ύψος 20.000.000 ευρώ).
    ii) Η δραστηριότητα σχετίζεται με τις κύριες δραστηριότητες του υπευθύνου επεξεργασίας, εφόσον η χορήγηση αντιγράφων πιστοποιητικών στους δημότες περιλαμβάνεται στις αρμοδιότητες του υπεύθυνου επεξεργασίας που ασκούνται σε καθημερινή βάση.
    iii) Ο αριθμός των υποκειμένων των δεδομένων ο οποίος φαίνεται να επηρεάστηκε δεν μπορεί να θεωρηθεί μικρός, καθώς φαίνεται να επηρεάστηκαν εννιακόσια (900) υποκείμενα δεδομένων που αποτελούν χρήστες των υπηρεσιών του υπεύθυνου επεξεργασίας, ενώ

[4] https://edpb.europa.eu/system/files/2023-06/edpb_guidelines_042022_calculationofadministrativefines_en.pdf

το γεγονός ότι δεν αντιμετωπίστηκε επαρκώς με αποτέλεσμα να συμβεί το ίδιο περιστατικό τρεις (3) φορές, δυνητικά θα μπορούσε να επηρεάσει μεγαλύτερο αριθμό επηρεαζόμενων υποκειμένων των δεδομένων.

iv) Η επεξεργασία αφορά μεν κυρίως «απλά» προσωπικά δεδομένα, στα οποία, όμως, περιλαμβάνονται και δεδομένα, όπως αστυνομικές ταυτότητες ή διαβατήρια τα οποία μπορούν εύκολα να χρησιμοποιηθούν σε περιστατικά υποκλοπής ταυτότητας (σε επιγραμμικά, π.χ., περιβάλλοντα) και, κατά συνέπεια, θεωρούνται δεδομένα των οποίων η παραβίαση μπορεί να επιφέρει σοβαρούς κινδύνους[5].

v) Ο υπεύθυνος επεξεργασίας επέδειξε δυσχέρεια στη συνεργασία με την Αρχή, παραλείποντας να παράσχει εγκαίρως τις πληροφορίες που του ζητήθηκαν.

vi) Η παράβαση ναι μεν δεν είχε μεγάλη διάρκεια και ο υπεύθυνος επεξεργασίας προέβη άμεσα στη διακοπή λειτουργίας της ιστοσελίδας, αλλά υπήρξαν πολλαπλές εσφαλμένες δοκιμές επαναλειτουργίας με το ίδιο κενό ασφαλείας, το οποίο δεν ήταν αντιληπτό ούτε από τον υπεύθυνο επεξεργασίας αλλά ούτε και από τον εκτελούντα την επεξεργασία και επομένως δυνητικά θα μπορούσε να είχε μεγαλύτερη διάρκεια.

vii) Δεν προκύπτει υλική βλάβη για τα υποκείμενα των δεδομένων.

viii) Δεν έχει διαπιστωθεί προηγούμενη αντίστοιχη παράβαση από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία.

ix) Το γεγονός ότι η φύση της εταιρείας του εκτελούντος την επεξεργασία είναι μικρή καθώς είναι Ομόρρυθμη Εταιρεία.

21. Η Αρχή κρίνει ότι, με βάση τις περιστάσεις που διαπιστώθηκαν και τα ανωτέρω κριτήρια, οι κυρώσεις που αναφέρονται στο διατακτικό της απόφασης είναι το αποτελεσματικό, αναλογικό και αποτρεπτικό μέτρο τόσο προς αποκατάσταση της συμμόρφωσης, όσο και για την τιμωρία της παράνομης συμπεριφοράς.

[5] Βλ. συναφώς και τη Σκέψη 57 των Κατευθυντηρίων Γραμμών 4/2022 του ΕΣΠΔ

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή λαμβάνοντας υπόψη τα παραπάνω:

α) Επιβάλλει με βάση το άρθρο 58 παρ. 2 εδ. θ' του ΓΚΠΔ, διοικητικό πρόστιμο στον Δήμο Αλίμου συνολικού ύψους 10.000 ευρώ, για την παραβίαση του άρθρου 5 παρ. 1 στοιχ. στ'. σε συνδυασμό με το άρθρο 32 παρ. 1 του Κανονισμού (ΕΕ) 2016/679.

β) Επιβάλλει με βάση το άρθρο 58 παρ. 2 εδ. θ' του ΓΚΠΔ, διοικητικό πρόστιμο στον Δήμο Αλίμου συνολικού ύψους 5.000 ευρώ, για την παραβίαση των άρθρων 28 παρ. 3, 33 παρ. 4 και 34 παρ. 1 και παρ. 2 του Κανονισμού (ΕΕ) 2016/679.

γ) Απευθύνει με βάση το άρθρο 58 παρ. 2 εδ. θ' του ΓΚΠΔ, επίπληξη στον Δήμο Αλίμου για την παραβίαση του άρθρου 25 παρ. 1 του Κανονισμού (ΕΕ) 2016/679.

δ) Επιβάλλει με βάση το άρθρο 58 παρ. 2 εδ. θ' του ΓΚΠΔ διοικητικό πρόστιμο στην εταιρεία με την επωνυμία «ΤΕΣΤ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ Ο.Ε.» συνολικού ύψους 5.000 ευρώ, για την παραβίαση των άρθρων 32 παρ. 1 και 28 παρ. 3 του Κανονισμού (ΕΕ) 2016/679.

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