Αρ. Φακ.: 11.17.001.008.029

ΜΕ ΤΟ ΧΕΡΙ

14 Οκτωβρίου, 2020

ΑΠΟΦΑΣΗ
Θέμα: Παράπονο για την ασφάλεια των προσωπικών δεδομένων που τηρούνται από το Σωματείο ΤΕΥ- ΑΤΗΚ και την Εταιρεία ΑΤΗΚ

Αναφέρομαι στη μεταξύ μας αλληλογραφία, σχετικά με το πιο πάνω θέμα και σας πληροφορώ τα κάτωθι:

Γεγονότα

1.1. Με βάση το καθήκον εξέτασης καταγγελιών που παρέχει στον Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα το άρθρο 57(1)(στ) του Κανονισμού (ΕΕ) 2016/679 (στο εξής «ο Κανονισμός») και το άρθρο 24(β) του Νόμου που προνοεί για την Προστασία των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και για την Ελεύθερη Κυκλοφορία των Δεδομένων Αυτών (Νόμος 125(Ι)/2018), εξέτασα την καταγγελία/παράπονο της XXXXX, εργοδοτούμενης στην Εταιρεία ΑΤΗΚ (Αρχής Τηλεπικοινωνιών Κύπρου - εφεξής «η Εταιρεία»), αναφορικά με θέματα ασφάλειας των προσωπικών δεδομένων των εργοδοτουμένων της Εταιρείας ΑΤΗΚ, τα οποία προέκυψαν κατά την εξέταση του αιτήματος της παραπονούμενης για άσκηση του δικαιώματος πρόσβασης στα προσωπικά δεδομένα της που τηρούνται από το Σωματείο ΤΕΥ-ΑΤΗΚ (Ταμείο Ευημερίας Υπαλλήλων Αρχής Τηλεπικοινωνιών Κύπρου – εφεξής «το Σωματείο»).

Συγκεκριμένα, η παραπονούμενη στις 26 Οκτωβρίου 2019, ζήτησε μέσω ηλεκτρονικού μηνύματος, από τον XXXXX, Υπεύθυνο Προστασίας Δεδομένων του Σωματείου, να ασκήσει το δικαίωμα πρόσβασης της βάσει του άρθρου 15 του Κανονισμού και να λάβει αντίγραφο των προσωπικών δεδομένων που διατηρεί το Σωματείο για το άτομό της καθώς και την πηγή προέλευσης των εν λόγω δεδομένων που δεν συλλέγησαν από την ίδια.

1.2. Στις 18 Νοεμβρίου 2019, ο XXXXX, απάντησε με ηλεκτρονικό μήνυμα στην παραπονούμενη, αναφέροντας τα εξής:

«Τα προσωπικά δεδομένα που διατηρεί το Σωματείο για το συγκεκριμένο μέλος είναι τα ακόλουθα:

Αριθμός υπαλλήλου, Φύλο, Ονοματεπώνυμο, Ημερομηνία γέννησης, Ημερομηνία πρόσληψης, Ημερομηνία εγγραφής στο ΤΕΥ-ΑΤΗΚ, Διεύθυνση αλληλογραφίας,

Υπηρεσιακό τηλέφωνο, Κινητό τηλέφωνο, Ηλεκτρονική διεύθυνση. Τα πιο πάνω συλλέγονται από τη βάση δεδομένων της ΟΥΤΑ μέσα από την «Συμφωνία Ανταλλαγής και Προστασίας Δεδομένων Προσωπικού Χαρακτήρα» που υπογράφηκε μεταξύ των ΤΕΥ-ΑΤΗΚ και ΟΥΤΑ.».

1.3. Στις 28 Νοεμβρίου 2019, η παραπονούμενη απέστειλε νέο αίτημα προς το Σωματείο, ζητώντας όπως «έχει απευθείας σχέση με το Σωματείο, όσον αφορά τα προσωπικά δεδομένα που διατηρούνται για το άτομο [της]».

1.4. Όπως αναφέρει στο παράπονο της η XXXXX, στις 3 Δεκεμβρίου 2019, επικοινώνησε τηλεφωνικώς μαζί της ο XXXXX και της ζήτησε να περάσει από το Γραφείο του για να της παραδώσει στο χέρι την επιστολή του Σωματείου, όσον αφορά στο αίτημα της ημερομηνίας 26 Οκτωβρίου 2019, και να λάβει αντίγραφο όλων των προσωπικών δεδομένων που διατηρούσε το Σωματείο για το άτομο της.

1.5. Με την εν λόγω επιστολή, το Σωματείο της επισύναψε και αντίγραφο της φωτογραφίας της.

1.6. Στις 22 Ιανουαρίου 2020, η παραπονούμενη αφού δεν είχε οποιαδήποτε ανταπόκριση από το Σωματείο αναφορικά με το αίτημα της ημερομηνίας 28 Νοεμβρίου 2020, απέστειλε νέο ηλεκτρονικό μήνυμα στον XXXXX, ζητώντας όπως έχει απάντηση στην επιστολή της.

1.7. Στις 23 Ιανουαρίου 2020, ο XXXXX ανταποκρίθηκε στο αίτημα της παραπονούμενης, ενημερώνοντας την ότι:

«Αναφορικά με το πιο πάνω θέμα και σε συνέχεια του αιτήματος σου για απευθείας σχέση με το ΤΕΥ-ΑΤΗΚ για τα προσωπικά δεδομένα που διατηρούνται για το άτομο σου, σε ενημερώνουμε ότι το αίτημα σου δεν μπορεί να ικανοποιηθεί.

Στο παρελθόν έγιναν προσπάθειες για διαχωρισμό της βάσης δεδομένων από το ΤΕΥ-ΑΤΗΚ για τα μέλη του από την βάση δεδομένων που διατηρεί η ΟΥΤΑ για τους υπαλλήλους της, αλλά είχαν παρουσιαστεί τεχνικά προβλήματα που παραμένουν ανυπέρβλητα.

Ως εκ τούτου, η συλλογή των δεδομένων από το ΤΕΥ-ΑΤΗΚ για τα μέλη του από την βάση δεδομένων της ΟΥΤΑ θεωρείται απαραίτητη προϋπόθεση για την ομαλή λειτουργία του ΤΕΥ-ΑΤΗΚ και τα δικά σας δεδομένα δεν μπορούν να τύχουν ξεχωριστής διαχείρισης.».

1.8. Ως εκ των ανωτέρω, στις 25 Φεβρουαρίου 2020, απέστειλα σχετική επιστολή στον Υπεύθυνο Προστασίας Δεδομένων της Εταιρείας και στον Υπεύθυνο Προστασίας Δεδομένων του Σωματείου. Με την εν λόγω επιστολή μου, έχοντας ως καθοριστικά κριτήρια για τον έλεγχο της νομιμότητας της επεξεργασίας των προσωπικών δεδομένων, τις αρχές της νομιμότητας, του περιορισμού του σκοπού και κυρίως της ελαχιστοποίησης (άρθρο 5(1)(α), (β) και (γ) του Κανονισμού), ζήτησα από τους Καθ'ων την καταγγελία να αναφέρουν, το αργότερο μέχρι τις 31 Μαρτίου 2020:
(α) τους λόγους που δεν μπορούσε να διαχωριστεί η βάση δεδομένων του Σωματείου με τη βάση δεδομένων της Εταιρείας, αφού ο υπεύθυνος επεξεργασίας και ο σκοπός τήρησης του κάθε αρχείου είναι διαφορετικός,

(β) κατά πόσο το προσωπικό του Σωματείου είχε πρόσβαση στα προσωπικά δεδομένα όλων των υπαλλήλων της Εταιρείας ή μόνο των μελών του και με ποιο τρόπο επιτυγχανόταν η εν λόγω πρόσβαση,

(γ) τα τεχνικά και οργανωτικά μέτρα ασφάλειας που τηρούσε το Σωματείο αναφορικά με τα προσωπικά δεδομένα που επεξεργαζόταν και

(δ) με ποια νομική βάση των άρθρων 6 και 9 του Κανονισμού νομιμοποιείται το Σωματείο να επεξεργάζεται προσωπικά δεδομένα, τα οποία συλλέγονται απευθείας από την Εταιρεία.

1.9. Η XXXXX, Υπεύθυνος Προστασίας Δεδομένων της Εταιρείας, με επιστολή της με Αρ. Φακ.: LGLK10-426 και με ημερομηνία 27.03.2020, μου ανέφερε, μεταξύ άλλων, τα κάτωθι:

(α) Το Σωματείο διατηρεί ηλεκτρονικό αρχείο με το Μητρώο Μελών Ταμείου, το οποίο επικαιροποιείται με άντληση πληροφοριών από τη βάση δεδομένων των Υπηρεσιών Προσωπικού της Εταιρείας με αυτόματο ηλεκτρονικό τρόπο. Το αρχείο του Σωματείου και η βάση δεδομένων των Υπηρεσιών Προσωπικού της Εταιρείας, είναι δύο διαφορετικά αρχεία.

(β) Η αυτόματη άντληση επικαιροποιημένων πληροφοριών από τη βάση δεδομένων των Υπηρεσιών Προσωπικού της Εταιρείας είναι απαραίτητη ούτως ώστε να διασφαλίζεται η ορθή παροχή ωφελημάτων στα μέλη του Σωματείου, στη βάση των επικαιροποιημένων αυτών πληροφοριών.

(γ) Το Μητρώο Μελών του Σωματείου περιλαμβάνει τα ακόλουθα δεδομένα υπαλλήλων και συνταξιούχων της Εταιρείας, τα οποία αντλεί αυτόματα από την ηλεκτρονική βάση δεδομένων της Εταιρείας:

- Αριθμός υπαλλήλου
- Φύλο
- Ονοματεπώνυμο
- **Φωτογραφία**
- Ημερομηνία γέννησης
- Ημερομηνία πρόσληψης
- Ημερομηνία θανάτου (όπου εφαρμόζεται)
- Ημερομηνία αφυπηρέτησης
- Διεύθυνση αλληλογραφίας
- Υπηρεσιακό τηλέφωνο (όπου είναι διαθέσιμο)
- Σταθερό τηλέφωνο (όπου είναι διαθέσιμο)
- Κινητό τηλέφωνο (όπου είναι διαθέσιμο)
- Ηλεκτρονική διεύθυνση
- Αριθμός συνδεδεμένου υπαλλήλου
- Κατάσταση: χήρος/χήρα, εξαρτώμενο τέκνο

Επιπρόσθετα, η Εταιρεία αποστέλλει προς το Σωματείο, αρχεία Excel, με τα ακόλουθα στοιχεία μελών του Σωματείου, για σκοπούς ελέγχου και συμψηφισμού συνδρομών και άλλων πληρωτέων ποσών προς το Σωματείο:

- Αριθμός υπαλλήλου
- Ονοματεπώνυμο υπαλλήλου
- Κατάσταση: Ενεργός υπάλληλος, Συνταξιούχος/χήρος/χήρα
- Ποσό μηνιαίας συνδρομής

- Ποσό ΦΠΑ επί της μηνιαίας συνδρομής
- Άλλο πληρωτέο, προς το Σωματείο, ποσό που αποκόπηκε από το μισθό/σύνταξη/παροχή μέλους του Σωματείου.

(δ) Το προσωπικό του Σωματείου (σύνολο εννιά άτομα), έχει αυτόματη ηλεκτρονική πρόσβαση στο Μητρώο Μελών Σωματείου και στα αρχεία excel που αποστέλλονται από την Εταιρεία ΑΤΗΚ.

(ε) Επιπρόσθετα, το προσωπικό του Σωματείου έχει πρόσβαση, στα ακόλουθα προσωπικά δεδομένα των εργοδοτουμένων της Εταιρείας που δεν είναι μέλη του Σωματείου:

- Αριθμός υπαλλήλου
- Ονοματεπώνυμο υπαλλήλου
- Υπηρεσιακό τηλέφωνο (όπου είναι διαθέσιμο)
- Κινητό τηλέφωνο (όπου είναι διαθέσιμο)
- Ηλεκτρονική διεύθυνση (όπου είναι διαθέσιμη)
- Βαθμός και ειδικότητα στην υπηρεσία
- Διεύθυνση εργασίας

(στ) Η πρόσβαση στα πιο πάνω δεδομένα εξασφαλίζεται με αυτόματη σύνδεση των υπηρεσιακών ηλεκτρονικών υπολογιστών του προσωπικού του Σωματείου με την υπηρεσιακή Πύλη Ενδοδικτύου (Intranet) της Εταιρείας.

(ζ) Η διακοπή της πρόσβασης από το Σωματείο στη βάση δεδομένων της Εταιρείας, σε προσωπικά δεδομένα υπαλλήλων της Εταιρείας, που δεν είναι μέλη του Σωματείου, αναμένεται να ολοκληρωθεί στις 31 Μαρτίου 2020.

(η) Από τη ψήφιση του Κανονισμού, το Σωματείο προχώρησε, μεταξύ άλλων, στα ακόλουθα τεχνικά και οργανωτικά μέτρα:

- Δημιουργία ασφαλούς χώρου φύλαξης του έντυπου αρχείου και εισαγωγή ασφαλιστικών δικλίδων φύλαξης του ηλεκτρονικού αρχείου, με περιορισμένη πρόσβαση, μόνο από το απαραίτητο προσωπικό του Σωματείου.

- Καταστροφή αρχείου που περιλάμβανε προσωπικά δεδομένα παλαιότερων ετών και επικαιροποίηση του ηλεκτρονικού και έντυπου αρχείου.

- Εκπαίδευση του προσωπικού.

- Διορισμό του XXXXX, ως Υπεύθυνος Προστασίας Δεδομένων.

- Υπογραφή Συμφωνίας Ανταλλαγής και Προστασίας Δεδομένων, με ημερομηνία 15 Οκτωβρίου 2018, μεταξύ της Εταιρείας και του Σωματείου.

- Ανάρτηση της Πολιτικής Απορρήτου Προσωπικών Δεδομένων, στην ιστοσελίδα του.

(θ) Η νομική βάση στην οποία στηρίχθηκε η επεξεργασία προσωπικών δεδομένων από το Σωματείο είναι τα άρθρα 6(1)(α) και (β) του Κανονισμού.

1.9.1 Στην εν λόγω επιστολή ημερ. 27.3.2020 επισυνάπτετο και η μεταξύ της Εταιρείας και Σωματείου σχετική συμφωνία ημερ. 15.10.2018 για «Ανταλλαγή και

Προστασία Δεδομένων Προσωπικού Χαρακτήρα». Στην παρ. 3.1 της Συμφωνίας αυτής, αναφέρονταν τα δεδομένα τα οποία η Εταιρεία αναλάμβανε να παραδώσει στο Ταμείο, αφού λάμβανε προηγουμένως την γραπτή συγκατάθεση των υπαλλήλων και συνταξιούχων της Εταιρείας. Συμφωνείτο όπως παραδοθεί Αρχείο με το **Μητρώο Μελών του Ταμείου** και στοιχεία όπως Αριθμός Υπαλλήλου, Αριθμός Δελτίου Ταυτότητας, Φύλο, Ονοματεπώνυμο, Ημερομηνία Γέννησης κ.ά. Στα δεδομένα τα οποία θα παραδίδονταν, **δεν υπήρχε** συμφωνημένη **η φωτογραφία** του υπαλλήλου.

1.10. Στις 9 Απριλίου 2020, απέστειλα επιστολή στον Ανώτατο Εκτελεστικό Διευθυντή της Εταιρείας και στον Πρόεδρο του Διοικητικού Συμβουλίου του Σωματείου, αναφέροντας, μεταξύ άλλων, ότι**:**

(α) Το Σωματείο και η Εταιρεία είναι δύο ξεχωριστοί υπεύθυνοι επεξεργασίας που τηρούν δύο ξεχωριστά αρχεία για διαφορετικούς σκοπούς.

(β) Το Σωματείο και η Εταιρεία έχουν υποχρέωση τήρησης των βασικών αρχών επεξεργασίας, όπως αυτές καθορίζονται στο άρθρο 5 του Κανονισμού. Συνεπώς, η Εταιρεία όφειλε να γνωρίζει ότι, η παραχώρηση πρόσβασης στο προσωπικό του Σωματείου, στη βάση δεδομένων της, αναφορικά με υπαλλήλους που δεν είναι μέλη του Σωματείου, παραβιάζει την αρχή του περιορισμού του σκοπού, την αρχή της ελαχιστοποίησης και την αρχή της ακεραιότητας και εμπιστευτικότητας (άρθρο 5(1) του Κανονισμού).

(γ) Επιπρόσθετα, η παράνομη παραχώρηση πρόσβασης από την Εταιρεία στο Σωματείο και κατ' επέκταση, η παράνομη πρόσβαση στο αρχείο της Εταιρείας από το Σωματείο, συνιστά παραβίαση της ασφάλειας της επεξεργασίας (άρθρο 32 του Κανονισμού).

(δ) Από το γράμμα και τον σκοπό του άρθρου 32 του Κανονισμού που αφορά στην ασφάλεια της επεξεργασίας, είναι σαφές ότι, η υποχρέωση του υπεύθυνου επεξεργασίας για διασφάλιση της ασφάλειας της επεξεργασίας, έχει τόσο προληπτικό, όσο και κατασταλτικό χαρακτήρα. Προληπτικό, ώστε, τα εφαρμοστέα μέτρα να αποτρέψουν περιστατικά παραβίασης προσωπικών δεδομένων, κατασταλτικό, ώστε τυχόν περιστατικό να μπορεί να ανιχνευθεί και να διερευνηθεί.

<u>Επισημάνεται ότι, η Εταιρεία δεν είχε θέσει σε εφαρμογή την τεχνική δυνατότητα να επιτρέπεται η πρόσβαση από το Σωματείο μόνο στα προσωπικά δεδομένα που νομιμοποιείται να επεξεργάζεται και αφορούν μόνο στα μέλη του.</u>

(ε) Με βάση τα ανωτέρω, προκύπτει ότι, η Εταιρεία δεν υιοθέτησε τα πλέον ενδεδειγμένα μέτρα για την ασφάλεια της επεξεργασίας, κατά παράβαση του 32 του Κανονισμού.

Με την ίδια επιστολή, ζήτησα τις θέσεις/σχόλια των Καθ'ων την καταγγελία για τα πιο πάνω καθώς επίσης όπως απαντήσουν στα ακόλουθα ερωτήματα:

(α) Τη νομική βάση με την οποία το Σωματείο είχε πρόσβαση στη βάση δεδομένων της Εταιρείας και λάμβανε προσωπικά δεδομένα **μη μελών** του Σωματείου (και κατ' επέκταση τη νομική βάση με την οποία η Εταιρεία παρείχε τέτοια πρόσβαση),

(β) κατά πόσον είχε ήδη διακοπεί η εν λόγω πρόσβαση,

(γ) τις ενέργειες που είχε προβεί το Σωματείο για καταστροφή των δεδομένων που διατηρούσε στο αρχείο του και αφορούσαν σε μη μέλη του και

(δ) τους λόγους που το Σωματείο χρειαζόταν να διατηρεί τη φωτογραφία των μελών του.

1.11. Η XXXXX με ηλεκτρονικό μήνυμα της με ημερομηνία 27 Απριλίου 2020, με ενημέρωσε ότι:

(α) Η πρόσβαση που είχε δοθεί στο Σωματείο από την Εταιρεία παρείχε στο Σωματείο τη δυνατότητα θέασης («view only») και άντλησης μόνο των απαραίτητων βασικών υπηρεσιακών στοιχείων των υπαλλήλων της Εταιρείας. Η άντληση των βασικών υπηρεσιακών στοιχείων επιτυγχανόταν με τη χρήση σχετικής εφαρμογής που σχεδίασε η Πληροφορική της Εταιρείας. Η εφαρμογή επέτρεπε στα εξουσιοδοτημένα άτομα του Σωματείου να καταχωρούν τον αριθμό υπαλλήλου, την κατάσταση του οποίου επιθυμούσαν να επικαιροποιήσουν και να λαμβάνουν μόνο μια επιβεβαίωση ότι, ο υπάλληλος με τον αριθμό που καταχώρησαν είναι μέλος του Σωματείου, με θέαση πληροφοριών όπως το ονοματεπώνυμο του υπαλλήλου , το τμήμα του, το κτίριο που εργάζεται, τον βαθμό και η ειδικότητα του, στοιχεία τα οποία βρίσκονταν ήδη καταχωρημένα στο Αρχείο Πληροφοριών Υπαλλήλων του ενδοδικτύου (intranet) της Εταιρείας.

(β) Δεν δημιουργούνταν αντίγραφα ή αρχεία από το Σωματείο με τα στοιχεία αυτά.

(γ) Το Σωματείο αφού είχε προβεί στη σχετική θέαση, επικαιροποιούσε στη συνέχεια τη σχετική κατάσταση του μέλους του. Η επικαιροποίηση των καταστάσεων αυτών γινόταν σε τακτά χρονικά διαστήματα.

(δ) Η Εταιρεία για σκοπούς ασφαλείας περιόρισε τα άτομα του Σωματείου που είχαν τη δυνατότητα θέασης των πιο πάνω αναφερόμενων πληροφοριών και εγκατέστησε σύστημα ιχνηλάτησης των προσβάσεων τους.

(ε) Η νομική βάση στην οποία βασίστηκε η πρόσβαση είναι τα άρθρα 6(1)(α) και 6(1)(β) του Κανονισμού.

(στ) Η δυνατότητα θέασης των πληροφοριών μη μελών του Σωματείου είχε διακοπεί από τις 31 Μαρτίου 2020, με σχετική αναβάθμιση της εφαρμογής.

(ζ) Το Σωματείο δεν τηρούσε αντίγραφα ή αρχεία με δεδομένα μη μελών του.

(η) Το Σωματείο δεν διατηρούσε την φωτογραφία των μελών του σε κάποιο αρχείο. Μόνο η Εταιρεία διατηρούσε φωτογραφία των υπαλλήλων της στο ενδοδίκτυο.

1.12. Με επιστολή του Γραφείου με Αρ. Φακ.: 11.17.001.008.029 και με ημερομηνία 29 Απριλίου 2020, ζήτησα από την Εταιρεία όπως αναφέρει:

(α) Επακριβώς ένα προς ένα τα είδη/κατηγορίες προσωπικών δεδομένων που το Σωματείο είχε δικαίωμα θέασης («view only») για τα μέλη του.

(β) Τα είδη/κατηγορίες προσωπικών δεδομένων που το Σωματείο αντλούσε από την βάση δεδομένων της Εταιρείας και να επεξηγήσει την έννοια του όρου «αντλεί» στην προκειμένη περίπτωση.

(γ) Τα είδη/κατηγορίες προσωπικών δεδομένων που το Σωματείο είχε δικαίωμα θέασης και/ή άντλησης και/ή επεξεργασίας οποιασδήποτε μορφής για τα μη μέλη του.

(δ) Τον αριθμό των ατόμων του Σωματείου που είχαν τη δυνατότητα θέασης των προσωπικών δεδομένων μελών και μη μελών τους πριν τις 31 Μαρτίου 2020, ημερομηνία κατά την οποία, όπως ανέφεραν οι Καθ'ών την καταγγελία στην επιστολή τους με ημερομηνία 27 Απριλίου 2020, είχε γίνει σχετική αναβάθμιση και διακόπηκε η δυνατότητα θέασης του Σωματείου σε πληροφορίες μη μελών του.

(ε) Τον αριθμό των ατόμων του Σωματείου που, μετά τις 31 Μαρτίου 2020, είχαν τη δυνατότητα θέασης των προσωπικών δεδομένων των μελών του Σωματείου.

(στ) Τους λόγους που η εν λόγω δυνατότητα θέασης δεν ήταν εξαρχής περιορισμένη στα απολύτως απαραίτητα άτομα.

(ζ) Τους λόγους που η Εταιρεία δεν είχε εξαρχής εγκαταστήσει σύστημα ιχνηλάτησης των προσβάσεων τους.

(η) Τους λόγους που το Σωματείο δεν μπορούσε να διατηρεί δική του βάση δεδομένων, ως ξεχωριστός και ανεξάρτητος υπεύθυνος επεξεργασίας.

1.13. Στις 12 Μαΐου 2020, μέσω ηλεκτρονικού μηνύματος, η κ. Χρίστου με πληροφόρησε, μεταξύ άλλων, ότι**:**

(α) Τα είδη/κατηγορίες προσωπικών δεδομένων που το Σωματείο έχει δικαίωμα θέασης («view only») για τα μέλη του από το ενδοδίκτυο είναι τα ακόλουθα:

Για τα εν ενεργεία μέλη: **φωτογραφία**, αριθμός υπαλλήλου, ονοματεπώνυμο, τηλέφωνο εργασίας, αριθμός υπηρεσιακού κινητού τηλεφώνου, υπηρεσιακό ηλεκτρονικό ταχυδρομείο, υπηρεσία, ειδικότητα, βαθμός και το κτήριο στο οποίο εργάζεται.

Για τα συνταξιούχα μέλη: **φωτογραφία**, αριθμός υπαλλήλου, ονοματεπώνυμο, αριθμός κινητού τηλεφώνου (για όσους έχουν υπογράψει έντυπο ότι επιθυμούν να εμφανίζεται το κινητό τους τηλέφωνο στο ενδοδίκτυο) και ειδικότητα.

(β) Το Σωματείο προβαίνει σε θέαση των δεδομένων του ενδοδικτύου, δεν αντλεί όμως οποιαδήποτε δεδομένα από τη βάση δεδομένων.

(γ) Τα είδη/κατηγορίες προσωπικών δεδομένων που το Σωματείο είχε δικαίωμα θέασης («view only») για τα μη μέλη του ήταν τα πιο κάτω:

Για τους εν ενεργεία υπαλλήλους που **δεν ήταν μέλη**: φωτογραφία, αριθμός υπαλλήλου, ονοματεπώνυμο, τηλέφωνο εργασίας, αριθμός υπηρεσιακού κινητού τηλεφώνου, υπηρεσιακή ηλεκτρονική διεύθυνση, υπηρεσία, ειδικότητα, βαθμός και το κτήριο στο οποίο εργάζεται.

Για τους συνταξιούχους υπαλλήλους που **δεν ήταν μέλη**: φωτογραφία, αριθμός υπαλλήλου, ονοματεπώνυμο, αριθμός κινητού τηλεφώνου και ειδικότητα.

(δ) Τα άτομα/προσωπικό του Σωματείου που είχαν τη δυνατότητα θέασης των προσωπικών δεδομένων μέχρι τις 31 Μαρτίου 2020, ημερομηνία κατά την οποία, όπως έχουν αναφέρει οι Καθ'ων την καταγγελία στην επιστολή τους ημερομηνίας 27 Απριλίου 2020, είχε γίνει σχετική αναβάθμιση της εφαρμογής και διακόπηκε η δυνατότητα θέασης του Σωματείου σε πληροφορίες μη μελών του, ήταν εννιά (9).

(ε) Αποφασίστηκε όπως από τις 15 Μαΐου 2020, δυνατότητα θέασης έχει πλέον μόνο ένας (1), ο Γενικός Διευθυντής, για σκοπούς καλύτερης συμμόρφωσης με τις πρόνοιες του Κανονισμού.

2.6. Αναφορικά με το ερώτημα μου για τους λόγους που η δυνατότητα θέασης δεν ήταν εξαρχής περιορισμένη στα απολύτως απαραίτητα άτομα, οι Καθ'ων την καταγγελία απάντησαν ότι**:**

«Η θέαση είχε κριθεί ότι ήταν περιορισμένη στα απολύτως απαραίτητα άτομα.».

2.7. Αναφορικά με το ερώτημα μου για τους λόγους που η Εταιρεία δεν είχε εξαρχής εγκαταστήσει σύστημα ιχνηλάτησης των προσβάσεων του προσωπικού του Σωματείου, οι Καθ'ων την καταγγελία απάντησαν ότι:

«Το Σύστημα ιχνηλάτησης εγκαταστάθηκε κατά την αναβάθμιση που έγινε στις 31.3.2020 προς υποβοήθηση του περιορισμού που πραγματοποιήθηκε.».

2.8. Οι λόγοι που το Σωματείο δεν μπορεί να διατηρεί δική του βάση δεδομένων είναι οικονομικοί. Το κόστος υλοποίησης δημιουργίας δικής του βάσης δεδομένων υπολογίστηκε περίπου σε €450.000.

1.14. Την 3 Ιουνίου, 2020, απέστειλα επιστολή προς την Εταιρεία και προς το Σωματείο με την οποία κατέληξα πως υπήρξαν ενδεχομένως παραβάσεις των διατάξεων των άρθρων 5(1)(α), 5(1)(β), 5(1)(γ), 5(1)(στ), 5(2), 13, 14, 25 και 32 του Κανονισμού, καθώς και του άρθρου 33(1)(ιγ) του Νόμου 125(Ι)/2018. Ζήτησα επ' αυτής της κατάληξης, όπως ενημερωθώ εντός καθορισμένης περιόδου, για ποιους λόγους δεν θα έπρεπε να επιβληθεί οποιαδήποτε διοικητική κύρωση, αλλά και για τον κύκλο εργασιών τους.

1.15. Την 22 Ιουνίου, 2020 με κοινή επιστολή τους, τόσο η Εταιρεία όσο και το Σωματείο, επικαλούντο ως λόγους μη επιβολής διοικητικής κύρωσης, εν συντομία τα ακόλουθα:

(α) <u>Έλλειψη δέουσας έρευνας</u>: Ο λόγος αυτός στηριζόταν στις αποφάσεις που εμπεριέχονταν στην επιστολή μου ημερ. 3 Ιουνίου, 2020, οι οποίες επαναλαμβάνονται και στην παρούσα απόφαση. Ειδικότερα, ήταν η θέση της Εταιρείας πως τα γεγονότα στα οποία στηρίχθηκε η Απόφαση 44/2019 της Ελληνικής Αρχής, ήταν διαφορετικά από την παρούσα. Στην περίπτωση εκείνη αφορούσε παράνομη αντιγραφή των δεδομένων προσωπικού χαρακτήρα και όλης της υπηρεσιακής ηλεκτρονικής αλληλογραφίας των υπαλλήλων και ανωτέρων στελεχών της θυγατρικής εταιρείας που βρισκόταν αποθηκευμένη στον εν λόγω διακομιστή (της θυγατρικής), από τρίτο άτομο που ισχυρίστηκε ότι ενεργούσε για τη μητρική εταιρεία. Η υπόθεση που διερευνά το Γραφείο μου, αφορά αποκλειστικά ένα μεμονωμένο παράπονο υπαλλήλου που είναι μέλος του Σωματίου και το οποίο ζήτησε από το Σωματείο, κατ' εξαίρεση, να επιβεβαιώνει από μόνο του τα στοιχεία του. Η δυνατότητα θέασης στα μη-μέλη που υπήρχε, ουσιαστικά δεν εξασκείτο από τα εξουσιοδοτημένα μέλη, καθότι οι υπάλληλοι του Σωματείου προέβαιναν σε θέαση μόνο των πληροφοριών των υπαλλήλων-μελών τους και μόνο όταν απαιτείτο για να τα εξυπηρετήσουν, διευκρίνιση που δόθηκε με τις επιστολές ημερ. 27.4.2020 και

12.5.2020. Δεν υπήρχε τεχνική δυνατότητα δημιουργίας αντιγράφων ή οιωνδήποτε άλλων αρχείων, ούτε δυνατότητα διασύνδεση βάσεων και διαρροής ή απώλειας πληροφοριών. Η θέαση ήταν απαραίτητη γιατί αποσκοπούσε στην επιβεβαίωση από το ίδιο το Σωματείο των στοιχείων των μελών του στην βάση επικαιροποιημένων πληροφοριών. Μόνο το 2% των υπαλλήλων της Εταιρείας δεν είναι ταυτόχρονα και μέλη του Σωματείου.

(β) Μετριαστικούς παράγοντες:
Αναφέρθηκαν οι ακόλουθοι μετριαστικοί παράγοντες:
(1) Η παραπονούμενη δεν είχε προβεί σε άμεσο παράπονο προς την Εταιρεία.
(2) Δεν έχει προκληθεί οποιαδήποτε βλάβη στην παραπονούμενη, η οποία είναι μέλος του Σωματείου.
(3) Οι πληροφορίες στις οποίες είχαν πρόσβαση τα 9 άτομα του Σωματείου, ήταν γενικές υπηρεσιακές πληροφορίες των υπαλλήλων που είναι ήδη αναρτημένες και επικαιροποιημένες στο ενδοδίκτυο της Εταιρείας και αποσκοπούν στην ταυτοποίηση τους και επικοινωνία μαζί τους όταν και εάν χρειαστεί.
(4) Δεν είχε δοθεί δυνατότητα θέασης περισσότερων πληροφοριών από τις απολύτως απαραίτητες επικαιροποιημένες υπηρεσιακές πληροφορίες. Η θέαση της φωτογραφίας κρίθηκε απαραίτητη για σκοπούς ταυτοποίησης.
(5) Δεν υπήρξε οποιοσδήποτε δόλος ή αμέλεια από πλευράς Εταιρείας ή Σωματείου.
(6) Δεν υπήρξε παράνομη απώλεια ή αντιγραφή ή κοινολόγηση δεδομένων σε μη εξουσιοδοτημένα άτομα. Τα 9 άτομα του Σωματείου που είχαν πρόσβαση είχαν εξουσιοδοτηθεί με σχετική συμφωνία.
(7) Δεν υπήρξε ανεξουσιοδότητη πρόσβαση σε δεδομένα προσωπικού χαρακτήρα.
(8) Δεν συντελέστηκε διασύνδεση βάσεων δεδομένων, ούτε οποιαδήποτε επεξεργασία με την χρήση κάποιου λογισμικού.
(9) Δεν υποβλήθηκε οποιοδήποτε παράπονο στο παρελθόν. Το 98% των υπαλλήλων της Εταιρείας είναι και μέλη του Σωματείου. Τόσο η Εταιρεία όσο και το Σωματείο είναι ταγμένα να εξυπηρετούν τους υπαλλήλους και τους συνταξιούχους της Εταιρείας.
(10) Κατόπιν τεχνικής υποστήριξης, διευθετήθηκε όπως τερματιστεί η δυνατότητα θέασης στο 2% των υπαλλήλων που δεν ήταν μέλη του Σωματείου. Τα εξουσιοδοτημένα άτομα για θέαση, περιορίστηκαν σε 1 από 9 που ήταν αρχικά.

(γ) Λέχθηκε τέλος, πως ο κύκλος εργασιών της Εταιρείας, σύμφωνα με τις αναρτημένες και ελεγμένες οικονομικές καταστάσεις του 2018, ανερχόταν σε €343.559.000 (τριακόσια σαράντα τρία εκατομμύρια και πεντακόσιες πενήντα εννέα χιλιάδες ευρώ).

Νομικό Πλαίσιο

2.1. Άρθρο 4 - Ορισμοί:

««δεδομένα προσωπικού χαρακτήρα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο **(«υποκείμενο των δεδομένων»)**· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.».

««επεξεργασία»: κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε

σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.».

««σύστημα αρχειοθέτησης»: κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση.».

««υπεύθυνος επεξεργασίας»: 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.».

2.2. Άρθρο 5 – Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα

Ο Κανονισμός επιβάλλει τα προσωπικά δεδομένα που τυγχάνουν επεξεργασίας να είναι σύμφωνα με τις αρχές του άρθρου 5 του Κανονισμού.

Συγκεκριμένα**:**

2.2.1. Η παράγραφος 1(α) του άρθρου 5 του Κανονισμού προβλέπει ότι τα προσωπικά δεδομένα:

«υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων (νομιμότητα, αντικειμενικότητα και διαφάνεια»)».

2.2.2. Η παράγραφος 1(β) του άρθρου 5 του Κανονισμού προβλέπει ότι τα προσωπικά δεδομένα:

«συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 («περιορισμός του σκοπού»).

2.2.3. Η παράγραφος 1(γ) του άρθρου 5 του Κανονισμού προβλέπει ότι τα προσωπικά δεδομένα:

«είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»).

2.2.4. Η παράγραφος 1(στ) του άρθρου 5 του Κανονισμού προβλέπει ότι τα προσωπικά δεδομένα:

«υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»)».

2.2.5. Επιπρόσθετα, η παράγραφος 2 του ίδιου άρθρου προβλέπει ότι**:**

«Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 («λογοδοσία»)».

2.2.6. Ο Κανονισμός έχει αναδείξει την αρχή της «ακεραιότητας και εμπιστευτικότητας» σε βασική αρχή επεξεργασίας των προσωπικών δεδομένων[1] ώστε με την εφαρμογή των «κατάλληλων τεχνικών και οργανωτικών μέτρων», να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση ή χρήση των δεδομένων και του εξοπλισμού που χρησιμοποιείται για την επεξεργασία (Αιτιολογική Σκέψη 39 του Κανονισμού και Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών-ENISA[2]).

2.2.7. Συνεπώς, όταν η επεξεργασία που πρόκειται να πραγματοποιηθεί, λάβει χώρα κατά τρόπο που δεν εγγυάται την ενδεδειγμένη ασφάλεια, είναι περιττή η εξέταση της πλήρωσης των αρχών που προβλέπονται στο άρθρο 5(1) του Κανονισμού, αφού η επεξεργασία δεν θα είναι ασφαλής και άρα θα είναι παράνομη.

2.2.8. Σύμφωνα με την Απόφαση της Ελληνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα με αρ. 44/2019:

«Η ύπαρξη κατάλληλων εγγράφων πολιτικών, εγκεκριμένων από τη διοίκηση ενός φορέα (υπεύθυνου ή εκτελούντα την επεξεργασία) που εφαρμόζονται και υλοποιούνται στην πράξη (a contrario ΑΠΔΠΧ 98/2013 παρ. 5), συνιστά βασικό κριτήριο για την απόδειξη της συμμόρφωσης προς την αρχή της ακεραιότητας και εμπιστευτικότητας, στο βαθμό που απουσιάζουν άλλου είδους αποδείξεις όπως η τήρηση εγκεκριμένου κώδικα δεοντολογίας ή εγκεκριμένου μηχανισμού πιστοποίησης.»

2.2.9. Η επεξεργασία προσωπικών δεδομένων με διαφανή τρόπο αποτελεί στοιχείο της αρχής της θεμιτής επεξεργασίας και συνδέεται με την αρχή της λογοδοσίας, παρέχοντας το δικαίωμα στα υποκείμενα να ασκούν έλεγχο επί των δεδομένων τους καθιστώντας υπόλογους τους υπεύθυνους επεξεργασίας, σύμφωνα με τις Κατευθυντήριες Γραμμές για την διαφάνεια (Guidelines on transparency under Regulation 2016/679), ημερομηνίας 11.4.2018.

2.2.10. Κατ' εξαίρεση και κατ' εφαρμογή του άρθρου 14(5)(β) του Κανονισμού που αφορούν στις πληροφορίες που παρέχονται εάν τα προσωπικά δεδομένα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων, δεν εφαρμόζονται οι παράγραφοι 1-4

[1] XXXXX, σελ. 219, η οποία αναφέρει ότι «Η ασφάλεια είναι συνθήκη εκ των ων ουκ άνευ για την αποτελεσματική προστασία προσωπικών δεδομένων. Ωστόσο πρέπει, ήδη προκαταρκτικά, να επισημανθεί ότι πρόκειται για μια αναγκαία πλην όμως μη επαρκή συνθήκη για την προστασία των δεδομένων, καθώς η προστασία τους από μη εξουσιοδοτημένη πρόσβαση, αποκάλυψη και εν γένει χρήση δεν σημαίνει αυτονόητα ότι αποτελούν αντικείμενο νόμιμης επεξεργασίας». Επίσης βλέπε: Ο Γενικός Κανονισμός Προστασίας Δεδομένων, νέο δίκαιο - νέες υποχρεώσεις - νέα δικαιώματα, Σάκκουλας 2017, σελ. 108.

[2] "Handbook on Security of Personal Data Processing", Δεκέμβριος 2017, σελ. 8 και "Guidelines for SMEs on the security of personal data processing", Δεκέμβριος 2016 σελ. 12.

του ίδιου άρθρου και δεν παρέχονται από τον υπεύθυνο επεξεργασίας οι σχετικές πληροφορίες εφόσον είναι πιθανό να βλάψει σε μεγάλο βαθμό την επίτευξη των σκοπών της εν λόγω επεξεργασίας.

Προϋπόθεση εφαρμογής της εν λόγω διάταξης σύμφωνα με τις Κατευθυντήριες Γραμμές για την διαφάνεια (Guidelines on transparency under Regulation 2016/679) ημερομηνίας 11.4.2018, (παράγραφος 65), συνιστά η επεξεργασία των εν λόγω προσωπικών δεδομένων να συμμορφώνεται με όλες τις αρχές που προβλέπονται στο άρθρο 5 του Κανονισμού, ενώ το σημαντικότερο είναι ότι, σε όλες τις περιστάσεις, η επεξεργασία των προσωπικών δεδομένων είναι θεμιτή και έχει νομική βάση.
Συνεπώς, ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει από μόνος του τα αναγκαία μέτρα για συμμόρφωσή του με τις διατάξεις του Κανονισμού και παράλληλα έχει υποχρέωση να αποδεικνύει ανά πάσα στιγμή την συμμόρφωσή του στην Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

2.2.11. Η αιτιολογική σκέψη 50 του Κανονισμού αναφέρει ότι:

«Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς άλλους από εκείνους για τους οποίους τα δεδομένα προσωπικού χαρακτήρα συλλέχθηκαν αρχικά θα πρέπει να επιτρέπεται μόνο εφόσον η επεξεργασία είναι συμβατή με τους σκοπούς για τους οποίους τα δεδομένα προσωπικού χαρακτήρα συλλέχθηκαν αρχικά. Σε αυτήν την περίπτωση, δεν απαιτείται νομική βάση χωριστή από εκείνη που επέτρεψε τη συλλογή των δεδομένων προσωπικού χαρακτήρα .....
Για να εξακριβωθεί αν ο σκοπός της περαιτέρω επεξεργασίας είναι συμβατός με τον σκοπό της αρχικής συλλογής των δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας, εφόσον πληροί όλες τις απαιτήσεις για τη νομιμότητα της αρχικής επεξεργασίας, θα πρέπει να λάβει υπόψη, μεταξύ άλλων: τυχόν συνδέσμους μεταξύ των σκοπών αυτών και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας· το πλαίσιο στο οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα, ιδίως τις εύλογες προσδοκίες του υποκειμένου των δεδομένων βάσει της σχέσης του με τον υπεύθυνο επεξεργασίας ως προς την περαιτέρω χρήση τους· τη φύση των δεδομένων προσωπικού χαρακτήρα· τις συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων· και την ύπαρξη κατάλληλων εγγυήσεων τόσο για τις αρχικές όσο και τις σκοπούμενες πράξεις περαιτέρω επεξεργασίας. Όταν το υποκείμενο των δεδομένων παρέσχε τη συναίνεσή του ή η επεξεργασία βασίζεται στο δίκαιο της Ένωσης ή κράτους μέλους που συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση, ειδικότερα, σημαντικών σκοπών στο πλαίσιο γενικού δημόσιου συμφέροντος, θα πρέπει να επιτρέπεται στον υπεύθυνο επεξεργασία να προβαίνει στην περαιτέρω επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ανεξάρτητα από τη συμβατότητα των σκοπών. Σε κάθε περίπτωση, θα πρέπει να διασφαλίζεται η εφαρμογή των αρχών που καθορίζονται στον παρόντα κανονισμό και, ιδίως, η ενημέρωση του υποκειμένου των δεδομένων σχετικά με τους άλλους αυτούς σκοπούς και σχετικά με τα δικαιώματά του, συμπεριλαμβανομένου του δικαιώματος προβολής αντιρρήσεων.».

2.2.12. Ο Κανονισμός υιοθέτησε την αρχή της λογοδοσίας ως μέτρο συμμόρφωσης, με βάση την οποία, ο υπεύθυνος επεξεργασίας έχει υποχρέωση να σχεδιάζει, να εφαρμόζει και να λαμβάνει τα αναγκαία μέτρα και πολιτικές ούτως ώστε η επεξεργασία των δεδομένων να είναι σύμφωνη με διατάξεις του Κανονισμού.

Επιπλέον, ο υπεύθυνος επεξεργασίας βαρύνεται με το περαιτέρω καθήκον να αποδεικνύει από μόνος του και ανά πάσα στιγμή τη συμμόρφωσή του με τις αρχές του άρθρου 5(1) του Κανονισμού.

Ο Κανονισμός συνεπώς μεταθέτει το «βάρος τη απόδειξης» ως προς τη νομιμότητα της επεξεργασίας (περιλαμβανομένης της τήρησης των αρχών) στον υπεύθυνο επεξεργασίας.

2.2.13. Χρήσιμο εργαλείο αποτελεί και η Γνώμη με αρ. 3/2010 της Ομάδας Εργασίας του άρθρου 29, σχετικά με την αρχή της λογοδοσίας, ημερομηνίας 13.7.2010, για τα διεθνή πρότυπα που εγκρίθηκαν στη Μαδρίτη από τις αρμόδιες αρχές προστασίας των δεδομένων προσωπικού χαρακτήρα.

Σύμφωνα με την εν λόγω Γνώμη, η Ομάδα Εργασίας συνέστησε όπως κατάλληλα μέτρα λογοδοσίας για την τήρηση των αρχών του άρθρου 5(1) του Κανονισμού μπορούν να περιλαμβάνουν: θέσπιση εσωτερικών διαδικασιών πριν την δημιουργία νέων εργασιών επεξεργασίας, θέσπιση γραπτών και δεσμευτικών πολιτικών προστασίας δεδομένων διαθέσιμες στα πρόσωπα στα οποία αναφέρονται τα δεδομένα, χαρτογράφηση των διαδικασιών, διατήρηση καταλόγου όλων των εργασιών επεξεργασίας δεδομένων, διορισμός υπευθύνου για την προστασία των δεδομένων και άλλων προσώπων με ευθύνη για την προστασία των δεδομένων, παροχή κατάλληλης εκπαίδευσης και κατάρτισης στους υπαλλήλους στην προστασία των δεδομένων, θέσπιση διαδικασιών για την διαχείριση των αιτημάτων πρόσβαση, διόρθωσης και διαγραφής, η οποία πρέπει να είναι διαφανής για τα άτομα στα οποία αναφέρονται τα δεδομένα, εγκαθίδρυση εσωτερικού μηχανισμού χειρισμού καταγγελιών, θέσπιση εσωτερικών διαδικασιών για την αποτελεσματική διαχείριση και αναφορά παραβιάσεων ασφαλείας, διενέργεια αξιολόγησης του αντικτύπου στην ιδιωτική ζωή σε ειδικές περιπτώσεις, εφαρμογή και επίβλεψη διαδικασιών επαλήθευσης, ώστε να διασφαλίζεται ότι όλα τα μέτρα όχι μόνον υπάρχουν στα χαρτιά, αλλά εφαρμόζονται και λειτουργούν στην πράξη (εσωτερικοί ή εξωτερικοί έλεγχοι κ.λπ.).

2.3. Άρθρο 6 – Νομιμότητα της επεξεργασίας

2.3.1. Σύμφωνα με τις διατάξεις του άρθρου 6 του Κανονισμού, που αφορούν στη νομιμότητα της επεξεργασίας:

«1. Η επεξεργασία είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:

α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,

γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,

δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,

ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,

στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Το στοιχείο στ) του πρώτου εδαφίου δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους.

2. Τα κράτη μέλη μπορούν να διατηρούν ή να θεσπίζουν πιο ειδικές διατάξεις για την προσαρμογή της εφαρμογής των κανόνων του παρόντος κανονισμού όσον αφορά την επεξεργασία για τη συμμόρφωση με την παράγραφο 1 στοιχεία γ) και ε), καθορίζοντας ακριβέστερα ειδικές απαιτήσεις για την επεξεργασία και άλλα μέτρα προς εξασφάλιση σύννομης και θεμιτής επεξεργασίας, μεταξύ άλλων για άλλες ειδικές περιπτώσεις επεξεργασίας όπως προβλέπονται στο κεφάλαιο IX.

3. Η βάση για την επεξεργασία που αναφέρεται στην παράγραφο 1 στοιχεία γ) και ε) ορίζεται σύμφωνα με:

α) το δίκαιο της Ένωσης, ή

β) το δίκαιο του κράτους μέλος στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας.

Ο σκοπός της επεξεργασίας καθορίζεται στην εν λόγω νομική βάση ή, όσον αφορά την επεξεργασία που αναφέρεται στην παράγραφο 1 στοιχείο ε), είναι η αναγκαιότητα της επεξεργασίας για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.

Η εν λόγω νομική βάση μπορεί να περιλαμβάνει ειδικές διατάξεις για την προσαρμογή της εφαρμογής των κανόνων του παρόντος κανονισμού, μεταξύ άλλων: τις γενικές προϋποθέσεις που διέπουν τη σύννομη επεξεργασία από τον υπεύθυνο επεξεργασίας· τα είδη των δεδομένων που υποβάλλονται σε επεξεργασία· τα οικεία υποκείμενα των δεδομένων· τις οντότητες στις οποίες μπορούν να κοινοποιούνται τα δεδομένα προσωπικού χαρακτήρα και τους σκοπούς αυτής της κοινοποίησης· τον περιορισμό του σκοπού· τις περιόδους αποθήκευσης· και τις πράξεις επεξεργασίας και τις διαδικασίες επεξεργασίας, συμπεριλαμβανομένων των μέτρων για τη διασφάλιση σύννομης και θεμιτής επεξεργασίας, όπως εκείνα για άλλες ειδικές περιπτώσεις επεξεργασίας όπως προβλέπονται στο κεφάλαιο IX.

Το δίκαιο της Ένωσης ή το δίκαιο του κράτους μέλους ανταποκρίνεται σε σκοπό δημόσιου συμφέροντος και είναι ανάλογο προς τον επιδιωκόμενο νόμιμο σκοπό.

4. Όταν η επεξεργασία για σκοπό άλλο από αυτόν για τον οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα δεν βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων ή στο δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους το οποίο αποτελεί αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση των σκοπών που αναφέρονται στο άρθρο 23 παράγραφος 1, ο υπεύθυνος επεξεργασίας, προκειμένου να εξακριβωθεί κατά πόσο η επεξεργασία για

άλλο σκοπό είναι συμβατή με τον σκοπό για τον οποίο συλλέγονται αρχικώς τα δεδομένα προσωπικού χαρακτήρα, λαμβάνει υπόψη, μεταξύ άλλων:

α) τυχόν σχέση μεταξύ των σκοπών για τους οποίους έχουν συλλεχθεί τα δεδομένα προσωπικού χαρακτήρα και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας,

β) το πλαίσιο εντός του οποίου συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα, ιδίως όσον αφορά τη σχέση μεταξύ των υποκειμένων των δεδομένων και του υπευθύνου επεξεργασίας,

γ) τη φύση των δεδομένων προσωπικού χαρακτήρα, ιδίως για τις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, σύμφωνα με το άρθρο 9, ή κατά πόσο δεδομένα προσωπικού χαρακτήρα που σχετίζονται με ποινικές καταδίκες και αδικήματα υποβάλλονται σε επεξεργασία, σύμφωνα με το άρθρο 10,

δ) τις πιθανές συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων,

ε) την ύπαρξη κατάλληλων εγγυήσεων, που μπορεί να περιλαμβάνουν κρυπτογράφηση ή ψευδωνυμοποίηση.».

2.3.2. Η αιτιολογική σκέψη 44 του Κανονισμού, αναφέρει τα κάτωθι αναφορικά με το άρθρο 6(1)(β) του Κανονισμού:

«Η επεξεργασία θα πρέπει επίσης να είναι σύννομη εφόσον είναι αναγκαία στο πλαίσιο σύμβασης ή πρόθεσης σύναψης.».

2.3.3. Αναφορικά με το άρθρο 6(4) του Κανονισμού, η αιτιολογική σκέψη 50 του Κανονισμού συμπληρώνει ότι:

«Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς άλλους από εκείνους για τους οποίους τα δεδομένα προσωπικού χαρακτήρα συλλέχθηκαν αρχικά θα πρέπει να επιτρέπεται μόνο εφόσον η επεξεργασία είναι συμβατή με τους σκοπούς για τους οποίους τα δεδομένα προσωπικού χαρακτήρα συλλέχθηκαν αρχικά. Σε αυτήν την περίπτωση, δεν απαιτείται νομική βάση χωριστή από εκείνη που επέτρεψε τη συλλογή των δεδομένων προσωπικού χαρακτήρα.
.....
Η νομική βάση που προβλέπεται από το δίκαιο της Ένωσης ή κράτους μέλους για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα μπορεί επίσης να συνιστά τη νομική βάση για την περαιτέρω επεξεργασία. Για να εξακριβωθεί αν ο σκοπός της περαιτέρω επεξεργασίας είναι συμβατός με τον σκοπό της αρχικής συλλογής των δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας, εφόσον πληροί όλες τις απαιτήσεις για τη νομιμότητα της αρχικής επεξεργασίας, θα πρέπει να λάβει υπόψη, μεταξύ άλλων: τυχόν συνδέσμους μεταξύ των σκοπών αυτών και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας· το πλαίσιο στο οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα, ιδίως τις εύλογες προσδοκίες του υποκειμένου των δεδομένων βάσει της σχέσης του με τον υπεύθυνο επεξεργασίας ως προς την περαιτέρω χρήση τους· τη φύση των δεδομένων προσωπικού χαρακτήρα· τις συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων· και την ύπαρξη κατάλληλων εγγυήσεων τόσο για τις αρχικές όσο και τις σκοπούμενες πράξεις περαιτέρω επεξεργασίας. Όταν το υποκείμενο των δεδομένων παρέσχε τη συναίνεσή του ή η επεξεργασία βασίζεται στο δίκαιο της Ένωσης ή κράτους μέλους που συνιστά αναγκαίο και αναλογικό μέτρο

σε μια δημοκρατική κοινωνία για τη διασφάλιση, ειδικότερα, σημαντικών σκοπών στο πλαίσιο γενικού δημόσιου συμφέροντος, θα πρέπει να επιτρέπεται στον υπεύθυνο επεξεργασία να προβαίνει στην περαιτέρω επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ανεξάρτητα από τη συμβατότητα των σκοπών. Σε κάθε περίπτωση, θα πρέπει να διασφαλίζεται η εφαρμογή των αρχών που καθορίζονται στον παρόντα κανονισμό και, ιδίως, η ενημέρωση του υποκειμένου των δεδομένων σχετικά με τους άλλους αυτούς σκοπούς και σχετικά με τα δικαιώματά του, συμπεριλαμβανομένου του δικαιώματος προβολής αντιρρήσεων.».

2.4. Άρθρα 13 και 14 – Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων και Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων *(ενημέρωση των υποκειμένων των δεδομένων)*

2.4.1. Σύμφωνα με την αιτιολογική σκέψη 39 του Κανονισμού**:**

«Κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σύννομη και δίκαιη. Θα πρέπει να είναι σαφές για τα φυσικά πρόσωπα ότι δεδομένα προσωπικού χαρακτήρα που τα αφορούν συλλέγονται, χρησιμοποιούνται, λαμβάνονται υπόψη ή υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία, καθώς και σε ποιο βαθμό τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται ή θα υποβληθούν σε επεξεργασία. Η αρχή αυτή απαιτεί κάθε πληροφορία και ανακοίνωση σχετικά με την επεξεργασία των εν λόγω δεδομένων προσωπικού χαρακτήρα να είναι εύκολα προσβάσιμη και κατανοητή και να χρησιμοποιεί σαφή και απλή γλώσσα. Αυτή η αρχή αφορά ιδίως την ενημέρωση των υποκειμένων των δεδομένων σχετικά με την ταυτότητα του υπευθύνου επεξεργασίας και τους σκοπούς της επεξεργασίας και την περαιτέρω ενημέρωση ώστε να διασφαλιστεί δίκαιη και διαφανής επεξεργασία σε σχέση με τα εν λόγω φυσικά πρόσωπα και το δικαίωμά τους να λαμβάνουν επιβεβαίωση και να επιτυγχάνουν ανακοίνωση των σχετικών με αυτά δεδομένων προσωπικού χαρακτήρα που υπόκεινται σε επεξεργασία. Θα πρέπει να γνωστοποιείται στα φυσικά πρόσωπα η ύπαρξη κινδύνων, κανόνων, εγγυήσεων και δικαιωμάτων σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και πώς να ασκούν τα δικαιώματά τους σε σχέση με την επεξεργασία αυτή. Ιδίως, οι συγκεκριμένοι σκοποί της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σαφείς, νόμιμοι και προσδιορισμένοι κατά τον χρόνο συλλογής των δεδομένων προσωπικού χαρακτήρα. Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να είναι επαρκή και συναφή και να περιορίζονται στα αναγκαία για τους σκοπούς της επεξεργασίας τους. Αυτό απαιτεί ειδικότερα να διασφαλίζεται ότι το διάστημα αποθήκευσης των δεδομένων προσωπικού χαρακτήρα να περιορίζεται στο ελάχιστο δυνατό .... 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 η χρήση αυτών των δεδομένων προσωπικού χαρακτήρα και του εν λόγω εξοπλισμού.».

2.4.2. Η αιτιολογική σκέψη 60 του Κανονισμού ορίζει τα εξής:

«Οι αρχές της δίκαιης και διαφανούς επεξεργασίας απαιτούν να ενημερώνεται το υποκείμενο των δεδομένων για την ύπαρξη της πράξης επεξεργασίας και τους σκοπούς της. Ο υπεύθυνος επεξεργασίας θα πρέπει να παρέχει στο υποκείμενο των δεδομένων κάθε περαιτέρω πληροφορία που είναι αναγκαία για τη διασφάλιση

δίκαιης και διαφανούς επεξεργασίας λαμβάνοντας υπόψη τις ειδικές συνθήκες και το πλαίσιο εντός του οποίου πραγματοποιείται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα».

2.4.3. Αναφορικά με την ενημέρωση των υποκειμένων των δεδομένων, η αιτιολογική σκέψη 61 του Κανονισμού συμπληρώνει ότι:

«Οι πληροφορίες σε σχέση με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που σχετίζονται με το υποκείμενο των δεδομένων θα πρέπει να του παρέχονται κατά τη συλλογή από το υποκείμενο των δεδομένων ή, εάν τα δεδομένα προσωπικού χαρακτήρα λαμβάνονται από άλλη πηγή, εντός εύλογης προθεσμίας, ανάλογα με τις συνθήκες κάθε περίπτωσης. Εάν τα δεδομένα προσωπικού χαρακτήρα επιτρέπεται να κοινολογηθούν σε άλλον αποδέκτη, το υποκείμενο των δεδομένων θα πρέπει να ενημερώνεται, όταν τα δεδομένα προσωπικού χαρακτήρα κοινολογούνται για πρώτη φορά στον αποδέκτη.....».

2.5. Άρθρο 24 – Ευθύνη του υπεύθυνου επεξεργασίας

«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.».

2.6. Άρθρο 32 – Ασφάλεια επεξεργασίας

2.6.1. Οι υποχρεώσεις του υπευθύνου επεξεργασίας σχετικά με την ασφάλεια της επεξεργασίας προσδιορίζονται ρητά στο άρθρο 32 Κανονισμού, το οποίο προβλέπει ότι:

«1. Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:»

«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.».

2.6.2. Στην παράγραφο 2 του ίδιου άρθρου, αναφέρεται ότι:

«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».

2.6.3. Σύμφωνα με το τελευταίο εδάφιο της αιτιολογικής σκέψης 39 του Κανονισμού:

«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 η χρήση αυτών των δεδομένων προσωπικού χαρακτήρα και του εν λόγω εξοπλισμού.».

2.6.4. Η αιτιολογική σκέψη 74 του Κανονισμού αναφέρει ότι:

«Θα πρέπει να θεσπιστεί ευθύνη και υποχρέωση αποζημίωσης του υπευθύνου επεξεργασίας για οποιαδήποτε επεξεργασία δεδομένων προσωπικού χαρακτήρα που γίνεται από τον υπεύθυνο επεξεργασίας ή για λογαριασμό του υπευθύνου επεξεργασίας. Ειδικότερα, ο υπεύθυνος επεξεργασίας θα πρέπει να υποχρεούται να υλοποιεί κατάλληλα και αποτελεσματικά μέτρα και να είναι σε θέση να αποδεικνύει τη συμμόρφωση των δραστηριοτήτων επεξεργασίας με τον παρόντα κανονισμό, συμπεριλαμβανομένης της αποτελεσματικότητας των μέτρων. Τα εν λόγω μέτρα θα πρέπει να λαμβάνουν υπόψη τη φύση, το πλαίσιο, το πεδίο εφαρμογής και τους σκοπούς της επεξεργασίας και τον κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.».

2.6.5. Σύμφωνα με την Αιτιολογική Σκέψη 78 του Κανονισμού:

«Η προστασία των δικαιωμάτων και των ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα απαιτεί τη λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων ώστε να διασφαλίζεται ότι τηρούνται οι απαιτήσεις του παρόντος κανονισμού. Προκειμένου να μπορεί να αποδείξει συμμόρφωση προς τον παρόντα κανονισμό, ο υπεύθυνος επεξεργασίας θα πρέπει να θεσπίζει εσωτερικές πολιτικές και να εφαρμόζει μέτρα τα οποία ανταποκρίνονται ειδικότερα στις αρχές της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού».

2.6.6. Αναφορικά με το άρθρο 32 του Κανονισμού, η αιτιολογική σκέψη 83 του Κανονισμού συμπληρώνει ότι:

«Για τη διατήρηση της ασφάλειας και την αποφυγή της επεξεργασίας κατά παράβαση του παρόντος κανονισμού, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία θα πρέπει να αξιολογεί τους κινδύνους που ενέχει η επεξεργασία και να εφαρμόζει μέτρα για το μετριασμό των εν λόγω κινδύνων, όπως για παράδειγμα μέσω κρυπτογράφησης. Τα εν λόγω μέτρα θα πρέπει να διασφαλίζουν κατάλληλο επίπεδο ασφάλειας, πράγμα που περιλαμβάνει και την εμπιστευτικότητα...Κατά την εκτίμηση του κινδύνου για την ασφάλεια των δεδομένων θα πρέπει να δίνεται προσοχή στους

κινδύνους που προκύπτουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα...».

2.6.7. Επιπρόσθετα, η Αιτιολογική Σκέψη 87 του Κανονισμού προβλέπει ότι:

«Θα πρέπει να εξακριβώνεται κατά πόσον έχουν τεθεί σε εφαρμογή όλα τα κατάλληλα μέτρα τεχνολογικής προστασίας και οργανωτικά μέτρα για τον άμεσο εντοπισμό κάθε παραβίασης δεδομένων προσωπικού χαρακτήρα και την άμεση ενημέρωση της εποπτικής αρχής και του υποκειμένου των δεδομένων», όπως αναλυτικά αναφέρονται στις από 06-02-2018 Κατευθυντήριες Γραμμές της Ομάδας Εργασίας του Άρθρου 29, ημερομηνίας 06.02.2018 αναφορικά με την γνωστοποίηση παραβίασης δεδομένων.

2.6.8. Σύμφωνα με την Απόφαση με αριθμό 186/2014 της Ελληνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στο μέρος «Δ. Μέτρα ασφάλειας – Τεχνικά μέτρα διαχωρισμού εφαρμογών», ουσιώδες στοιχείο της νόμιμης λειτουργίας πληροφοριακών συστημάτων και άλλων υποδομών κατά την επεξεργασία προσωπικών δεδομένων είναι η λήψη των κατάλληλων μέτρων ασφαλείας, ιδίως μέτρων φυσικού και λογικού διαχωρισμού του υλικού, του λογισμικού και των δεδομένων.

Ακολουθεί σχετικό απόσπασμα:

«Λογικός διαχωρισμός υπάρχει όταν το λογισμικό, όλων των επιπέδων, που χρησιμοποιείται για πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που τηρούνται για την ικανοποίηση ενός συγκεκριμένου σκοπού είναι διακριτό και λογικά απομονωμένο από το λογισμικό που χρησιμοποιείται για πρόσβαση σε δεδομένα που τηρούνται για άλλους σκοπούς. Τούτο χωρίς να απαιτείται η υλική υποδομή που χρησιμοποιείται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα ενός συγκεκριμένου σκοπού να είναι φυσικά διαχωρισμένη από τα υπόλοιπα δεδομένα ....».

2.7. Αποφάσεις

2.7.1. Με Απόφαση του ημερομηνίας 17.7.2009 *(αρ. προσφυγής 20511/2003, παρ. 37 - 46)*, το Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου στην υπόθεση *I. κατά Φινλανδίας*, εξέτασε κατά πόσον ο υπεύθυνος επεξεργασίας διασφάλισε την ασφάλεια των προσωπικών δεδομένων και διαπίστωσε παραβίαση του άρθρου 8 της Ευρωπαϊκής Σύμβασης για τα Δικαιώματα του Ανθρώπου, από την μη εφαρμογή μέτρων ασφαλείας που οδήγησαν στην άνευ δικαιώματος πρόσβαση σε αυτά.

2.7.2. Χρήσιμη παραπομπή μπορεί να γίνει και στα πιο κάτω αποσπάσματα της Ελληνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα:

Απόφαση Αρ. 98/2013

«Καταρχάς η ασφάλεια εξειδικεύεται σε τρεις βασικούς στόχους, ήτοι την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων, ενώ συμπληρωματικοί στόχοι, ιδίως από τη σκοπιά της προστασίας των προσωπικών δεδομένων, αποτελούν ιδίως η μη αποποίηση της ευθύνης (ή λογοδοσία) καθώς και ο διαχωρισμός των δεδομένων ανάλογα με το σκοπό της επεξεργασίας. Κατά τα διεθνώς αποδεκτά πρότυπα ασφάλειας πληροφοριακών συστημάτων (π.χ. βλ. σειρά ISO/IEC 27000) τα κατάλληλα μέτρα κατά το άρθρο 10 παρ. 3 ν. 2472/1997 εντάσσονται σε ένα Σύστημα Ασφάλειας Πληροφοριακών Συστημάτων (ISMS). Το εν

λόγω Σύστημα προϋποθέτει την εκπόνηση μελέτης επικινδυνότητας με βάση τους κινδύνους και τη φύση των δεδομένων, και μεταξύ άλλων περιλαμβάνει την κατάρτιση πολιτικής και σχεδίων ασφάλειας, όπου προσδιορίζονται συγκεκριμένα τεχνικά και οργανωτικά μέτρα. Τα μέτρα αυτά, εκτός του ότι πρέπει να εφαρμόζονται, επιπλέον παρακολουθούνται και αξιολογούνται με σκοπό τη διαρκή προσαρμογή τους στις επιχειρησιακές ανάγκες του υπευθύνου επεξεργασίας και στις τεχνολογικές εξελίξεις, τις οποίες οφείλει να λαμβάνει υπόψιν ο υπεύθυνος επεξεργασίας (βλ. άρθρο 17 παρ. 1 Οδηγία 95/46/ΕΚ).».

Απόφαση Αρ. 44/2019

«Εν όψει των ανωτέρω η Αρχή κρίνει ότι η ελεγχόμενη εταιρία AMPNI ως υπεύθυνος επεξεργασίας:

Αφενός, δεν εφάρμοσε το σύνολο των αρχών του άρθρου 5 παρ. 1 ΓΚΠΔ (*Γενικού Κανονισμού Προστασίας Δεδομένων)* και 6 παρ. 1 ΓΚΠΔ σχετικά με τη νομιμότητα της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα …… που λάμβανε χώρα στη χρησιμοποιούμενη υπολογιστική υποδομή …… αλλά και στο πλαίσιο κάθε μεταγενέστερης ή περαιτέρω επεξεργασίας των ίδιων δεδομένων προσωπικού χαρακτήρα, ούτε απέδειξε κατ' αρ. 5 παρ. 2 ΓΚΠΔ την τήρηση αυτών.

Αφετέρου, παραβίασε τις διατάξεις των άρθρων 5 παρ. 1 εδ. α' και στ' και παρ. 2 σε συνδυασμό με τα άρθρα 24 παρ. 1 και 2 και 32 παρ. 1 και 2 ΓΚΠΔ σχετικά με την αρχή της ασφαλούς επεξεργασίας (ιδίως της «εμπιστευτικότητας») των δεδομένων προσωπικού χαρακτήρα που λάμβανε χώρα στη χρησιμοποιούμενη υπολογιστική υποδομή …… από την μη λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων, αλλά και στο πλαίσιο κάθε μεταγενέστερης ή περαιτέρω επεξεργασίας των ίδιων δεδομένων προσωπικού χαρακτήρα, <u>ώστε να παρέλκει η εξέταση της τήρησης των αρχών επεξεργασίας των εδαφίων β', γ', δ' και ε' της παρ. 1 του άρθρου 5 καθώς και του άρθρου 6 παρ. 1 ΓΚΠΔ…».</u>

<u>3. Σκεπτικό</u>

3.1. <u>Ορισμοί</u>

3.1.1. Τα δεδομένα που τηρούνται από τους Καθ'ων την καταγγελία και αφορούν σε πρόσωπο εν ζωή συνιστούν **«δεδομένα προσωπικού χαρακτήρα».**

3.1.2. <u>Η πρόσβαση (όπως είναι η θέαση/προβολή των δεδομένων)</u>, χρήση, αναζήτηση, επιβεβαίωση/έλεγχος και συσχέτιση/συνδυασμός προσωπικών δεδομένων που τηρούνται σε βάση δεδομένων αποτελούν **επεξεργασία προσωπικών δεδομένων**, κατά την έννοια του άρθρου 4(2) του Κανονισμού.

3.1.3. Το αυτοματοποιημένο σύστημα που λειτουργεί και χρησιμοποιείται από την Εταιρεία και αφορά στους εργοδοτούμενους της συνιστά **«σύστημα αρχειοθέτησης»** βάσει του ορισμού στο άρθρο 4(6) του Κανονισμού.

3.1.4. **Υπεύθυνοι επεξεργασίας** είναι *η Εταιρεία και το Σωματείο* (άρθρο 4(7) του Κανονισμού) και αποτελούν δύο ξεχωριστούς υπεύθυνους επεξεργασίας.

3.1.5. **Υποκείμενα των δεδομένων** είναι *οι εργοδοτούμενοι της Εταιρείας που <u>δεν</u> είναι μέλη του Σωματείου και οι εργοδοτούμενοι της Εταιρείας που είναι μέλη του Σωματείου* (άρθρο 4(1) του Κανονισμού).

3.2. <u>Αρχές επεξεργασίας</u>

3.2.1. Τα προσωπικά δεδομένα για να τύχουν νόμιμης επεξεργασίας θα πρέπει να πληρούνται σωρευτικά οι προϋποθέσεις τήρησης των αρχών που διέπουν την επεξεργασία προσωπικών δεδομένων (άρθρο 5 του Κανονισμού), όπως εξάλλου προκύπτει και από την απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης ημερ. 16.01.2019 στην υπόθεση C-496/2017 XXXXX[3].

Σύμφωνα με την εν λόγω Απόφαση, η ύπαρξη ενός νόμιμου θεμελίου (άρθρου 6(1) του Κανονισμού) δεν απαλλάσσει τον υπεύθυνο επεξεργασίας από την υποχρέωση τήρησης των αρχών (άρθρο 5 του Κανονισμού).

3.2.2. Όπως σχετικά αναφέρει και ο XXXXX, Δικηγόρος, Μέλος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και Μέλος του Expert Group της Ε.Ε. για τον Κανονισμό 2016/679 και την Οδηγία 2016/680:

«**Σωρευτική πλήρωση προϋποθέσεων εφαρμογής και τήρησης αρχών αρ.5 παρ.1 και 6 ΓΚΠΔ *(Γενικός Κανονισμός Προστασίας Δεδομένων)***

• Η ύπαρξη ενός νόμιμου θεμελίου (αρ. 6 παρ.1 ΓΚΠΔ δεν απαλλάσσει τον υπ. Επ. *(υπεύθυνο επεξεργασίας)* από την υποχρέωση τήρησης των αρχών του άρ.5 παρ.1 ΓΚΠΔ. Η κατά παράβαση των αρχών του αρ.5 ΓΚΠΔ μη νόμιμη συλλογή και επεξεργασία δεν θεραπεύεται από την ύπαρξη νόμιμου σκοπού.

• Εάν παραβιάζεται μια από τις αρχές του άρθρου 5 παρ.1 ΓΚΠΔ (π.χ. θεμιτή και νόμιμη επεξεργασία, ασφάλεια) παρέλκει η εξέταση των λοιπών αρχών ή του άρθρου 6 παρ.1 ΓΚΠΔ.».[4]

3.2.3. Επιπλέον, **ο υπεύθυνος επεξεργασίας βαρύνεται με το περαιτέρω καθήκον να αποδεικνύει ανά πάσα στιγμή τη συμμόρφωση του με τις αρχές** που διέπουν την επεξεργασία προσωπικών δεδομένων, όπως εκτίθενται στο άρθρο 5 του Κανονισμού. **Συγκεκριμένα, η λογοδοσία εντάσσεται στις αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων και στην ουσία μεταθέτει στον υπεύθυνο επεξεργασίας «το βάρος της απόδειξης» της νομιμότητας της επεξεργασίας.**

3.2.4. Επιπλέον, το Δικαστήριο της Ευρωπαϊκής Ένωσης στην Απόφαση C-201/14 (XXXXX), ημερομηνίας 01.10.2015, έκρινε ως προϋπόθεση της θεμιτής και νόμιμης επεξεργασίας των προσωπικών δεδομένων την ενημέρωση του υποκειμένου των δεδομένων πριν την επεξεργασία αυτών.

---

[3] «57. Ωστόσο, κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να είναι σύμφωνη, αφενός προς τις αρχές που πρέπει να τηρούνται ως προς την ποιότητα των δεδομένων, τις οποίες θέτει το άρθρο 6 της οδηγίας 95/46 ή το άρθρο 5 του κανονισμού 2016/679 και, αφετέρου, προς τις βασικές αρχές της νόμιμης επεξεργασίας δεδομένων που απαριθμεί το άρθρο 7 της οδηγίας αυτής ή το άρθρο 6 του κανονισμού αυτού (Σχετικές αποφάσεις ...C-465/00, C-138/01, C-139/01, C-131/12».

[4] Βλέπε Απόφαση 517/2018 του Συμβουλίου της Επικράτειας της Ελληνικής Δημοκρατίας, παράγραφος 12 «…προκειμένου τα δεδομένα προσωπικού χαρακτήρα να τύχουν νόμιμης επεξεργασίας, απαιτείται σε κάθε περίπτωση να συντρέχουν σωρευτικά οι προϋποθέσεις του άρθρου 4 παρ. 1 του ν. 2472/1997, που μεταξύ άλλων, ορίζει ότι τα δεδομένα πρέπει να συλλέγονται και να υφίστανται επεξεργασία κατά τρόπο θεμιτό και νόμιμο, για σαφείς και νόμιμους σκοπούς.....Εφόσον συντρέχουν οι προϋποθέσεις του άρθρου 4 παρ. 1 του ν. 2472/1997 (νόμιμη συλλογή και επεξεργασία δεδομένων για σαφείς και νόμιμους σκοπούς), εξετάζεται περαιτέρω αν συντρέχουν και οι προϋποθέσεις της διατάξεως του άρθρου 5 παρ. 2 του ν. 2472/1997 [νομικές βάσεις]».

Ακολουθούν σχετικά αποσπάσματα:

«Ο υπεύθυνος της επεξεργασίας των δεδομένων ή ο εκπρόσωπος του υπέχουν υποχρέωση ενημερώσεως, το περιεχόμενο της οποίας ορίζεται στα άρθρα 10 και 11 της οδηγίας 95/46 και διαφέρει αναλόγως του αν τα δεδομένα συγκεντρώνονται από το πρόσωπο το οποίο αφορούν τα δεδομένα ή όχι, και τούτο υπό την επιφύλαξη των εξαιρέσεων που προβλέπει το άρθρο 13 της εν λόγω οδηγίας.».

«Συνεπώς, η απαίτηση περί θεμιτής επεξεργασίας δεδομένων την οποία προβλέπει το άρθρο 6 της οδηγίας 95/46 υποχρεώνει τη διοικητική αρχή να ενημερώνει τα πρόσωπα τα οποία αφορούν τα δεδομένα σχετικά με τη διαβίβαση των εν λόγω δεδομένων σε άλλη διοικητική αρχή προς τον σκοπό επεξεργασίας τους από τη δεύτερη ως αποδέκτρια των εν λόγω δεδομένων».

3.3. Άρθρα 13 και 14 – Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων και Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων *(ενημέρωση των υποκειμένων των δεδομένων)*

Οι Καθ' ων την καταγγελία όφειλαν να ενημερώσουν τα μέλη του Σωματείου ότι, το Σωματείο θα είχε πρόσβαση σε περισσότερα προσωπικά δεδομένα που τους αφορούσαν (φωτογραφία) από ότι ήταν αναγκαίο για να γίνει επιβεβαίωση των στοιχείων τους. Επιπλέον, όφειλαν όπως ενημερώσουν τους εργοδοτουμένους της Εταιρείας ότι, το Σωματείο θα είχε πρόσβαση σε προσωπικά δεδομένα που αφορούσαν στο άτομό τους.

3.4. Ευθύνη του υπεύθυνου επεξεργασίας (άρθρο 24 του Κανονισμού), προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (άρθρο 25 του Κανονισμού) και ασφάλεια της επεξεργασίας (άρθρο 32 του Κανονισμού)

3.4.1. Οι Καθ'ων την καταγγελία, στο πλαίσιο εφαρμογής του Κανονισμού, όφειλαν να τηρούν τις υποχρεώσεις τους σχετικά με την ασφάλεια και την γενικότερη ευθύνη τους για τον προσδιορισμό των κατάλληλων τεχνικών και οργανωτικών μέτρων, λαμβάνοντας ενδεδειγμένα μέτρα, τα οποία να μπορούν να τεκμηριώνονται σε επιμέρους διαδικασίες ή σε γενικότερες πολιτικές ασφαλείας[5].

3.4.2. Τέτοια ενδεδειγμένα τεχνικά και οργανωτικά μέτρα για την ασφάλεια της επεξεργασίας των προσωπικών δεδομένων στο πλαίσιο του Κανονισμού προτείνονται και από τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA).

3.4.3. Επιπρόσθετα, πριν τον καθορισμό των μέτρων ασφάλειας που επρόκειτο να υιοθετηθούν, οι Καθ'ων την καταγγελία όφειλαν να αξιολογήσουν τους κινδύνους και τις πιθανές συνέπειες τους για τα υποκείμενα των δεδομένων[6].

---

[5] Βλέπε ιστοσελίδα Ελληνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα www.dpa.gr, Ενότητα Ασφάλεια και ειδικότερα «Πολιτική Ασφαλείας, Σχέδιο Ασφαλείας και Σχέδιο Ανάκαμψης από Καταστροφές»).

[6] Βλέπε XXXXX, ειδικού επιστήμονα Ελληνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, «Ασφάλεια επεξεργασίας και γνωστοποίηση περιστατικών παραβίασης» σε Έκθεση Εθνικού Κέντρου Δημόσιας Διοίκησης και Αυτοδιοίκησης «ΓΚΠΔ: το νέο τοπίο και οι υποχρεώσεις της δημόσιας διοίκησης», Αθήνα, Ιανουάριος 2018, σελ. 20 (www.ekdd.gr/images/seminaria/GDPR.pdf).

3.4.4. Από το γράμμα και τον σκοπό των διατάξεων της αιτιολογικής σκέψης 83 του Κανονισμού είναι σαφές ότι, **η υποχρέωση τήρησης της ασφάλειας της επεξεργασίας από τον υπεύθυνο επεξεργασία έχει τόσο προληπτικό, όσο και κατασταλτικό χαρακτήρα.** Προληπτικό, ούτως ώστε τα εφαρμοστέα μέτρα να μπορούν να αποτρέπουν περιστατικά παραβίασης της ασφάλειας και κατασταλτικό, ούτως ώστε τυχόν περιστατικό να μπορεί να ανιχνευθεί και να διερευνηθεί.

3.4.5. Επίσης, τα υλοποιημένα μέτρα θα έπρεπε να επανεξετάζονταν και να επικαιροποιούνταν, όπως προβλέπεται στο άρθρο 24(1) του Κανονισμού.

4. Συμπεράσματα

Στην υπό εξέταση περίπτωση, από τα στοιχεία του φακέλου της υπόθεσης, έχω την άποψη ότι:

4.1. Η Εταιρεία δεν έλαβε τα αναγκαία τεχνικά και οργανωτικά μέτρα, ιδίως εκείνα που επιτάσσουν τον φυσικό και λογικό διαχωρισμό, με αποτέλεσμα το Σωματείο:

- Μέχρι τις 31 Μαρτίου 2020, είχε πρόσβαση για θέαση/προβολή προσωπικών δεδομένων υποκειμένων των δεδομένων που δεν συνδέονταν με το Σωματείο (μη μελών του) και

- είχε πρόσβαση σε περισσότερα προσωπικά δεδομένα μελών του (φωτογραφία) από ότι είναι αναγκαία για την πραγματοποίηση της απαιτούμενης επεξεργασίας *(επιβεβαίωση προσωπικών δεδομένων μελών)*, αλλά και από ότι ήταν συμφωνημένο με την μεταξύ τους Συμφωνία ημερομηνίας 15 Οκτωβρίου, 2018.

Ως εκ τούτου:

- προσωπικά δεδομένα μελών του Σωματείου υποβλήθηκαν σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τον αρχικό σκοπό της επεξεργασίας, **παραβιάζοντας την αρχή του περιορισμού του σκοπού (άρθρο 5(1)(β) του Κανονισμού)**,

- προσωπικά δεδομένα μη μελών του Σωματείου εξακολουθούσαν μέχρι και την 31.3.2020, να υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τον αρχικό σκοπό της επεξεργασίας, **παραβιάζοντας την αρχή του περιορισμού του σκοπού (άρθρο 5(1)(β) του Κανονισμού)**,

- το Σωματείο έχει πρόσβαση *(υπό τη μορφή θέασης/προβολής)* σε περισσότερα προσωπικά δεδομένα που αφορούν στα μέλη του (φωτογραφία), τα οποία όμως δεν είναι αναγκαία για την επιβεβαίωση των στοιχείων τους, **παραβιάζοντας την αρχή της ελαχιστοποίησης (άρθρο 5(1)(γ) του Κανονισμού),**

- Το Σωματείο είχε πρόσβαση σε προσωπικά δεδομένα εργοδοτουμένων της Εταιρείας που δεν ήταν μέλη του, **παραβιάζοντας την αρχή της ελαχιστοποίησης (άρθρο 5(1)(γ) του Κανονισμού),**

- προσωπικά δεδομένα των εργοδοτουμένων της Εταιρείας που δεν είναι μέλη του Σωματείου, υποβλήθηκαν σε επεξεργασία κατά τρόπο που δεν εγγυάται την ενδεδειγμένη ασφάλεια τους, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη πρόσβαση και έτσι επήλθε ο απειλούμενος

κίνδυνος για την εμπιστευτικότητα τους, **παραβιάζοντας την αρχή της ακεραιότητας και εμπιστευτικότητας (άρθρο 5(1)(στ) του Κανονισμού).**

- Το ίδιο ισχύει και για τα προσωπικά δεδομένα μελών του Σωματείου, στα οποία το Σωματείο εξακολουθεί να έχει πρόσβαση (φωτογραφία). Την 22 Ιουνίου, 2019 αναφέρθηκε πως θεωρούν απαραίτητη την φωτογραφία προς τον σκοπό ταυτοποίησης και επικοινωνίας μαζί με τα υποκείμενα των δεδομένων. Η θέση αυτή δεν συνάδει με την θέση την οποία προέβαλαν την 27 Απριλίου, 2020, ότι δηλαδή η εφαρμογή επέτρεπε στα εξουσιοδοτημένα άτομα του Σωματείου πρόσβαση για σκοπούς επιβεβαίωσης, πως ο υπάλληλος με τον αριθμό που καταχώρησαν είναι μέλος του Σωματείου. Πέραν του ότι το δεδομένο αυτό κρίνεται δυσανάλογο, αποτελεί και δεδομένο του οποίου η παραχώρηση πρόσβασης δεν είχε συμφωνηθεί, στην μεταξύ της Εταιρείας και Σωματείου Συμφωνία, ημερομηνίας 15 Οκτωβρίου, 2018. Σε κάθε περίπτωση, οι σκοποί για τους οποίους δινόταν η πρόσβαση στο Σωματείο, θα ικανοποιούντο ακόμη και εάν δεν υπήρχε πρόσβαση στην φωτογραφία του υπαλλήλου.

4.2. Ως εκ τούτου, **η επεξεργασία που διενεργείτο από τους Καθ'ων την καταγγελία ήταν αθέμιτη** αφού δεν τηρήθηκαν οι αρχές του περιορισμού του σκοπού, της ελαχιστοποίησης και της ακεραιότητας και εμπιστευτικότητας των δεδομένων.

4.3. Εν όψει των ανωτέρω, δεδομένου ότι, στην εξεταζόμενη υπόθεση, η επεξεργασία προσωπικών δεδομένων κρίνεται ήδη ως μη νόμιμη και παραβιάζουσα τις διατάξεις του άρθρου 5(1) του Κανονισμού σε συνδυασμό με τα άρθρα 24(1) – (2), 25(1) – (2) και 32 (1) – (2), παρέλκει η εξέταση του νόμιμου σκοπού και της νομικής βάσης της επεξεργασίας.

4.4. Οι Καθ'ων την καταγγελία, πριν τον καθορισμό των μέτρων ασφάλειας που επρόκειτο να υιοθετηθούν, δεν αξιολόγησαν τους κινδύνους και τις πιθανές συνέπειες τους στα δικαιώματα και στις ελευθερίες των υποκειμένων των δεδομένων, όπως εξάλλου προβλέπουν τα άρθρα 25 και 32 του Κανονισμού.

4.5. Οι Καθ'ων την καταγγελία, δεν εκπόνησαν οποιοδήποτε σχέδιο με σκοπό την εφαρμογή και παρακολούθηση τέτοιων μέτρων για τήρηση της ασφάλειας της επεξεργασίας με σκοπό τον εντοπισμό οποιωνδήποτε αδυναμιών/κενών. Ως εκ τούτου, το Σωματείο είχε πρόσβαση σε περισσότερα δεδομένα από ότι χρειαζόταν για να επιβεβαιώσει τα στοιχεία των μελών του (φωτογραφία) και παράλληλα είχε πρόσβαση σε δεδομένα μη μελών του.

4.6. Οι Καθ'ων την καταγγελία, δεν εφάρμοσαν τα δέοντα τεχνικά και οργανωτικά μέτρα ασφάλειας που να διασφαλίζουν ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα προσωπικά δεδομένα που ήταν απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Όπως αναφέρεται ρητά στο άρθρο 25(2) του Κανονισμού, η εν λόγω υποχρέωση των Καθ'ων την καταγγελία, ισχύει για το εύρος των δεδομένων που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητα τους. Στην προκειμένη περίπτωση, τα υλοποιημένα μέτρα δεν διασφάλιζαν ότι, εξ ορισμού, τα προσωπικά δεδομένα τύγχαναν επεξεργασίας μόνο από εξουσιοδοτημένα πρόσωπα, τηρώντας τις αρχές που καθορίζονται στο άρθρο 5 του Κανονισμού.

4.7. Συνεπώς, από τα ανωτέρω, διαπιστώνω ότι, η Εταιρεία:

4.7.1. Εξαρχής, δεν υιοθέτησε/υλοποίησε κατά τον ορθό και ενδεδειγμένο τρόπο τα κατάλληλα οργανωτικά και τεχνικά μέτρα ασφάλειας που να διασφαλίζουν ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για το σκοπό της επεξεργασίας που εκτελεί (άρθρο 25 του Κανονισμού),

4.7.2. κατά την εκτέλεση της επεξεργασίας, δεν υλοποίησε κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων (άρθρο 32 του Κανονισμού) και

4.7.3. δεν προέβηκε στην επανεξέταση/επικαιροποίηση των υφιστάμενων μέτρων ασφάλειας για εντοπισμό τυχόν αδυναμιών/κενών (άρθρο 24 του Κανονισμού), παρά μόνο αφότου ξεκίνησε η διαδικασία διερεύνησης του παρόντος παραπόνου, όπου και αποφασίστηκε ο τερματισμός της δυνατότητας θέασης στα δεδομένα του 2% μη μελών του Σωματείου, από την 31.3.2020 και μετά,

με επακόλουθο:
Την παροχή πρόσβασης στο Σωματείο σε προσωπικά δεδομένα μη μελών του μέχρι και την 31.3.2020, καθώς και σε περισσότερα προσωπικά δεδομένα (φωτογραφία) που αφορούσαν στα μέλη του τα οποία δεν ήταν αναγκαία για την πραγματοποίηση του απαιτούμενου σκοπού της επεξεργασίας *(δηλαδή την επιβεβαίωση των στοιχείων των μελών του),* παραβιάζοντας τις αρχές του περιορισμού του σκοπού, της ελαχιστοποίησης και της ακεραιότητας και εμπιστευτικότητας των δεδομένων (άρθρο 5 του Κανονισμού).

Επιπροσθέτως, η Εταιρεία:

4.7.4. Δεν σχεδίασε, κατάρτισε και εφάρμοσε, σε συμμόρφωση με τις διατάξεις του άρθρου 5(1) του Κανονισμού οποιοδήποτε μέτρο λογοδοσίας, όπως προβλέπεται στο άρθρο 5(2) του Κανονισμού, περιλαμβανομένων πολιτικών ασφάλειας προσωπικών δεδομένων, ούτε έλαβε μέτρα φυσικού διαχωρισμού των δεδομένων *(δηλαδή διαφορετικής βάσης δεδομένων)* ή και λογικού διαχωρισμού των δεδομένων *(δηλαδή τα είδη/κατηγορίες προσωπικών δεδομένων στα οποία παραχωρείται πρόσβαση)*.

4.7.5. Επίσης, η Εταιρεία δεν προσκόμισε στο Γραφείο μου οποιαδήποτε απόδειξη ότι:

(α) ενημέρωσε τα μέλη του Σωματείου ότι, το Σωματείο θα είχε πρόσβαση σε περισσότερα προσωπικά τους δεδομένα από ότι χρειαζόταν για να επιβεβαιώσει τα στοιχεία τους, όπως προβλέπεται στα άρθρα 13 και 14 του Κανονισμού,

(β) ενημέρωσε τους εργοδοτούμενους της ότι, το Σωματείο, ως ξεχωριστός υπεύθυνος επεξεργασίας, θα είχε πρόσβαση σε προσωπικά δεδομένα τους, όπως προβλέπεται στα άρθρα 13 και 14 του Κανονισμού.

4.8. Επιπλέον, από τα ανωτέρω, διαπιστώνω ότι, το Σωματείο:

4.8.1. Εξαρχής, δεν υιοθέτησε/εφάρμοσε κατά τον ορθό και ενδεδειγμένο τρόπο τα κατάλληλα οργανωτικά και τεχνικά μέτρα ασφάλειας που να διασφαλίζουν ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για το σκοπό της επεξεργασίας που εκτελεί (άρθρο 25 του Κανονισμού),

4.8.2. κατά την εκτέλεση της επεξεργασίας, δεν εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων (άρθρο 32 του Κανονισμού) και

4.8.3. δεν προέβηκε στην επανεξέταση/επικαιροποίηση των υφιστάμενων μέτρων ασφάλειας για εντοπισμό τυχόν αδυναμιών/κενών (άρθρο 24 του Κανονισμού), παρά μόνο αφότου ξεκίνησε η διαδικασία διερεύνησης του παρόντος παραπόνου, όπου και αποφασίστηκε ο τερματισμός της δυνατότητας θέασης στα δεδομένα του 2% μη μελών του Σωματείου, από την 31.3.2020 και μετά,

με επακόλουθο:
Την πρόσβαση από τη βάση δεδομένων της Εταιρείας σε προσωπικά δεδομένα μη μελών του μέχρι και την 31.3.2020, καθώς και σε περισσότερα προσωπικά δεδομένα που αφορούσαν στα μέλη του (φωτογραφία), τα οποία δεν ήταν αναγκαία για την πραγματοποίηση του απαιτούμενου σκοπού της επεξεργασίας (δηλαδή την επιβεβαίωση των στοιχείων των μελών του), παραβιάζοντας τις αρχές του περιορισμού του σκοπού, της ελαχιστοποίησης και της ακεραιότητας και εμπιστευτικότητας των δεδομένων (άρθρο 5 του Κανονισμού).

Επιπροσθέτως, το Σωματείο:

4.8.4. Δεν σχεδίασε, κατάρτισε και εφάρμοσε, σε συμμόρφωση προς τις διατάξεις του άρθρου 5(1) του Κανονισμού οποιοδήποτε μέτρο λογοδοσίας, όπως προβλέπεται στο άρθρο 5(2) του Κανονισμού, περιλαμβανομένων πολιτικών ασφάλειας προσωπικών δεδομένων που αφορούν ιδιαιτέρως στην ύπαρξη/διατήρηση ξεχωριστής βάσης δεδομένων από τη βάση δεδομένων της Εταιρείας.

4.8.5. Δεν προσκόμισε στο Γραφείο μου οποιαδήποτε απόδειξη ότι:

(α) ενημέρωσε τα μέλη του ότι, θα έχει πρόσβαση σε περισσότερα προσωπικά τους δεδομένα από ότι είναι απαραίτητο για να επιβεβαιώσει τα στοιχεία τους, όπως προβλέπεται στα άρθρα 13 και 14 του Κανονισμού,

(β) ενημέρωσε τους εργοδοτούμενους της Εταιρείας ότι, θα είχε πρόσβαση σε προσωπικά δεδομένα που τους αφορούν, όπως προβλέπεται στα άρθρα 13 και 14 του Κανονισμού.

4.9. Ενώ η Εταιρεία παραχωρούσε πρόσβαση στη βάση δεδομένων της στο Σωματείο, κατά παράβαση του ισχύοντος νομοθετικού πλαισίου, όπως λεπτομερώς αναφέρω στις παραγράφους 4.7.– 4.8.5. ανωτέρω, ουδέποτε ενημερώθηκα από τους Καθ'ων την καταγγελία για τη διενέργεια/διεξαγωγή τέτοιας επεξεργασίας ούτε και αυτόβουλα προέβηκαν στη διακοπή της,

παρά μόνο όταν τους απέστειλα σχετική επιστολή στις 25 Φεβρουαρίου 2020, αφότου έλαβα γραπτό παράπονο από εργοδοτούμενη στην Εταιρεία και μέλος του Σωματείου.

4.10. Ο ισχυρισμός της Εταιρείας ότι, ο λόγος που το Σωματείο δεν μπορεί να διατηρεί δική του βάση δεδομένων, ως ξεχωριστός υπεύθυνος επεξεργασίας *(παράγραφος 2.8. της απάντησης της Εταιρείας, η οποία στάληκε στο Γραφείο μου με ηλεκτρονικό μήνυμα στις 12.05.2020),* δεν ευσταθεί, ούτε έχει οποιαδήποτε νομική ισχύ, λαμβάνοντας υπόψη τις διατάξεις των άρθρων 25(1) και 32(1) του Κανονισμού που ορίζουν τα εξής:

Άρθρο 25(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.**».

Άρθρο 32(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**,....».

4.11. Ως εκ των ανωτέρω, η λήψη και η εφαρμογή των ενδεδειγμένων οργανωτικών και τεχνικών μέτρων ασφαλείας, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας ΔΕΝ αναιρεί το κόστος εφαρμογής της επεξεργασίας.

Αντιθέτως, βάσει των άρθρων 25 και 32 του Κανονισμού, ο υπεύθυνος επεξεργασίας έχει υποχρέωση να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα ήδη από το σχεδιασμό κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας. Η εκπλήρωση των υποχρεώσεων αυτών συνιστά χρήσιμο εργαλείο για τη σύννομη συμμόρφωση του καθώς ο σχεδιασμός διαδικασιών και συστημάτων εξαρχής με τη φιλοσοφία της προστασίας των προσωπικών δεδομένων, θα οδηγήσει στην αποτελεσματική διάγνωση και αντιμετώπιση προβλημάτων σε αρχικό επίπεδο και συνεπώς, να μειώσει την πιθανότητα επέλευσης κινδύνων από την επεξεργασία.

4.12. Η νομική βάση, στην οποία στηρίχθηκε το Σωματείο να προβαίνει σε επεξεργασία προσωπικών δεδομένων μη μελών του και σε επεξεργασία περισσότερων προσωπικών δεδομένων που αφορούσαν στα μέλη του, είναι οι διατάξεις του άρθρου 6(1)(α) και (β) του Κανονισμού, όπως σχετικά αναφέρουν οι Καθ'ων την καταγγελία στις επιστολές τους με ημερομηνίες 27 Μαρτίου 2020, 27 Απριλίου 2020 και 12 Μαΐου 2020.

4.12.1. Να σημειώσω ότι, καταρχήν, οι Καθ'ων την καταγγελία δεν προσκόμισαν οποιαδήποτε απόδειξη/μαρτυρία που να καταδεικνύει ότι, τα μέλη του Σωματείου είχαν συναινέσει/συγκατατεθεί στην επεξεργασία περισσότερων προσωπικών δεδομένων που τους αφορούν από ότι είναι αναγκαίο για να επιβεβαιωθούν τα στοιχεία τους από το Σωματείο, ούτε επίσης προσκόμισαν οποιαδήποτε απόδειξη/μαρτυρία που να καταδεικνύει ότι, τα μη μέλη του είχαν συναινέσει/συγκατατεθεί για επεξεργασία προσωπικών δεδομένων τους από το Σωματείο.

4.12.2. Το Έντυπο «Αίτηση για Εγγραφή Μέλους» που επισυνάφθηκε στην απάντηση των Καθ' ων την καταγγελία προς το Γραφείο μου, ημερομηνίας 12 Μαΐου

2020, ΔΕΝ αποτελεί συγκατάθεση των μελών για επεξεργασία των προσωπικών τους δεδομένων, πόσο μάλλον για επεξεργασία περισσότερων προσωπικών δεδομένων απ' ότι χρειάζεται (φωτογραφία) από το Σωματείο, όπως εσφαλμένα ισχυρίζονται στην επιστολή τους οι Καθ' ων την καταγγελία. Το έντυπο αυτό φέρει τον τίτλο «Αίτηση για Εγγραφή Μέλους», σύμφωνα με την οποία ο συμβαλλόμενος υπάλληλος υπογράφει «αίτηση για εγγραφή ως μέλους του Σωματείου» και δίδει συγκατάθεση για να κρατείται από το μισθό του η μηνιαία συνδρομή που έχει καθοριστεί από το Διοικητικό Συμβούλιο του Σωματείου. Ακολούθως υπάρχει χώρος για συμπλήρωση «στοιχείων αιτητή», τα οποία εν πάση περιπτώσει στοιχεία, δεν είναι συμβατά με τα στοιχεία για τα οποία είχε συναφθεί συμφωνία μεταξύ Εταιρείας και Σωματείου για ανταλλαγή. Σε κάθε περίπτωση όμως, το συγκεκριμένο έγγραφο δεν μπορεί να θεωρηθεί πως αποτελεί συγκατάθεση για επεξεργασία δεδομένων με την έννοια την οποία στηρίζουν οι Καθ' ων την Καταγγελία, αφού δεν πληρούνται οι πρόνοιες που απαιτεί ο Κανονισμός, σε σχέση με την παροχή των εν λόγω πληροφοριών από το υποκείμενο των δεδομένων (ενημέρωσης και ελεύθερης ρητής συγκατάθεσης για συγκεκριμένη επεξεργασία).

4.12.3. Επιπρόσθετα, οι διατάξεις του άρθρου 6(1)(β) του Κανονισμού δεν ισχύουν δεδομένου ότι, τα μη μέλη του Σωματείου δεν είχαν οποιαδήποτε σύμβαση με το Σωματείο. Όσον αφορά στα μέλη του Σωματείου, αυτά είχαν σύμβαση με δύο ξεχωριστούς υπεύθυνους επεξεργασίας που εξυπηρετούσαν δύο διαφορετικούς σκοπούς επεξεργασίας.

4.12.4. Εν πάση περιπτώσει, τονίζω ότι, ακόμα και σε περίπτωση ύπαρξης νομικής βάσης της εξεταζόμενης επεξεργασίας, δεδομένου ότι, εξαρχής η επεξεργασία που εκτελείτο από τους Καθ'ων την καταγγελία παραβίαζε τις αρχές της επεξεργασίας, όπως αυτές εκτίθενται στα άρθρα 5(1)(α), (β), (γ) και (στ) του Κανονισμού, η επεξεργασία καθίσταται παράνομη και παρέλκει η εξέταση της νομικής βάσης της επεξεργασίας.

4.13. Η σύναψη της Συμφωνίας ημερομηνίας 15 Οκτωβρίου, 2018, μεταξύ της Εταιρείας και του Σωματείου για ανταλλαγή προσωπικών δεδομένων, δεν έχει οποιαδήποτε νομική ισχύ, αφού η επεξεργασία που εκτελείται είναι εξαρχής παράνομη.

4.14. Η Εταιρεία παραδέχτηκε τη διενέργεια της εν λόγω παράνομης επεξεργασίας αφού:

4.14.1. Η XXXXX, με επιστολή της με Αρ. Φακ.: LGLK10-426 και με ημερομηνία 27 Μαρτίου 2020, μου ανέφερε, μεταξύ άλλων, τα κάτωθι:

(α) Το Σωματείο διατηρεί ηλεκτρονικό αρχείο με το Μητρώο Μελών Ταμείου, το οποίο επικαιροποιείται με άντληση πληροφοριών από τη βάση δεδομένων των Υπηρεσιών Προσωπικού της Εταιρείας με αυτόματο ηλεκτρονικό τρόπο.

(β) Το Μητρώο Μελών του Σωματείου περιλαμβάνει τα ακόλουθα δεδομένα υπαλλήλων και συνταξιούχων της Εταιρείας, τα οποία αντλεί αυτόματα από την ηλεκτρονική βάση δεδομένων της Εταιρείας:

- Αριθμός υπαλλήλου
- Φύλο
- Ονοματεπώνυμο
- **Φωτογραφία**
- Ημερομηνία γέννησης

- Ημερομηνία πρόσληψης
- Ημερομηνία θανάτου (όπου εφαρμόζεται)
- Ημερομηνία αφυπηρέτησης
- Διεύθυνση αλληλογραφίας
- Υπηρεσιακό τηλέφωνο (όπου είναι διαθέσιμο)
- Σταθερό τηλέφωνο (όπου είναι διαθέσιμο)
- Κινητό τηλέφωνο (όπου είναι διαθέσιμο)
- Ηλεκτρονική διεύθυνση
- Αριθμός συνδεδεμένου υπαλλήλου
- Κατάσταση: χήρος/χήρα, εξαρτώμενο τέκνο

(γ) Επιπρόσθετα, το προσωπικό του Σωματείου έχει πρόσβαση στα ακόλουθα προσωπικά δεδομένα των εργοδοτούμενων της Εταιρείας που δεν είναι μέλη του Σωματείου:

- Αριθμός υπαλλήλου
- Ονοματεπώνυμο υπαλλήλου
- Υπηρεσιακό τηλέφωνο (όπου είναι διαθέσιμο)
- Κινητό τηλέφωνο (όπου είναι διαθέσιμο)
- Ηλεκτρονική διεύθυνση (όπου είναι διαθέσιμη)
- Βαθμός και ειδικότητα στην υπηρεσία
- Διεύθυνση εργασίας

(δ) Η πρόσβαση στα πιο πάνω δεδομένα εξασφαλίζεται με αυτόματη σύνδεση των υπηρεσιακών ηλεκτρονικών υπολογιστών του προσωπικού του Σωματείου με την υπηρεσιακή Πύλη Ενδοδικτύου (Intranet) της Εταιρείας.

4.14.2. Η XXXXX, με ηλεκτρονικό μήνυμα της με ημερομηνία 27.04.2020, ανέφερε ότι: «Η δυνατότητα θέασης των πληροφοριών μη μελών του ΤΕΥ-ΑΤΗΚ έχει διακοπεί από τις 31.03.2020, με σχετική αναβάθμιση της εφαρμογής.».

4.15. Ενώ με μια απλή αναβάθμιση της εφαρμογής διακόπηκε η πρόσβαση από το Σωματείο στη θέαση/προβολή των προσωπικών δεδομένων μη μελών του Σωματείου, κάτι το οποίο έπρεπε να γίνει εξαρχής, εντούτοις η κοινή βάση δεδομένων παραμένει, παραβιάζοντας τις διατάξεις του Κανονισμού, όπως περιγράφω αναλυτικά στις παραγράφους 4.1. – 4.9. πιο πάνω.

4.16 Αναφορικά με τον λόγο που προβλήθηκε στην επιστολή των Καθ' ων την καταγγελία ημερ. 22 Ιουνίου, 2020 για έλλειψη δέουσας έρευνας, να αναφέρω πως αυτός ο λόγος δεν μπορεί να έχει ως βάση την τυχόν αναφορά αποσπάσματος σε προηγούμενη σχετική απόφαση, αλλά το κατά πόσον μια Αρχή έχει προβεί στην δέουσα έρευνα σε σχέση με τα περιστατικά της υπό διερεύνησης υπόθεσης, όπως η παρούσα. Συνεπώς, η αναφορά μου σε απόσπασμα της Απόφασης 44/19 της Ελληνικής Αρχής, δεν μπορεί να αιτιολογήσει έλλειψη δέουσας έρευνας. Η αναφορά είχε γίνει κυρίως, για να καταδείξει πως ένας υπεύθυνος επεξεργασίας πρέπει να λαμβάνει κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των προσωπικών δεδομένων που κατέχει (άρθρο 32), αλλά και να εφαρμόζει τις γενικές αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα (άρθρο 5) και νομιμότητας (άρθρο 6 του ΓΚΠΔ). Σε σχέση με το ότι δεν υπήρχε τεχνική δυνατότητα δημιουργίας αντιγράφων των δεδομένων, να αναφέρω πως αυτό δεν αιτιολογεί την οποιαδήποτε δυνατότητα θέασης των δεδομένων, από την στιγμή που δεν εξυπηρετούσαν τον συγκεκριμένο σκοπό για τον οποίον δινόταν η πρόσβαση. Εάν κάποιος επιθυμεί να καταχραστεί την δυνατότητα θέασης, υπάρχουν και άλλοι

τρόποι να το κάνει αυτό, πέραν της ηλεκτρονικής αντιγραφή των δεδομένων, όπως π.χ. φωτογράφιση ή απλή χειρόγραφη αντιγραφή. Δεν είναι επίσης δικαιολογία πως μόνο 2% των υπαλλήλων της Εταιρείας δεν είναι μέλη του Σωματείου. Ενός και μόνο ατόμου τα δικαιώματα να επηρεάζονται, είναι αρκετό για να καταλήξω πως υπάρχει παράβαση του Κανονισμού, πόσο μάλλον το 2%, σε ένα οργανισμό του μεγέθους της συγκεκριμένης Εταιρείας.

5. Κυρώσεις

5.1.1. Όπως ορίζεται στις διατάξεις του άρθρου 83(5) του Κανονισμού, παράβαση των διατάξεων των **άρθρων 5, 13 και 14**, επισύρει, «σύμφωνα με την παράγραφο 2, διοικητικά πρόστιμα έως 20 000 000 EUR ή, σε περίπτωση επιχειρήσεων, έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο».

5.1.2. Όπως ορίζεται στις διατάξεις του άρθρου 83(4) του Κανονισμού, παράβαση των διατάξεων των **άρθρων 25 και 32**, επισύρει, «σύμφωνα με την παράγραφο 2, διοικητικά πρόστιμα έως 10 000 000 EUR ή, σε περίπτωση επιχειρήσεων, έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο».

5.1.3. Παρατίθεται αυτούσια η παράγραφος 2 του άρθρου 83 του Κανονισμού:

«2. Τα διοικητικά πρόστιμα, ανάλογα με τις περιστάσεις κάθε μεμονωμένης περίπτωσης, επιβάλλονται επιπρόσθετα ή αντί των μέτρων που αναφέρονται στο άρθρο 58 παράγραφος 2 στοιχεία α) έως η) και στο άρθρο 58 παράγραφος 2 στοιχείο ι). Κατά τη λήψη απόφασης σχετικά με την επιβολή διοικητικού προστίμου, καθώς και σχετικά με το ύψος του διοικητικού προστίμου για κάθε μεμονωμένη περίπτωση, λαμβάνονται δεόντως υπόψη τα ακόλουθα:

α) η φύση, η βαρύτητα και η διάρκεια της παράβασης, λαμβάνοντας υπόψη τη φύση, την έκταση ή το σκοπό της σχετικής επεξεργασίας, καθώς και τον αριθμό των υποκειμένων των δεδομένων που έθιξε η παράβαση και το βαθμό ζημίας που υπέστησαν,

β) ο δόλος ή η αμέλεια που προκάλεσε την παράβαση,

γ) οποιεσδήποτε ενέργειες στις οποίες προέβη ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία για να μετριάσει τη ζημία που υπέστησαν τα υποκείμενα των δεδομένων,

δ) ο βαθμός ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, λαμβάνοντας υπόψη τα τεχνικά και οργανωτικά μέτρα που εφαρμόζουν δυνάμει των άρθρων 25 και 32,

ε) τυχόν σχετικές προηγούμενες παραβάσεις του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία,

στ) ο βαθμός συνεργασίας με την αρχή ελέγχου για την επανόρθωση της παράβασης και τον περιορισμό των πιθανών δυσμενών επιπτώσεών της,

ζ) οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζει η παράβαση,

η) ο τρόπος με τον οποίο η εποπτική αρχή πληροφορήθηκε την παράβαση, ειδικότερα εάν και κατά πόσο ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία κοινοποίησε την παράβαση,

θ) σε περίπτωση που διατάχθηκε προηγουμένως η λήψη των μέτρων που αναφέρονται στο άρθρο 58 παράγραφος 2 κατά του εμπλεκόμενου υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σχετικά με το ίδιο αντικείμενο, η συμμόρφωση με τα εν λόγω μέτρα,

ι) η τήρηση εγκεκριμένων κωδίκων δεοντολογίας σύμφωνα με το άρθρο 40 ή εγκεκριμένων μηχανισμών πιστοποίησης σύμφωνα με το άρθρο 42 και

ια) κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο που προκύπτει από τις περιστάσεις της συγκεκριμένης περίπτωσης, όπως τα οικονομικά οφέλη που αποκομίστηκαν ή ζημιών που αποφεύχθηκαν, άμεσα ή έμμεσα, από την παράβαση.».

6. Επιμέτρηση ποινής

6.1. Λαμβάνοντας υπόψη τις διατάξεις του άρθρου 83 του Κανονισμού, που αφορά στους Γενικούς Όρους επιβολής διοικητικών προστίμων, κατά την επιμέτρηση του διοικητικού προστίμου έλαβα υπόψιν μου τους ακόλουθους μετριαστικούς (1-3) και επιβαρυντικούς (4-7) παράγοντες:

(1) Την θέση των Καθ' ων την καταγγελία, πως δεν υπήρξε οποιοσδήποτε δόλος ή αμέλεια από πλευράς Σωματείου ή της Εταιρείας.

(2) Την συνεργασία που υπήρξε με το Γραφείο μου, σε σχέση με την επανόρθωση της παράβασης και τον περιορισμό των πιθανών δυσμενών επιπτώσεων της, αφού κατά την διάρκεια εξέτασης του συγκεκριμένου παραπόνου, η Εταιρεία έχει προβεί σε τεχνολογική αναβάθμιση σύμφωνα με την οποία: (α) από την 31.3.2020 δεν υπάρχει πλέον πρόσβαση στα δεδομένα μη μελών του Σωματείου, (β) έχει περιοριστεί η πρόσβαση στο Σωματείο, από εννέα άτομα που ήταν προηγουμένως, σε ένα άτομο, και (γ) εγκατέστησε σύστημα ιχνηλάτισης.

(3) Σε σχέση με τον βαθμό ευθύνης του υπεύθυνου επεξεργασίας, θεωρώ πως η ευθύνη βαρύνει περισσότερο την Εταιρεία, η οποία παρείχε ευχέρεια πρόσβασης στο Σωματείο, σε δεδομένα τα οποία δεν ανήκαν στα μέλη του.

(4) Την έκταση της παράβασης, η οποία δεν περιορίζεται μόνο στην παραπονουμένη, αλλά αφορά και το 2% των υπαλλήλων της Εταιρείας, τα οποία δεν ήταν μέλη του Σωματείου.

(5) Το γεγονός πως, σύμφωνα με την θέση την οποία εξακολουθούν να υποστηρίζουν οι Καθ' ων την καταγγελία, ότι δηλαδή η φωτογραφία τους είναι απαραίτητη για σκοπούς ταυτοποίησης και επικοινωνίας, δεικνύει πρόθεση μη συμμόρφωσης, μέχρι στιγμής, με τις υποδείξεις μου, πως είναι δυσανάλογη η πρόσβαση σε αυτό το στοιχείο.

(6) Το γεγονός πως η παράβαση περιήλθε εις γνώση μου, από το υποκείμενο των δεδομένων και όχι από τον υπεύθυνο επεξεργασίας.

(7) Δεν δέχομαι την θέση των Καθ' ων την καταγγελία πως δεν φαίνεται να έχει προκληθεί οποιαδήποτε βλάβη προς την παραπονούμενη. Η παράβαση, δεν περιορίζεται μόνο σ' αυτή, αλλά αφορά και το 2% των υπολοίπων επηρεαζομένων

υπαλλήλων της Εταιρείας, στα δεδομένα των οποίων είχε πρόσβαση το Σωματείο. Η Εταιρεία δεν είχε προβεί σε αξιολόγηση των κινδύνων λαμβάνοντας επαρκή τεχνικά και οργανωτικά μέτρα εξ αρχής, για διαχωρισμό στην πρόσβαση σε δεδομένα μελών και μη μελών του Σωματείου.

6.2. Έχοντας υπόψιν όλα τα ανωτέρω, με κυριότερο παράγοντα το γεγονός πως η ΤΕΥ-ΑΤΗΚ δεν έχει πρόσβαση από την 31.3.2020 σε δεδομένα μη μελών της, αποφασίζω όπως μη επιβάλω διοικητικό πρόστιμο στην παρούσα φάση.

6.3. Δίδεται όμως εντολή, συμφώνως των εξουσιών που μου παρέχει το Άρθρο 58(2)(δ) του ΓΚΠΔ 2016/679, προς την ΑΤΗΚ, όπως θεσπίσει τέτοια μέτρα ασφαλείας και πρακτικές, έτσι ώστε το ΤΕΥ-ΑΤΗΚ να μην έχει πλέον πρόσβαση σε δεδομένα δυσανάλογα απ' ότι εξυπηρετεί ο σκοπός, αποκλείοντας την πρόσβαση προς αυτό στην φωτογραφία των μελών του.

6.4 Εντέλλεται επίσης η ΑΤΗΚ, όπως σε διάστημα δύο μηνών από σήμερα, με πληροφορήσει για τις ενέργειες στις οποίες προέβη για συμμόρφωση με την παρούσα Απόφαση.

Ειρήνη Λοϊζίδου Νικολαϊδου
Επίτροπος Προστασίας Δεδομένων
Προσωπικού Χαρακτήρα