Αρ. Φακ.: 12.10.001.011.016

ΑΠΟΦΑΣΗ

Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην Αγγλική Σχολή (English School)

Στις 7/10/2021 υποβλήθηκε στο Γραφείο μου, Γνωστοποίηση Παραβίασης Προσωπικών Δεδομένων από την Αγγλική Σχολή, μέσω του Δικηγορικού Γραφείου [redacted] στο εξής «η Σχολή», αναφορικά με περιστατικό χρήσης διευθύνσεων ηλεκτρονικού ταχυδρομείου από την καθηγήτρια της Σχολής και Πρόεδρο της οργάνωσης του προσωπικού της Σχολής (ESSA), [redacted], για την αποστολή επιστολής ηλεκτρονικού ταχυδρομείου προς όλους τους γονείς/κηδεμόνες των μαθητών και προς το προσωπικό της Αγγλικής Σχολής, για σκοπούς που δεν συνδέονται με τον σκοπό για τον οποίο οι διευθύνσεις είχαν αρχικά συλλεγεί και χωρίς οι γονείς να έχουν ενημερωθεί για τέτοια χρήση της διεύθυνσης τους.

Ιστορικό

2.1. Με επιστολή μου μέσω ηλεκτρονικού ταχυδρομείου ημερομηνίας 8/10/2021, είχα ζητήσει ορισμένες διευκρινήσεις και επιπρόσθετες πληροφορίες από την Σχολή αναφορικά με το περιστατικό και την διαχείριση των προσωπικών δεδομένων από την Σχολή, τις οποίες έλαβα με την επιστολή της ημερ. 20/10/2021.

2.2. Λόγω του ότι η Σχολή ανέφερε ότι η παραβίαση έγινε από την [redacted], με επιστολή μου ημερ. 1/11/2021, κάλεσα την [redacted] όπως μου αποστείλει τις απόψεις / θέσεις της, και όπως απαντήσει σε ορισμένα ερωτήματα σχετικά με τα όσα αναφέρει η Σχολή. Η [redacted] απάντησε με επιστολή της μέσω ηλεκτρονικού ταχυδρομείου ημερ. 22/11/2021.

2.3. Από την πιο πάνω αλληλογραφία προκύπτουν τα ακόλουθα:

α) Στις 28/9/2021 περί τις 9:30μμ η [redacted] έστειλε επιστολή μέσω ηλεκτρονικού ταχυδρομείου σε 1695 διευθύνσεις γονέων/κηδεμόνων των μαθητών και διευθύνσεις του προσωπικού, μέσω του συστήματος επικοινωνίας της Σχολής, [redacted]. Η επιστολή φέρει την υπογραφή της [redacted] ως Πρόεδρος της οργάνωσης του προσωπικού της Σχολής, ESSA. Αντικείμενο της επιστολής ήταν η ενημέρωση των παραληπτών κυρίως των γονέων/κηδεμόνων, μεταξύ άλλων, σχετικά με τους σκοπούς της ESSA, ως Οργάνωση για την προάσπιση των εργασιακών δικαιωμάτων

όλου του προσωπικού της Σχολής, στο πλαίσιο της οποίας είχε αποφασιστεί 2ωρη απεργία. Η ενημέρωση περιελάμβανε επίσης λεπτομέρειες σχετικά με τις διαφορές της ESSA με το Συμβούλιο της Σχολής.
Σημειώνεται ότι, στην επιστολή που έλαβε ο κάθε γονέας/κηδεμόνας, δεν εμφανίζονταν οι διευθύνσεις των υπόλοιπων γονέων/κηδεμόνων, στους οποίους αποστάληκε το μήνυμα.

β) Με την πρόσβαση της στο σύστημα επικοινωνίας [redacted], ανάλογα με τον τρόπο επιλογής των παραληπτών του μηνύματος η [redacted] θα μπορούσε να έχει πρόσβαση στο ονοματεπώνυμο, ταυτότητα, τμήμα και έτος φοίτησης των μαθητών, Ως εκ του αποτελέσματος, η [redacted] προέβη σε χρήση των διευθύνσεων ηλεκτρονικού ταχυδρομείου των γονέων/κηδεμόνων των μαθητών.

γ) Η [redacted] απέστειλε επιστολή μέσω ηλεκτρονικού ταχυδρομείου προς τον Διευθυντή στις 28/9/2021 8:16μμ, με την οποία τον ενημέρωσε για την πρόθεσή της να αποστείλει επιστολή προς το προσωπικό και τους γονείς/κηδεμόνες, στην οποία δεν έλαβε απάντηση.

δ) Αμέσως μετά το περιστατικό, η Σχολή περιόρισε τεχνικά τη δυνατότητα αποστολής γενικού μηνύματος σε μεγάλο αριθμό παραληπτών και ρύθμισε το σύστημα ώστε οι καθηγητές να έχουν πρόσβαση μόνο στα δεδομένα των μαθητών τους οποίους διδάσκουν και μόνο στα e-mails των γονιών αυτών των μαθητών.

2.4. Με βάση την Γνωστοποίηση Παραβίασης Προσωπικών Δεδομένων, τα υποστηρικτικά έγγραφα που είχαν επισυναφθεί και τις διευκρινήσεις που έλαβα από την Σχολή, η Σχολή υποστηρίζει τα ακόλουθα:

α) Η χρήση των διευθύνσεων ηλεκτρονικού ταχυδρομείου στην οποία προέβηκε η [redacted], αποτελεί παράβαση της Πολιτικής Ασφάλειας της Σχολής στην οποία, μεταξύ άλλων, αναγράφεται ότι, «*Important and general information/announcements need to be forwarded to a group of the parent and/or student population; the letter/announcement must be sent on the appropriate letterhead to the Headmaster for approval. Once approved, the message must be forwarded to* [redacted]@[redacted] *to be sent to the target audience by the Media Coordinator.*» Η επιστολή της [redacted] μέσω ηλεκτρονικού ταχυδρομείου προς τον Διευθυντή στις 28/9/2021 8:16μμ, με την οποία τον ενημέρωσε για το γεγονός ότι προτίθετο να αποστείλει επιστολή προς το προσωπικό και τους γονείς, δεν απαντήθηκε και ως εκ τούτου δεν δόθηκε η έγκριση του διευθυντή.

β) Η αποστολή έγινε για σκοπούς οι οποίοι δεν συνδέονται με τους σκοπούς για τους οποίους οι διευθύνσεις είχαν συλλεγεί, χωρίς να είχε δοθεί ενημέρωση στους γονείς για τέτοια χρήση των διευθύνσεων τους και χωρίς νομική βάση. Οι σκοποί για τους οποίους οι διευθύνσεις είχαν συλλεγεί, όπως καταγράφονται στην Πολιτική Ασφάλειας, είναι «*to Communicate appropriately with parents to strengthen the home/School relationship*». Επιπρόσθετα, η αποστολή αυτή αντιβαίνει με την Πολιτική Ασφάλειας, όσον αφορά στα καθήκοντα των καθηγητών «*To act at all times while engaged in School duties in accordance with the School's Code of Professional Conduct*».

γ) η αποστολή έγινε υπό την ιδιότητα της [redacted] ως Πρόεδρος της συντεχνίας του προσωπικού της Σχολής (ESSA) και όχι υπό την ιδιότητα της ως καθηγήτρια (φέρει την υπογραφή της ως Πρόεδρος ESSA).

2.5. Η [redacted] με την επιστολή της μέσω ηλεκτρονικού ταχυδρομείου ημερ. 22/11/2021 υποστηρίζει, μεταξύ άλλων ότι, ο Πρόεδρος και τα μέλη της οργάνωσης Προσωπικού της Σχολής (ESSA) δεν έχουν γραφεία ούτε και δικό τους ηλεκτρονικό σύστημα αλλά χρησιμοποιούν το σύστημα της Αγγλικής Σχολής για όλη την επικοινωνία. Η Σχολή δεν έχει γραπτή πολιτική σχετικά με την πιο πάνω χρήση και δεν χρειάζεται έγκριση ή άδεια από τη Διεύθυνση για αποστολή οποιασδήποτε επικοινωνίας. Κατά το 1998 η ESSA είχε επικοινωνήσει με το σύνολο των γονέων, χρησιμοποιώντας το αρχείο της Αγγλικής Σχολής, χωρίς πρόβλημα.

2.6.1. Με την επιστολή μου ημερομηνίας 17/12/2021 ενημέρωσα την Σχολή ότι υπάρχει εκ πρώτης όψεως παράβαση του άρθρου 32 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679, εφεξής «ο Κανονισμός», εκ μέρους της Σχολής, σχετικά με την μη εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων, από τον μη περιορισμό της πρόσβασης των καθηγητών σε ηλεκτρονικές διευθύνσεις γονέων/κηδεμόνων, καθότι, εκ πρώτης όψεως διαφάνηκε ότι, το σύστημα δεν ήταν κατάλληλα διαμορφωμένο, από τεχνικής άποψης, σύμφωνα με την Πολιτική Ασφάλειας για την διαδικασία αποστολής email. Ενώ στην Πολιτική Ασφάλειας προβλέπεται ότι, για την αποστολή επιστολής προς ομάδα γονέων ή μαθητών, η επιστολή πρέπει να σταλεί στον διευθυντή για έγκριση και στη συνέχεια να προωθηθεί στον Media Coordinator για να την αποστείλει, στο σύστημα είχε δοθεί σε όλους τους καθηγητές πρόσβαση στις διευθύνσεις όλων των γονέων/κηδεμόνων. Ως εκ τούτου, με βάση την Πολιτική Ασφάλειας, τέτοια πρόσβαση θα έπρεπε να είχε μόνο ο Media Coordinator. Με βάση την αρχή της «ανάγκης γνώσης» και της ελαχιστοποίησης των δεδομένων (Άρθρο 5(1)(γ) του Κανονισμού), οι καθηγητές θα έπρεπε να έχουν πρόσβαση μόνο στα δεδομένα των μαθητών, τους οποίους διδάσκουν.

2.6.2. Στην ίδια επιστολή μου, ζήτησα από την Σχολή να υποβάλει τις απόψεις/θέσεις της σχετικά με τα πιο πάνω, να αναφέρει τους λόγους για τους οποίους θεωρεί ότι δεν συντρέχουν λόγοι για την επιβολή κάποιας κύρωσης και/ ή οποιουσδήποτε μετριαστικούς παράγοντες, καθώς επίσης και να τοποθετηθεί μεταξύ άλλων σχετικά με τα ακόλουθα:

α) Η πολιτική της Σχολής που είναι αναρτημένη στην ιστοσελίδα της δεν παρέχει ενημέρωση για τους σκοπούς της επεξεργασίας, τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων και τα υπόλοιπα στοιχεία που απαιτούνται από το άρθρο 13 του Κανονισμού και δεν έχουν τεθεί ενώπιον μου στοιχεία που να δείχνουν κατά πόσο παρέχεται οποιαδήποτε επιπρόσθετη ενημέρωση στους γονείς/κηδεμόνες κατά το στάδιο της συλλογής των δεδομένων.

β) Στις επιστολές της η Σχολή δεν έχει κάνει οποιαδήποτε αναφορά και δεν έχει υποβάλει οποιαδήποτε στοιχεία που να υποδεικνύουν κατά πόσο είχε εξεταστεί ή συζητηθεί με την ESSA το θέμα της χρήσης των συστημάτων της Σχολής από την ESSA και/ή κατά πόσο είχε επίσημα ή ανεπίσημα επιτραπεί ή απαγορευθεί η εν λόγω χρήση.

γ) Στην επιστολή της ημερ. 20/10/2021, η Σχολή αναφέρει ότι μετά το συμβάν, έχει περιοριστεί και τεχνικά η δυνατότητα αποστολής γενικού μηνύματος σε μεγάλο αριθμό παραληπτών, αλλά δεν διευκρινίζεται σε τι ακριβώς αναφέρεται ο «μεγάλος αριθμός».

2.7. Η Σχολή, με επιστολή της ημερ. 12/1/2022, αναφέρει μεταξύ άλλων τα ακόλουθα:

α) Το σύστημα της Σχολής ήταν απόλυτα εναρμονισμένο με την γραπτή πολιτική για την αποστολή e-mail, η οποία αποτελείται από δύο σκέλη. Πέραν της διαδικασίας στην οποία είχα αναφερθεί (σύμφωνα με την οποία, αφού ληφθεί η έγκριση του διευθυντή, η επιστολή πρέπει να προωθηθεί στον Media Coordinator για να την αποστείλει), υπάρχει δεύτερο

σκέλος που αφορά σε επικοινωνία από τους καθηγητές προς ομάδα μαθητών ή γονέων με την προηγούμενη έγκριση του Υπεύθυνου Τμήματος (Head of Department): «*Should teachers like to communicate: a) with a group of students and parents, communication need to be prior approved by the Head of Department …*».
Επομένως, το σύστημα ήταν σωστά διαμορφωμένο από τεχνικής άποψης για να επιτρέπει την αποστολή ομαδικών e-mails από καθηγητές και η πρόσβαση τους σε όλες τις ηλεκτρονικές διευθύνσεις, είχε αξιολογηθεί από την Σχολή με βάση τις ανάγκες για την εύρυθμη λειτουργία του Σχολείου και την πιθανότητα και σοβαρότητα του κινδύνου. Για την απρόσκοπτη λειτουργία της Σχολής, σε αρκετές περιπτώσεις απαιτείται όπως οι καθηγητές επικοινωνούν με μεγαλύτερες ομάδες γονέων και μαθητών. Παράλληλα, λήφθηκε υπόψιν ότι, πρόκειται για κλειστό σύστημα επικοινωνίας μεταξύ συγκεκριμένων κατηγοριών υποκειμένων των δεδομένων με συγκεκριμένη σχέση μεταξύ τους, ήτοι, μεταξύ των μαθητών, γονιών και Σχολείου, και επομένως η πιθανότητα επέλευσης κινδύνου και η σοβαρότητα του κινδύνου είχαν εκτιμηθεί σε χαμηλά επίπεδα. Τα δεδομένα που αφορά η δοθείσα πρόσβαση είναι η διεύθυνση ηλεκτρονικού ταχυδρομείου και τα ονοματεπώνυμα των γονιών και των μαθητών.

β) Αναφορικά με το θέμα της ενημέρωσης που παρέχεται στους γονείς/κηδεμόνες για την επεξεργασία των δεδομένων τους, η Σχολή κατά το στάδιο της συλλογής των προσωπικών δεδομένων από τους γονείς και τους μαθητές παρέχει ξεχωριστές ενημερώσεις σε σχέση με την επεξεργασία των δεδομένων για συγκεκριμένους σκοπούς. Στην επιστολή της, η Σχολή ανέφερε ως παράδειγμα συγκεκριμένες περιπτώσεις εντύπων (τα οποία επισύναψε).
Περαιτέρω, η Σχολή ανέφερε ότι, έχει ετοιμαστεί επικαιροποιημένη ενημερωτική δήλωση, η οποία αναμένεται να αναρτηθεί στην ιστοσελίδα της Σχολής το συντομότερο (την οποία επίσης επισύναψε).

γ) Η Σχολή έχει ξεκάθαρη πολιτική σχετικά με την χρήση των emails και την επικοινωνία με τους γονείς και μαθητές. Στην Πολιτική Ασφάλειας / Access control mechanism αναγράφεται ότι τα υπηρεσιακά e-mail πρέπει να χρησιμοποιούνται μόνο για σκοπούς εργασίας εντούτοις, επιτρέπεται σε κάποιο περιορισμένο βαθμό η σποραδική χρήση του υπηρεσιακού e-mail για προσωπικούς σκοπούς, πρακτική η οποία συνάδει με την Γνώμη της Ομάδας Εργασίας του Άρθρου 29 για την επεξεργασία των δεδομένων στην εργασία, με την νομολογία της ΕΣΔΑ καθώς και με προηγούμενη καθοδήγηση του Γραφείου μου. Εφόσον υπάρχει η πολιτική η οποία ρυθμίζει την αποστολή μηνυμάτων σε γονείς ή μαθητές, δεν υπάρχει κάτι άλλο που πρέπει να συζητηθεί με την ESSA.
Αναφορικά με τον ισχυρισμό της [redacted] ότι είχε επικοινωνήσει κατά το 1998 με το σύνολο των γονέων και καθηγητών χρησιμοποιώντας το αρχείο της Σχολής, η Σχολή ανέφερε ότι, ακόμη και να είχε λάβει χώρα αυτή η επικοινωνία πριν από 23 χρόνια, πλέον υφίστανται ειδικές νομοθεσίες και σαφείς πολιτικές σε σχέση με την επικοινωνία με τους γονείς και το προσωπικό έχει λάβει γνώση των πολιτικών και έχει λάβει εκπαίδευση.

δ) Με την αναφορά της στην επιστολή της ημερ. 20/10/2021 ότι «έχει περιοριστεί και τεχνικά η δυνατότητα αποστολής γενικού μηνύματος σε μεγάλο αριθμό παραληπτών» εννοεί ότι έχει περιοριστεί η δυνατότητα αποστολής μαζικών μηνυμάτων (mass e-mails) και πλέον με τις νέες ρυθμίσεις οι καθηγητές έχουν πρόσβαση μόνο στα δεδομένα των μαθητών τους οποίους διδάσκουν και μόνο στα e-mails των γονιών αυτών των μαθητών. Παράλληλα σημείωσε ότι ο τεχνικός αυτός περιορισμός δημιουργεί προβλήματα στην καθημερινή εύρυθμη λειτουργία της Σχολής.

ε) Με βάση τα πιο πάνω, θεωρεί ότι, δεν υπάρχει παράβαση του Άρθρου 32 του Κανονισμού εκ μέρους της και ότι, υπό τις περιστάσεις, η επιβολή οποιασδήποτε κύρωσης εις βάρος της δεν δικαιολογείται.

Νομικό Πλαίσιο

3.1. Σύμφωνα με την ερμηνεία που αποδίδεται από το Άρθρο 4(1) του Κανονισμού, δεδομένα προσωπικού χαρακτήρα είναι «*κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου,*»

3.2. Σύμφωνα με την ερμηνεία που αποδίδεται από το Άρθρο 4(2) του Κανονισμού, «επεξεργασία» είναι «*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.*»

3.3. «υπεύθυνος επεξεργασίας», σύμφωνα με την ερμηνεία που αποδίδεται από το Άρθρο 4(7), είναι «*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.*»

3.4. Με βάση το Άρθρο 5(1)(α) του Κανονισμού τα δεδομένα προσωπικού χαρακτήρα «*υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»)*»

3.5. Με βάση δε το Άρθρο 5(1)(β), τα δεδομένα προσωπικού χαρακτήρα «*συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς ... («περιορισμός του σκοπού»)*».

3.6. Με βάση το άρθρο 5(1)(γ) του Κανονισμού τα δεδομένα προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας θα πρέπει *να «είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»)»*,

3.7. Στο Άρθρο 13 αναφέρονται οι πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων, όταν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων.

3.8. Το Άρθρο 32 του Κανονισμού προβλέπει ότι, «*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…».

3.9. Το Άρθρο 33 του Κανονισμού, μεταξύ άλλων προβλέπει ότι, «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*...Σε περίπτωση που και εφόσον δεν είναι δυνατόν να παρασχεθούν οι πληροφορίες ταυτόχρονα, μπορούν να παρέχονται σταδιακά χωρίς αδικαιολόγητη καθυστέρηση».

Σκεπτικό

4.1. Οι διευθύνσεις ηλεκτρονικού ταχυδρομείου στο σύστημα [redacted] είναι «συνδεδεμένες» με τους μαθητές, και ως εκ τούτου αποτελούν προσωπικά δεδομένα, σύμφωνα με την ερμηνεία που δίνεται στο Άρθρο 4(1) του Κανονισμού, ανεξάρτητα εάν από κάποιες διευθύνσεις ηλεκτρονικού ταχυδρομείου δεν μπορεί να ταυτοποιηθεί άμεσα το υποκείμενο των δεδομένων.

4.2. Η πρόσβαση και χρήση των διευθύνσεων ηλεκτρονικού ταχυδρομείου αποτελούν μορφές επεξεργασίας σύμφωνα με την ερμηνεία που δίνεται στο Άρθρο 4(2) του Κανονισμού.

4.3.1. Η πρόσβαση στο σύστημα αποστολής email ([redacted]) είχε δοθεί στην [redacted] λόγω της ιδιότητας της ως καθηγήτρια και όχι ως μέλος της ESSA, ενώ η επιστολή στάλθηκε υπό την ιδιότητα της ως Πρόεδρος της ESSA και η επιστολή αφορούσε σε εργατικά/συνδικαλιστικά θέματα του προσωπικού.
Η ESSA αποτελεί ξεχωριστή οντότητα από την Αγγλική Σχολή, η οποία έχει διαφορετικό στόχο / σκοπό λειτουργίας από αυτόν της σχολής και κατά συνέπεια αποτελεί ξεχωριστό υπεύθυνο επεξεργασίας. Επιπρόσθετα, δεν υπάρχει κατάλληλη σχέση μεταξύ των υποκειμένων των δεδομένων (γονείς/κηδεμόνες) και της ESSA, εφόσον δεν είναι μέλη της και δεν είχαν δώσει τις διευθύνσεις τους στην ESSA.

4.3.2. Με βάση τα πιο πάνω, υπήρξε μη εξουσιοδοτημένη πρόσβαση / χρήση των δεδομένων από ξεχωριστό υπεύθυνο επεξεργασίας.

4.4. Η ευθύνη της [redacted] και/ή της ESSA για την πιο πάνω χρήση των διευθύνσεων εξετάζεται σε ξεχωριστή Απόφαση.

4.5. Ανεξάρτητα από την ευθύνη της [redacted] και/ή της ESSA, με βάση το άρθρο 32 η Σχολή ως υπεύθυνος επεξεργασίας των δεδομένων που διατηρεί και επεξεργάζεται πρέπει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων 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. Σημειώνεται ότι, η διερεύνηση επικεντρώνεται στα σημεία που σχετίζονται με το συγκεκριμένο περιστατικό, και δεν αποτελεί εξαντλητικό έλεγχο όλων των πολιτικών και μέτρων ασφαλείας της Σχολής.

4.5.1. Ένα από τα κυριότερα μέτρα που πρέπει να λαμβάνει ο κάθε υπεύθυνος επεξεργασίας είναι η ενημέρωση / εκπαίδευση του προσωπικού σχετικά με τον χειρισμό των δεδομένων προσωπικού χαρακτήρα. Με την υποβολή της Γνωστοποίησης, η Σχολή επισύναψε αποσπάσματα της γραπτής πολιτικής αναφορικά με την διαδικασία που πρέπει να ακολουθείται κατά την αποστολή email, αντίγραφα διαφανειών της παρουσίασης / εκπαίδευσης που έγινε στο προσωπικό αναφορικά με θέματα προστασίας δεδομένων προσωπικού χαρακτήρα κατά το 2018 και αντίγραφο ενημέρωσης που φαίνεται να στάληκε προς το προσωπικό στις 31/8/2021 το οποίο περιλαμβάνει μεταξύ άλλων πολιτικές, κώδικες δεοντολογίας και πληροφορίες σχετικά με τον Κανονισμό για την προστασία δεδομένων προσωπικού χαρακτήρα.

4.5.2. Η λήψη κατάλληλων μέτρων με βάση την αρχή της «ανάγκης γνώσης» και της ελαχιστοποίησης των δεδομένων (Άρθρο 5(1)(γ)) και λαμβάνοντας υπόψη την πιθανότητα επέλευσης των κινδύνων, θα πρέπει πάντοτε να είναι η βάση της πολιτικής οποιουδήποτε οργανισμού. Αντιλαμβάνομαι ότι υπό προϋποθέσεις και υπό κατάλληλες εγγυήσεις / διαδικασίες, οι καθηγητές θα πρέπει να μπορούν να χρησιμοποιούν και διευθύνσεις ορισμένων άλλων γονέων πέραν των γονέων των μαθητών στους οποίους διδάσκουν, αλλά η γενική και απεριόριστη πρόσβαση στα emails όλων των γονιών και όλων των μαθητών δεν θα πρέπει να είναι ο κανόνας αλλά η εξαίρεση, ακλουθώντας τις κατάλληλες διαδικασίες.

Η Σχολή αναφέρει ότι με βάση το δεύτερο σκέλος της Πολιτικής Ασφάλειας, το οποίο αφορά στην επικοινωνία από τους καθηγητές προς ομάδα μαθητών ή γονέων με την προηγούμενη έγκριση του Υπεύθυνου Τμήματος (Head of Department), δεν θα μπορούσε να περιοριστεί τεχνικά η πρόσβαση των καθηγητών, αφού με βάση την διαδικασία της πολιτικής, οι καθηγητές θα πρέπει να είναι σε θέση να αποστέλλουν emails σε ομάδες μαθητών και γονέων (με την έγκριση του Υπεύθυνου Τμήματος). Ωστόσο, δεν υπήρχε κάποιος τεχνικός μηχανισμός για διασφάλιση ότι προηγήθηκε η εξασφάλιση έγκρισης από τον Διευθυντή ή τον Υπεύθυνο του Τμήματος.

Στην ιστοσελίδα της Σχολής στο μέρος «The English School Staff List (2021-22) (https://www.englishschool.ac.cy/staff-list» αναγράφονται πέραν των 100 ονομάτων στο μέρος «Teaching staff». Ακόμη και εάν δεν έχουν όλοι αυτοί πρόσβαση στα emails, ο αριθμός των καθηγητών είναι σχετικά μεγάλος και ως εκ τούτου η πιθανότητα επέλευσης του κινδύνου μη εξουσιοδοτημένης χρήσης των διευθύνσεων από καθηγητές είναι σχετικά μεγάλη.

Ως εκ τούτου θα έπρεπε να υπάρχει τουλάχιστον ένας μηχανισμός μέσω του οποίου να δίνεται, ή να διασφαλίζεται ότι έχει δοθεί η έγκριση του Διευθυντή ή του Υπεύθυνου Τμήματος. Εναλλακτικά, η Σχολή θα μπορούσε να διαμόρφωνε την πολιτική της, έτσι ώστε στις περιπτώσεις όπου καθηγητές επιθυμούν να επικοινωνήσουν με ομάδα γονέων πέραν των γονέων των μαθητών στους οποίους διδάσκουν, τα emails να αποστέλλονται από τους Υπεύθυνους Τμήματος ή από ειδικά εξουσιοδοτημένα άτομα, ώστε να περιορίζεται ο αριθμός των ατόμων που έχουν πρόσβαση στα emails.

Ως εκ του αποτελέσματος, φάνηκε ότι τα τεχνικά και οργανωτικά μέτρα που λαμβάνονταν δεν ήταν ικανοποιητικά ώστε να αποτρέψουν μη εξουσιοδοτημένη χρήση των διευθύνσεων ηλεκτρονικού ταχυδρομείου των γονέων/κηδεμόνων. Ανεξάρτητα εάν η αποστολή της επιστολής έγινε από την [redacted], υπό την ιδιότητα της ως Πρόεδρος της ESSA και όχι ως καθηγήτρια, το εν λόγω περιστατικό πιθανό να μην συνέβαινε εάν είχε περιοριστεί η πρόσβαση των καθηγητών ή υπήρχε τεχνικός μηχανισμός που να

διασφαλίζει ότι είχε εξασφαλιστεί η έγκριση από τον Διευθυντή ή από τον Υπεύθυνο του Τμήματος.

Ανεξάρτητα από τυχόν ευθύνη της [redacted] και/ή της ESSA για την πιο πάνω χρήση των διευθύνσεων, η Σχολή ως υπεύθυνος επεξεργασίας φέρει ευθύνη να λαμβάνει τα κατάλληλα μέτρα. Οι γονείς/κηδεμόνες που δίνουν τα προσωπικά δεδομένα τους στην Σχολή, αναμένουν από την Σχολή, ως υπεύθυνος επεξεργασίας, να λαμβάνει τα κατάλληλα μέτρα για προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση/ χρήση.

4.5.3. Με βάση τα πιο πάνω κρίνω ότι υπήρξε παράβαση του Άρθρου 32 για τη μη λήψη των κατάλληλων τεχνικών και οργανωτικών μέτρων για την προστασία των διευθύνσεων ηλεκτρονικού ταχυδρομείου από μη εξουσιοδοτημένη πρόσβαση/χρήση.

4.6.1. Αναφορικά με το παρεμπίπτον ζήτημα της πολιτικής της Σχολής για την ενημέρωση των γονέων/κηδεμόνων, συστήνεται όπως η Σχολή βεβαιωθεί ότι η ενημέρωση που ετοιμάστηκε είναι σύμφωνη με τις διατάξεις του άρθρου 13 και των παραγράφων (60) και (61) του προοιμίου του Κανονισμού και την επικαιροποιεί σε τακτά χρονικά διαστήματα.

4.6.2. Αναφορικά με το θέμα κατά πόσο είχε επίσημα ή ανεπίσημα επιτραπεί ή απαγορευθεί η χρήση των συστημάτων της Σχολής από την ESSA, κρίνω αποδεκτή την απάντηση της σχολής (παράγραφος 2(7)(γ)) καθώς θα ήταν πρακτικά αδύνατο οι Πολιτικές Ασφάλειας να περιλαμβάνουν κατάλογο προσώπων ή οντοτήτων που δεν έχουν δικαίωμα και /ή δεν αποτελούν εξουσιοδοτημένους χρήστες των συστημάτων και /ή των δεδομένων προσωπικού χαρακτήρα.

Κατάληξη

5.Αφού έλαβα υπόψη μου όλα τα περιστατικά που αφορούν στην παρούσα υπόθεση, έλαβα επίσης υπόψη μου και τους πιο κάτω παράγοντες:

5.1. Μετριαστικοί Παράγοντες:

α) Τα δεδομένα που αφορά η πρόσβαση είναι η διεύθυνση ηλεκτρονικού ταχυδρομείου και τα ονοματεπώνυμα των γονέων/κηδεμόνων και των μαθητών,

β) Το σύστημα ήταν διαμορφωμένο με τρόπο ώστε στο email που έλαβαν οι γονείς/κηδεμόνες, να μην ήταν ορατές οι διευθύνσεις ηλεκτρονικού ταχυδρομείου των άλλων γονέων/κηδεμόνων,

γ) Η Σχολή διέθετε πολιτική αναφορικά με το θέμα της αποστολής email σε γονείς/κηδεμόνες,

δ) Αμέσως μετά το περιστατικό, η Σχολή ρύθμισε το σύστημα ώστε οι καθηγητές να έχουν πρόσβαση μόνο στα δεδομένα των μαθητών τους οποίους διδάσκουν και μόνο στα e-mails των γονιών αυτών των μαθητών.

5.2 Επιβαρυντικοί Παράγοντες

α) Ο μεγάλος αριθμός διευθύνσεων ηλεκτρονικού ταχυδρομείου γονέων / κηδεμόνων,

β) Δεν υπήρξε παραδοχή της Σχολής σχετικά με παράβαση / ευθύνη από την Σχολή.

Συνεκτιμώντας όλα τα πιο πάνω καθώς επίσης και το μέγεθος της Σχολής, με βάση τις εξουσίες που μου απονέμει ο Κανονισμός και ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018 (Νόμος 125(I)/2018), αποφάσισα όπως επιβάλω στην Σχολή την κύρωση του **Διοικητικού Προστίμου ύψους €4,000 (τεσσάρων χιλιάδων ευρώ),** δυνάμει των άρθρων 58(2)(θ) και 83 του Κανονισμού.

Ειρήνη Λοϊζίδου Νικολαΐδου
Επίτροπος Προστασίας Δεδομένων
Προσωπικού Χαρακτήρα

22 Μαρτίου 2022