Αρ. Φακ.: 12.10.001.011.001 Α/Α 45/2019

4 Μαρτίου, 2020

κα xxxxxx xxxxxxxxxx
Υπεύθυνο Προστασίας Δεδομένων
Ελληνικής Τράπεζας

ΑΠΟΦΑΣΗ
Θέμα: Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα

Έχω οδηγίες να αναφερθώ στην γνωστοποίηση παραβίασης που αποστείλατε στο Γραφείο της Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέσω ηλεκτρονικού ταχυδρομείου στις 20 Σεπτεμβρίου, 2019 και να σας πληροφορήσω τα ακόλουθα:

1. Περιστατικό

α) Καταχώριση στοιχείων

Στη γνωστοποίηση παραβίασης δεδομένων, αναφέρθηκε ότι το περιστατικό περιήλθε στην αντίληψη της Τράπεζας όταν πελάτης (Σ.Γ.) επικοινώνησε με το κατάστημα και προέβη σε παράπονο διότι έβλεπε στοιχεία κάρτας και λογαριασμού άλλου πελάτη (Μ.Κ.) στο Web Banking του. Μετά από έρευνα διεφάνη ότι και οι δύο πελάτες ήταν καταχωρισμένοι σε σύστημα της Τράπεζας με τον ίδιο αριθμό διαβατηρίου. Επιπρόσθετα, η νέα κάρτα του Μ.Κ. λόγω της αυτόματης ένωσης στο σύστημα, στάληκε αυτόματα στην διεύθυνση του Σ.Γ., κάτι το οποίο σας ανέφερε και ο Σ.Γ.. Μετά την πιο πάνω ενημέρωση, η κάρτα ακυρώθηκε και ζητήθηκε από τον Σ.Γ. να την επιστρέψει στην Τράπεζα.

Κατόπιν διευκρινίσεων που σας ζητήθηκαν, με επιστολή σας ημερ. 4 Νοεμβρίου, 2019, αναφέρατε ότι το web banking του Μ.Κ. δημιουργήθηκε στις 29/06/2016. Στις 02/05/2019 έγινε η επικαιροποίηση με αποτέλεσμα ο Μ.Κ. και Σ.Γ. να έχουν στο σύστημα της Τράπεζας τον ίδιο αριθμό διαβατηρίου. Τα εμπλεκόμενα πρόσωπα μπορούσαν να έχουν πρόσβαση στα στοιχεία αλλά δεν μπορούσαν να προβούν σε μεταφορές χρημάτων εις βάρος του άλλου υποκειμένου. Λόγω του ότι το περιστατικό οφείλεται σε ανθρώπινο λάθος, και όχι σε λάθος στις διαδικασίες ή στα συστήματα, η Τράπεζα υπενθύμισε στους εμπλεκόμενους συναδέλφους την ορθή τήρηση του «four eye principle» και των ενεργειών που προκύπτουν λόγω των «messages».

Την 17 Ιανουαρίου, 2020 (μετά και από την έκδοση εκ πρώτης όψεως απόφασης από το Γραφείο μου στις 16 Δεκεμβρίου, 2019 με την οποία κατέληξα ότι υπήρξε εκ πρώτης παράβαση των Άρθρων 32 παρ. 1(β) και 33 παρ. 1), διευκρινίσατε περαιτέρω ότι η εξέταση του περιστατικού συνεχίστηκε και μετά την υποβολή της Γνωστοποίησης ημερ. 20/09/19 και από την εξέταση του περιστατικού έχουν διαφανεί και άλλα δεδομένα. Διευκρινίσατε ότι την 29/5/19 η Τράπεζα ενημερώθηκε από συγκεκριμένο πελάτη (Σ.Γ.) ότι ο ίδιος έβλεπε, μέσω της υπηρεσίας Web Banking, πληροφορίες που αφορούσαν στον αριθμό λογαριασμού και στοιχεία κάρτας άλλου πελάτη. Μετά από αυτό, λήφθηκαν άμεσα μέτρα έτσι ώστε ο Σ.Γ. να βλέπει μόνο τα δικά του στοιχεία.

Προσθέσατε ως νέα δεδομένα, ότι στις 16/4/19, λόγω λάθους υπαλλήλου της Τράπεζας κατά την πληκτρολόγηση των στοιχείων του Μ.Κ. (χωρίς να αναφέρεται ο λόγος της καταχώρησης), καταχωρίστηκε εκ λάθους ως αριθμός διαβατηρίου του Μ.Κ., ο νέος αριθμός διαβατηρίου του Σ.Γ. Ο αριθμός αυτός καταχωρείτο στα στοιχεία της Τράπεζας, για πρώτη φορά και γι' αυτό τον λόγο δεν εμφάνισε οποιαδήποτε προειδοποίηση. Ακολούθως την 2/5/19, λόγω επικαιροποίησης των στοιχείων του Σ.Γ. καταχωρίστηκε ο νέος αριθμός διαβατηρίου του, ο οποίος όμως είχε εξ' αρχής καταχωρηθεί την 16/4/19 στα στοιχεία που αφορούσαν τον Μ.Κ.. Το σύστημα τότε παρουσίασε στην υπάλληλο προειδοποιητικό μήνυμα για την ύπαρξη άλλου πελάτη με τον ίδιο αριθμό. Η υπάλληλος, βασιζόμενη στο γεγονός ότι τα στοιχεία του Σ.Γ. επιβεβαιώνονταν από έγγραφα τα οποία είχε στη διάθεση της, προχώρησε στην καταχώρηση του νέου αριθμού διαβατηρίου. Η καταχώρηση

εγκρίθηκε από δεύτερο υπάλληλο. Την 2/5/19, το σύστημα της Τράπεζας αυτόματα επικαιροποίησε τα στοιχεία του ΜΚ, με αποτέλεσμα να έχει την ίδια διεύθυνση με τον Σ.Γ.

Αναφέρατε επίσης, ότι τελικά όπως διεφάνη, στις 2/5/19 ο Μ.Κ. δεν είχε προσωπικό λογαριασμό στην Τράπεζα, αλλά διατηρούσε λογαριασμό εταιρείας με τον οποίο ήταν συνδεδεμένη η χρεωστική κάρτα, εκδοθείσα την 9/8/19 στο όνομά του. Τα στοιχεία τα οποία παρουσιάστηκαν στον Σ.Γ. μέσω της υπηρεσίας Web Banking αφορούσαν τον εταιρικό λογαριασμό και όχι τον προσωπικό λογαριασμό του Μ.Κ. και η διεύθυνση που φαινόταν ως διεύθυνση του Μ.Κ. ήταν η διεύθυνση του Σ.Γ. Δεν παρουσιάστηκαν στον Σ.Γ. οποιαδήποτε στοιχεία κίνησης του εταιρικού λογαριασμού ή συναλλαγών που έγιναν με την εταιρική κάρτα και η μόνη φορά που είχε εξασφαλίσει πρόσβαση ο Σ.Γ. στην υπηρεσία Web Banking μετά τις 2/3/19, ήταν στις 28/5/19, μια μέρα πριν ενημερώσει την Τράπεζα. Παρόλο που όταν ειδοποιηθήκατε στις 29/5/19 διορθώθηκε ο αριθμός διαβατηρίου του Μ.Κ., έτσι ώστε τα στοιχεία του Μ.Κ. να μην παρουσιάζονται στο Web Banking του Σ.Γ., εντούτοις οι υπάλληλοι της Τράπεζας δεν προχώρησαν και στη διόρθωση της διευθύνσεως του Μ.Κ. Αποτέλεσμα αυτού, όταν στις 9/8/19 εκδόθηκε νέα κάρτα στο όνομα του Μ.Κ., αυτή απεστάλει στη διεύθυνση του Σ.Γ. Ο Σ.Γ. σας ενημέρωσε για την παραλαβή της κάρτας την 26/8/19. Τότε, προχωρήσατε σε ακύρωση της κάρτας και διόρθωση της διεύθυνσης του Μ.Κ. Ζητήσατε από τον Σ.Γ. να σας επιστρέψει την κάρτα πίσω, εντούτοις μέχρι και τις 9 Οκτωβρίου, 2019 που ζητήσαμε διευκρίνιση γι' αυτό, η κάρτα δεν είχε επιστραφεί.

Στην επιστολή σας ημερ. 4 Νοεμβρίου, 2019, αναφέρατε ότι το πιο πάνω συμβάν ήταν αποτέλεσμα ανθρώπινου λάθους κατά την επικαιροποίηση του λογαριασμού, και όχι λάθους στις διαδικασίες ή στα συστήματα. Το ίδιο επαναλάβατε και με την επιστολή σας ημερ. 17 Ιανουαρίου, 2020 αναφέροντας ότι η Τράπεζα δεν εντόπισε άμεση ανάγκη διαφοροποίησης των συστημάτων και διαδικασιών της, αφού το περιστατικό οφείλεται σε ανθρώπινο λάθος και όχι σε οποιοδήποτε ελάττωμα του ίδιου του συστήματος ή των διαδικασιών που έχει θεσπίσει η Τράπεζα.

β) Warning message

Σε διευκρινίσεις που σας ζητήθηκαν σχετικά με τον τρόπο λειτουργίας του four-eye principle και του warning message, τα οποία υπήρχαν και λειτούργησαν ως μέτρα ασφαλείας, στην επιστολή σας ημερ. 9 Οκτωβρίου, 2019 αναφέρατε ότι *«ένα εξουσιοδοτημένο μέλος του προσωπικού (χρήστης 1) προβαίνει σε αλλαγή του αριθμού αναγνώρισης. Κατά την υποβολή της αλλαγής στο βήμα 1, και πριν προχωρήσει το σύστημα στο βήμα 2, γίνεται αυτόματος έλεγχος για υφιστάμενο πελάτη με τον νέο αριθμό αναγνώρισης. Εάν υπάρχει άλλος υφιστάμενος πελάτης, εμφανίζεται στην οθόνη του χρήστη 1 προειδοποιητικό μήνυμα «WARNING: AT LEAST ONE CUSTOMER EXISTS WITH THE NEW TRIFOLD». Σχετική εγκύκλιος της Τράπεζας, ημερομηνίας 02/03/2016, παρέχει κατευθυντήριες γραμμές για την ορθή διεκπεραίωση της διεργασίας και απαιτεί όπως ο χρήστης 1 επιβεβαιώσει τα στοιχεία των πελατών πριν προχωρήσει στην αλλαγή.* ***Για να προχωρήσει στο βήμα 2 η πιο πάνω διαδικασία, ο χρήστης 1 πρέπει να καταχωρήσει «Υ» στην οθόνη του συστήματος. Δεύτερο εξουσιοδοτημένο μέλος του προσωπικού (χρήστης 2), αυτόματα λαμβάνει στην οθόνη του την υφιστάμενη και την νέα τιμή των στοιχείων που αλλάζουν. Εγκρίνει την αλλαγή*** *όποτε και η αλλαγή εφαρμόζεται στο σύστημα ή την απορρίπτει οπότε η αλλαγή θεωρείται μη γενόμενη.»*

Με την επιστολή σας ημερ. 17 Ιανουαρίου, 2020, αναφέρατε ότι κατά τη δεύτερη καταχώρηση του ίδιου αριθμού διαβατηρίου την 2/5/19, το σύστημα παρουσίασε στην υπάλληλο προειδοποιητικό μήνυμα για την ύπαρξη του ίδιου διακριτικού αριθμού. Η υπάλληλος βασίστηκε στα έγγραφα που είχε στη διάθεση της και ενέκρινε την καταχώρηση του εν λόγω αριθμού. Η καταχώριση εγκρίθηκε και από δεύτερο υπάλληλο, ο οποίος όμως, όπως λέτε τώρα, σε αντίθεση με το τι αναφέρατε στις 9 Οκτωβρίου, 2019, δεν έλαβε οποιοδήποτε προειδοποιητικό μήνυμα και δεν είχε λόγο να αμφισβητήσει την ορθότητα της καταχώρησης. Προσθέσατε επίσης ότι κατά την καταχώρηση αριθμού διαβατηρίου ή ταυτότητας στο σύστημα, απαιτείται η συνεργασία δύο υπαλλήλων της Τράπεζας (four eye principle), ούτως ώστε ο ένας να εντοπίζει τυχόν λάθος του άλλου. **Ο πρώτος καταχωρεί τα στοιχεία στο σύστημα και ο δεύτερος τα εγκρίνει. Εάν προκύψει διακριτικός αριθμός που είναι ήδη καταχωρισμένος στο σύστημα, το σύστημα εμφανίζει σχετικό**

προειδοποιητικό μήνυμα στον υπάλληλο που προβαίνει στην καταχώρηση, αλλά όχι στον υπάλληλο που την εγκρίνει. Το σύστημα επιτρέπει την καταχώρηση, παρά την προειδοποίηση, αφού υπάρχουν περιπτώσεις που ο διακριτικός αριθμός συνδέεται με δύο ή περισσότερους πελάτες/πρόσωπα ή λογαριασμούς. **Εάν ο πρώτος υπάλληλος αποφασίσει να προχωρήσει με την καταχώρηση, ο δεύτερος υπάλληλος που καλείται να την εγκρίνει δεν λαμβάνει από το σύστημα αντίστοιχο προειδοποιητικό μήνυμα**.

γ) Λήψη γνώσης

Με την αποστολή του εντύπου Γνωστοποίησης Παραβίασης την 20 Σεπτεμβρίου, 2019 στο Γραφείο μου, την οποία χαρακτηρίσατε ως «Πλήρη» (όρος ο οποίος χρησιμοποιείται όταν έχει περατωθεί η διερεύνηση ενός περιστατικού και έχει διαφανεί τι το προκάλεσε), αναφέρατε ότι το περιστατικό επισυνέβη την 2/5/19, κατά προσέγγιση έληξε την 30/5/19, ενώ ο Υπεύθυνος Προστασίας Δεδομένων έλαβε **γνώση την 29/5/19 και ειδοποιήσατε την Αρχή την 20/9/19**. Αιτιολογήσατε την καθυστέρηση αυτή λόγω της πολυπλοκότητας του συμβάντος, η οποία είχε ως αποτέλεσμα να συμμετάσχουν στην έρευνα διάφορα τμήματα της Τράπεζας όπως η Υπηρεσία Ασφάλειας Πληροφοριών, το Κατάστημα της Τράπεζας στο οποίο εξυπηρετούνται οι πελάτες, το Γραφείο Προσωπικών Δεδομένων, το τμήμα Πληροφορικής, το Fraud Management Operations και η Μονάδα Διαχείρισης Λειτουργικών Κινδύνων.

Διαφοροποιήσατε την θέση σας και πάλι την 17 Ιανουαρίου, 2020, αναφέροντας ότι η εξέταση του περιστατικού συνεχίστηκε και μετά την υποβολή της Γνωστοποίησης (παρόλο που η Γνωστοποίηση που στάληκε την 20/9/19 χαρακτηρίστηκε ως «Πλήρης»), με σκοπό την πλήρη κατανόηση των σχετικών γεγονότων και καθορισμό οποιωνδήποτε μέτρων που θα μπορούσαν να ληφθούν προς βελτίωση των διαδικασιών. **Επαναλάβατε ότι η Τράπεζα ενημερώθηκε στις 29/5/19 αλλά προσθέσατε ότι το περιστατικό καταχωρίστηκε στο σχετικό σύστημα της Τράπεζας και ενημερώθηκε το γραφείο της Υπεύθυνης Προστασίας Δεδομένων της Τράπεζας (το «ΓΠΔ») στις 28/8/19 (δύο μέρες μετά τη δεύτερη φορά που ειδοποιηθήκατε από τον Σ.Γ. και τρεις μήνες μετά την πρώτη ενημέρωση από τον Σ.Γ. για το περιστατικό της διπλής καταγραφής), οπότε τότε ενεργοποιήθηκε ο μηχανισμός χειρισμού πιθανών παραβιάσεων προσωπικών δεδομένων.** Κατόπιν διερεύνησης και αξιολόγησης του περιστατικού σε συνεργασία με άλλα αρμόδια τμήματα της Τράπεζας, υποβλήθηκε η Γνωστοποίηση στο Γραφείο μου. **Προσθέσατε περαιτέρω ότι η Γνωστοποίηση στο Γραφείο μου, περιείχε τις πληροφορίες οι οποίες ήταν διαθέσιμες κατά τον ουσιώδη χρόνο και οι οποίες συνηγορούσαν στην υποβολή γνωστοποίησης.**

Αναφέρατε επίσης ότι λόγω του ότι η διερεύνηση του περιστατικού συνεχίστηκε και μετά την Γνωστοποίηση με αποτέλεσμα να διαφανεί ότι το περιστατικό αφορούσε λογαριασμό νομικού προσώπου και ότι η μόνη συνέπεια για φυσικό πρόσωπο ήταν η αποκάλυψη του ονοματεπωνύμου του κατόχου της σχετικής εταιρικής κάρτας, ενδεχομένως να μην χρειαζόταν καν να είχε υποβληθεί η γνωστοποίηση στο Γραφείο αφού, βάσει του **Άρθρου 33 του ΓΚΠΔ**, δεν απαιτείται γνωστοποίηση όταν η παραβίαση δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα των σχετικών φυσικών προσώπων.

2. Πιθανές συνέπειες

Δεν περιλαμβάνονται ευαίσθητα προσωπικά δεδομένα. Θεωρήσατε ότι η σοβαρότητα των πιθανών συνεπειών είναι μικρή. Την 20 Σεπτεμβρίου, 2019 αναφέρατε ότι τα δεδομένα που εκτέθηκαν ήταν ονοματεπώνυμο, διεύθυνση αλληλογραφίας, αριθμός κάρτας, iban, είδος κάρτας, νόμισμα, επιτόκιο, επιτόκιο καθυστερήσεων, ημερομηνία τελευταίας πληρωμής, σύνολο τελευταίας πληρωμής, ημερομηνία τελευταίας συναλλαγής, σύνολο συναλλαγών τρέχοντος μήνα, κατάσταση μέσω ταχυδρομείου, συσσωρευμένοι βαθμοί, βαθμοί που εξαργυρώθηκαν, διαθέσιμοι βαθμοί, κύρια ή συμπληρωματική κάρτα, κατάσταση κάρτας, ημερομηνία έκδοσης, ημερομηνία λήξης, όριο κύριας κάρτας, υπόλοιπο κάρτας, διαθέσιμο υπόλοιπο κύριας κάρτας, δεσμευμένο ποσό, καθυστερημένο ποσό, μόνιμη εντολή, λογαριασμός μόνιμης εντολής, ποσοστό μόνιμης εντολής και ελάχιστο ποσό πληρωμής.

Την 17 Ιανουαρίου, 2020 διαφοροποιήσατε και σε αυτό το σημείο την θέση σας αναφέροντας ότι τα στοιχεία που αποκαλύφθηκαν αφορούσαν εταιρικό λογαριασμό και ήταν ο αριθμός εταιρικού λογαριασμού, ο αριθμός εταιρικής χρεωστικής κάρτας συνδεδεμένης με τον εταιρικό λογαριασμό, ονοματεπώνυμο κατόχου εταιρικής χρεωστικής κάρτας (Μ.Κ.), ημερομηνία τελευταίας συναλλαγής εταιρικής χρεωστικής κάρτας και ημερομηνία λήξης εταιρικής χρεωστικής κάρτας. **Από τα πιο πάνω στοιχεία λέτε, προσωπικά δεδομένα αποτελούν μόνο τα στοιχεία που αφορούν τον ίδιο τον Μ.Κ. ως κάτοχο της εταιρικής χρεωστικής κάρτας, δηλαδή το ονοματεπώνυμο του**. Τα υπόλοιπα στοιχεία αφορούν τον εταιρικό λογαριασμό και την εταιρική χρεωστική κάρτα που ήταν συνδεδεμένη με αυτόν και επομένως δεν αποτελούν προσωπικά δεδομένα του Μ.Κ.. Προσθέσατε ότι ο Σ.Γ. δεν έλαβε γνώση οποιωνδήποτε συναλλαγών που διενεργήθηκαν μέσω του εταιρικού λογαριασμού ή με την χρεωστική κάρτα και η διεύθυνση που παρουσίαζε στο Web Banking του Σ.Γ. ήταν η δική του.

Επιπρόσθετα αναφέρατε ότι ο Μ.Κ. δεν έχει υποστεί οποιαδήποτε οικονομική ή άλλη ζημιά από την αποκάλυψη του ονόματος του στον Σ.Γ., ούτε και υπήρξε οποιοσδήποτε κίνδυνος βλάβης των δικαιωμάτων του Μ.Κ. εφόσον δεν υπήρχε δυνατότητα πρόσβασης σε στοιχεία προηγούμενων συναλλαγών ή εκτέλεσης νέων μη εξουσιοδοτημένων συναλλαγών, για τις οποίες απαιτείται επιπρόσθετος κωδικός ασφαλείας – one time password.

3. Το υποκείμενο των δεδομένων Μ.Κ. δεν έχει ειδοποιηθεί

Θεωρείτε ότι η σοβαρότητα των συνεπειών προς το υποκείμενο των δεδομένων είναι μικρή και γι' αυτό τον λόγο, παρόλο που σας ζητήθηκε από το Γραφείο μου με επιστολή ημερ. 24 Σεπτεμβρίου, 2019, δεν ειδοποιήθηκε το επηρεαζόμενο υποκείμενο των δεδομένων, εφόσον αναφέρατε με την επιστολή σας ημερ. 9 Οκτωβρίου, 2019, ότι:
«(α)Τα εμπλεκόμενα πρόσωπα δεν μπορούσαν να προβούν σε μη εξουσιοδοτημένες πράξεις/απάτη μέσω του Web Banking που θα είχαν ως αποτέλεσμα πιθανή οικονομική ζημιά λόγω των μέτρων που έχει η Τράπεζα στο σύστημα,
(β)Δεν υπήρχαν στοιχεία ταυτότητας που θα μπορούσαν να καταστήσουν εύκολη την ταυτοποίηση
(γ)Λήφθηκαν άμεσα μέτρα για την αντιμετώπιση του συμβάντος ως αυτά περιγράφονται στην γνωστοποίηση(όλα τα στοιχεία διορθώθηκαν στα συστήματα της Τράπεζας).»

4. Μέτρα που είχαν ληφθεί πριν το περιστατικό

Ως αναφέρατε υπήρχε το four-eye principle, warning message στο σύστημα στην περίπτωση που υπάρξουν διπλοί αριθμοί αναγνώρισης. Επίσης, το Γραφείο Προσωπικών Δεδομένων απέστειλε σε όλο το προσωπικό μήνυμα/Data Protection Awareness Message με σκοπό να τονίσει την σημασία της εμπιστευτικότητας για την Τράπεζα και την χρήση των προσωπικών δεδομένων μόνο για τους σκοπούς της εκτέλεσης των καθηκόντων τους και στο πλαίσιο των αρμοδιοτήτων που έχει ορίσει η Τράπεζα.

Επιπρόσθετα, η Τράπεζα έχει προβεί στη διεξαγωγή διαδικτυακού σεμιναρίου προς όλο το προσωπικό αναφορικά με την εφαρμογή του Γενικού Κανονισμού για τα προσωπικά δεδομένα.

Σε διευκρινίσεις που σας ζητήθηκαν απαντήσατε ότι *«η εκπαίδευση και η επιμόρφωση του προσωπικού της Τράπεζας γίνεται σε συνεχή βάση, μεταξύ άλλων, μέσω διαφόρων σεμιναρίων, αναθεώρησης πολιτικών, διαδικασιών και οδηγιών του Γραφείου Προσωπικών Δεδομένων. Σημειώνουμε ότι τα τελευταία σεμινάρια σχετικά με τον ΓΚΠΔ έχουν πραγματοποιηθεί από την Τράπεζα από τις 15/03/2019 μέχρι τις 03/05/2019 διαδικτυακά προς όλο το προσωπικό. Επιπλέον στις 4 Σεπτεμβρίου του 2019 ξεκίνησε από την Υπηρεσία Ασφάλειας Πληροφοριών σεμινάριο που αφορά την προστασία προσωπικών δεδομένων και Ασφάλειας Πληροφοριών το οποίο μέχρι σήμερα έχουν παρακολουθήσει 1738 υπάλληλοι της Τράπεζας. Το σεμινάριο είναι προγραμματισμένο να ολοκληρωθεί 14 Οκτωβρίου 2019.*

Επιπρόσθετα, το Γραφείο Προσωπικών Δεδομένων ετοιμάζει «Awareness Messages» τα οποία αποστέλλονται σε όλο το προσωπικό, ανά τακτά χρονικά διαστήματα. Στόχος της αποστολής των Awareness Messages είναι η επαγρύπνηση του προσωπικού σχετικά με τις υποχρεώσεις της Τράπεζας για συμμόρφωση με το ΓΚΠΔ.

Συγκεκριμένα στάλθηκαν τα εξής Awareness Messages:

- *Awareness Message το οποίο αφορούσε την τήρηση εμπιστευτικότητας αποστάλθηκε τον Δεκέμβριο του 2018.*
- *Awareness Message αναφορικά με το τι αποτελεί παραβίαση προσωπικών δεδομένων τον Μάρτιο του 2019.*
- *Awareness Message το οποίο αφορούσε τα δικαιώματα των φυσικών προσώπων σύμφωνα με το Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (εφεξής «ΓΚΠΔ») τον Ιούνιο του 2019.*
- *Awareness Message το οποίο αφορούσε την αποστολή προσωπικών δεδομένων μέσω ηλεκτρονικών μηνυμάτων τον Σεπτέμβριο του 2019.»*

5. Μέτρα για την αντιμετώπιση του περιστατικού

Μετά την ενημέρωση που λάβατε από τον Σ.Γ., ως αναφέρετε στην Γνωστοποίηση Παραβίασης ημερ. 20 Σεπτεμβρίου, 2019, προβήκατε σε: (α) αποκατάσταση και διόρθωση των δεδομένων, (β) ακύρωση της κάρτας και (γ) ζητήθηκε από τον Σ.Γ. να επιστρέψει την κάρτα στην Τράπεζα.

Επιπρόσθετα, με την επιστολή σας ημερ. 17 Ιανουαρίου, 2020 αναφέρατε ότι παρόλο που η Τράπεζα δεν εντόπισε άμεση ανάγκη διαφοροποίησης των συστημάτων και διαδικασιών της, εντούτοις έχουν αποσταλεί από τον Γενικό Διευθυντή του Τομέα Ιδιωτών της Τράπεζας, οδηγίες προς όλο το προσωπικό να είναι ιδιαίτερα προσεκτικό κατά την καταχώριση προσωπικών δεδομένων στα συστήματα της Τράπεζας, ούτως ώστε να αποφευχθούν κατά το δυνατό τέτοια περιστατικά. Προγραμματίζεται να γίνουν πιο εντατικές ενημερώσεις στο προσωπικό της Τράπεζας από το ΓΠΔ για θέματα που αφορούν τη διαχείριση προσωπικών δεδομένων κατά την ενημέρωση των συστημάτων της Τράπεζας και εξετάζεται η δυνατότητα λήψης επιπρόσθετων μέτρων με σκοπό την ενίσχυση της ασφάλειας των πληροφοριών στα συστήματα της Τράπεζας αλλά και η πιθανότητα, εάν αυτό είναι τεχνικά εφικτό, το προειδοποιητικό μήνυμα που αφορά κοινό διακριτικό αριθμό να παρουσιάζεται δύο φορές, και στον υπάλληλο που καταχωρεί τα στοιχεία στο σύστημα και σε αυτόν που τα εγκρίνει, για να ελαχιστοποιηθεί κατά το δυνατό η πιθανότητα να μην εντοπιστεί από έναν από τους δύο οποιοδήποτε λάθος ή απροσεξία.

6. Παραδοχή λαθών

Παραδέχεστε και αναγνωρίζετε με την επιστολή σας ημερ. 17 Ιανουαρίου, 2020 την **ανάγκη της Τράπεζας για άμεση ανάληψη δράσης για διερεύνηση περιστατικών** που αφορούν δεδομένα φυσικών προσώπων και για υποβολή σχετικής γνωστοποίησης στο Γραφείο μου εντός της προθεσμίας που καθορίζεται στο **Άρθρο 33 του ΓΚΠΔ 2016/679**, από το χρονικό σημείο που εξακριβώνεται με εύλογο βαθμό βεβαιότητας ότι έχει σημειωθεί παραβίαση προσωπικών δεδομένων. Αναγνωρίζετε επίσης το γεγονός ότι η παρούσα περίπτωση **(και ενόσω υπήρχε ακόμα η αντίληψη ότι το περιστατικό αφορούσε λογαριασμό φυσικού προσώπου)** υπήρξε καθυστέρηση στην υποβολή της Γνωστοποίησης. Αναφέρετε επίσης ότι η Τράπεζα θα λάβει τα απαραίτητα μέτρα για να διασφαλίσει ότι, εάν στο μέλλον απαιτηθεί υποβολή γνωστοποίησης στο γραφείο της Επιτρόπου, αυτή θα υποβληθεί εντός της σχετικής προθεσμίας, έστω και αν η Τράπεζα δεν έχει ακόμη στη διάθεση της όλες τις απαραίτητες πληροφορίες. Για τον σκοπό αυτό η Τράπεζα προτίθεται να προβεί σε περαιτέρω ενημερώσεις προς το προσωπικό, υπογραμμίζοντας την ευθύνη όλων για έγκαιρη αναγνώριση και καταχώριση στο σχετικό σύστημα της Τράπεζας πιθανών περιστατικών παραβίασης προσωπικών δεδομένων.

Παραδέχεστε επίσης ότι καμία από τις δύο δικλείδες ασφαλείας του συστήματος δεν εμπόδισε το λάθος που έγινε, **γιατί υπό τις συγκεκριμένες περιστάσεις οι δικλείδες ασφαλείας θα**

μπορούσαν να λειτουργήσουν αποτελεσματικά μόνο με τη συμβολή των εμπλεκόμενων υπαλλήλων της Τράπεζας. Ο υπάλληλος της Τράπεζας, λέτε, θα έπρεπε σύμφωνα με τις οδηγίες του Τμήματος Οργάνωσης και Διαδικασιών της Τράπεζας, να είχε διερευνήσει το λόγο παρουσίας του προειδοποιητικού μηνύματος ούτως ώστε να εντοπίσει το λάθος που είχε γίνει από τη συνάδελφο της στις 16/4/19 και έτσι να αποφευχθούν τα όσα ακολούθησαν. Καταλήγετε επί αυτού, ότι αιτία του περιστατικού ήταν το ανθρώπινο λάθος και απροσεξία κατά την εφαρμογή των διαδικασιών της Τράπεζας κατά την καταχώρηση στοιχείων στο σύστημα. Το ίδιο το σύστημα, αναφέρετε, δεν παρουσιάζει αδυναμία ή ελάττωμα, ενώ οι δικλείδες ασφαλείας του συστήματος δεν λειτούργησαν στην παρούσα περίπτωση λόγω των ενεργειών και αποφάσεων των εμπλεκόμενων υπαλλήλων.

7. Μετριαστικοί παράγοντες που εκτέθηκαν εκ μέρους σας

Δεν υπήρχε πρόθεση λέτε να αγνοηθεί ο ρόλος της Εποπτικής Αρχής και αντίθετα επιδιώκετε να έχετε άριστη συνεργασία με το Γραφείο μου, λαμβάνοντας σοβαρά υπόψιν την οποιαδήποτε καθοδήγηση και συστάσεις, με ανταπόκριση το συντομότερο δυνατόν σε ό,τι σας ζητηθεί.

Επικαλείστε ως αίτια του περιστατικού το ανθρώπινο λάθος κατά την εκτέλεση από υπάλληλο της Τράπεζας συγκεκριμένης εργασίας στα πλαίσια των καθηκόντων της (καταχώρηση των στοιχείων πελάτη στο σύστημα της Τράπεζας). Επικαλείστε επίσης ασυνήθιστες συγκεκριμένες περιστάσεις, οι οποίες δεν εμπόδισαν το λάθος το οποίο έγινε κατά την πληκτρολόγηση των στοιχείων στις 16/4/19, όταν ο νέος αριθμός διαβατηρίου του Σ.Γ. καταχωρίστηκε στο σύστημα της Τράπεζας ως αριθμός διαβατηρίου του Μ.Κ..

Μόνο κατά την διάρκεια του έτους 2019 έγιναν πέραν των 15000 καταχωρίσεων στο σύστημα της Τράπεζας. Το παρόν είναι ένα μεμονωμένο περιστατικό, ενώ παρόμοιες καταχωρίσεις στοιχείων πελατών στο σύστημα της Τράπεζας γίνονται επί καθημερινής βάσης εδώ και χρόνια. Η πιθανότητα να επαναληφθεί ένα τέτοιο περιστατικό είναι εξαιρετικά μικρή.

Τα δεδομένα αποκαλύφθηκαν για περιορισμένο χρονικό διάστημα, την 28/5/19 όταν ο Σ.Γ. συνδέθηκε με το σύστημα του Web Banking. Ο ίδιος ενημέρωσε την Τράπεζα και την επόμενη ημέρα η Τράπεζα έλαβε τα απαραίτητα μέτρα για τερματισμό της εν λόγω πρόσβασης.

Αφορά δύο υποκείμενα των δεδομένων/φυσικά πρόσωπα. Τον Σ.Γ. (για τον οποίο δεν έχουμε πληροφόρηση κατά πόσο ο Μ.Κ. είχε πρόσβαση στα στοιχεία του), τον Μ.Κ. (όνομα και στοιχεία χρεωστικής κάρτας), και τον εταιρικό λογαριασμό του Μ.Κ..

Ο Μ.Κ. λέτε δεν έχει υποστεί οποιαδήποτε οικονομική ή άλλη ζημιά από την αποκάλυψη του ονόματος του στον Σ.Γ. ούτε υπήρξε κίνδυνος βλάβης των δικαιωμάτων του (π.χ. να υπήρξε θύμα απάτης ή υποκλοπής ταυτότητας ή να υποστεί οποιαδήποτε βλάβη στη φήμη του ή δυσμενή διάκριση).

Δεν εξασφάλισε η Τράπεζα ή οποιοσδήποτε υπάλληλος της οποιοδήποτε οικονομικό ή άλλο όφελος.

Δεν υπήρχε δυνατότητα πρόσβασης σε στοιχεία προηγούμενων συναλλαγών ή εκτέλεσης νέων μη εξουσιοδοτημένων συναλλαγών, αφού απαιτείτο επιπρόσθετος κωδικός ασφάλειας – one time password.

Δεν πραγματοποιήθηκαν μη εξουσιοδοτημένες συναλλαγές και δεν υπήρξαν ή δύναται να υπάρξουν, οικονομικές συνέπειες στην εταιρεία – πελάτη που διατηρεί τον Εταιρικό Λογαριασμό με την Τράπεζα συνεπεία του συγκεκριμένου λάθους. Ούτε και υπήρξαν, ή δύνανται να υπάρξουν οποιεσδήποτε συνέπειες για τον Μ.Κ. ως κάτοχο της σχετικής εταιρικής κάρτας.

Δεν παρουσιάστηκαν στον Σ.Γ. οποιαδήποτε στοιχεία κίνησης ή άλλες συναλλαγές που έγιναν με την κάρτα.

Τέλος, αναφέρατε ότι ο πελάτης, τα πλείστα στοιχεία του οποίου τελικά αποκαλύφθηκαν, ήταν νομικό και όχι φυσικό πρόσωπο. Η μόνη συνέπεια για το φυσικό πρόσωπο, ήταν η αποκάλυψη του ονοματεπωνύμου του κατόχου της σχετικής εταιρικής κάρτας, όπου ενδεχομένως να μην χρειαζόταν καν να είχε υποβληθεί γνωστοποίηση στο Γραφείο μου με βάση το Άρθρο 33.

8. Σύνοψη γεγονότων μέχρι και την 17 Ιανουαρίου, 2020

Αποδεχόμενοι τα γεγονότα, ως αυτά έχουν αναφερθεί από εσάς μέχρι και την 17 Ιανουαρίου, 2020, τα περιστατικά που περιβάλλουν το υπό αναφορά συμβάν, έχουν ως εξής:

Το web banking του Μ.Κ. δημιουργήθηκε στις 29/06/2016. Στις 16/4/19, λόγω λάθους υπαλλήλου της Τράπεζας κατά την πληκτρολόγηση στοιχείων του Μ.Κ., καταχωρίστηκε εκ λάθους ως αριθμός διαβατηρίου του, ο νέος αριθμός διαβατηρίου του Σ.Γ.. Ο νέος αριθμός διαβατηρίου του Σ.Γ. μέχρι εκείνη την στιγμή δεν υπήρχε στα δεδομένα της Τράπεζας. Ο αριθμός αυτός καταχωρείτο για πρώτη φορά και γι' αυτό τον λόγο δεν εμφάνισε οποιαδήποτε προειδοποίηση. Την 2/5/19, επικαιροποιήθηκαν τα στοιχεία του Σ.Γ. Κατά την εν λόγω επικαιροποίηση, καταχωρίστηκε στα δεδομένα της Τράπεζας ο νέος αριθμός διαβατηρίου του Σ.Γ., για δεύτερη φορά, αφού υπήρχε ήδη στα δεδομένα της Τράπεζας, όταν καταχωρίστηκε στις 16/4/19 ως διακριτικός αριθμός του Μ.Κ.. Το σύστημα τότε παρουσίασε στην υπάλληλο προειδοποιητικό μήνυμα για την ύπαρξη άλλου πελάτη με τον ίδιο αριθμό. Η υπάλληλος, βασιζόμενη στο γεγονός ότι τα στοιχεία του Σ.Γ. επιβεβαιώνονταν από έγγραφα τα οποία είχε στη διάθεση της, προχώρησε στην επιβεβαίωση της καταχώρησης του νέου αριθμού διαβατηρίου, χωρίς να προβεί σε περαιτέρω διερεύνηση του προειδοποιητικού μηνύματος που είχε εμφανιστεί στην οθόνη του ηλεκτρονικού υπολογιστή. Η καταχώριση εγκρίθηκε και από δεύτερο υπάλληλο, ο οποίος όμως, δεν έλαβε οποιοδήποτε προειδοποιητικό μήνυμα και δεν είχε λόγο να αμφισβητήσει την ορθότητα της καταχώρησης. Σύμφωνα με το four eye principle, κατά την καταχώρηση αριθμού διαβατηρίου ή ταυτότητας στο σύστημα, απαιτείται η συνεργασία δύο υπαλλήλων της Τράπεζας, ούτως ώστε ο ένας να εντοπίζει τυχόν λάθος του άλλου. Ο πρώτος καταχωρεί τα στοιχεία στο σύστημα και ο δεύτερος τα εγκρίνει. Εάν προκύψει διακριτικός αριθμός που είναι ήδη καταχωρισμένος στο σύστημα, το σύστημα εμφανίζει σχετικό προειδοποιητικό μήνυμα στον υπάλληλο που προβαίνει στην καταχώρηση, αλλά όχι στον υπάλληλο που την εγκρίνει. Το σύστημα επιτρέπει την καταχώρηση, παρά την προειδοποίηση. Εάν ο πρώτος υπάλληλος αποφασίσει να προχωρήσει με την καταχώρηση, ο δεύτερος υπάλληλος που καλείται να την εγκρίνει δεν λαμβάνει από το σύστημα αντίστοιχο προειδοποιητικό μήνυμα.

Την 29/5/19 ειδοποιηθήκατε από τον Σ.Γ. ότι έβλεπε στοιχεία κάρτας και λογαριασμού του Μ.Κ. στο Web Banking του. Έγινε έρευνα και διαπιστώθηκε η διπλή καταχώρηση του αριθμού διαβατηρίου του Σ.Γ.. Ο Μ.Κ. δεν είχε προσωπικό λογαριασμό στην Τράπεζα, αλλά διατηρούσε λογαριασμό εταιρείας με τον οποίο ήταν συνδεδεμένη χρεωστική κάρτα, η οποία εκδόθηκε την 9/8/19 στο όνομα του. Τα στοιχεία τα οποία παρουσιάστηκαν στον Σ.Γ. μέσω της υπηρεσίας Web Banking, αφορούσαν τον εταιρικό λογαριασμό και όχι τον προσωπικό λογαριασμό του Μ.Κ. Δεν παρουσιάστηκαν στον Σ.Γ. οποιαδήποτε στοιχεία κίνησης του εταιρικού λογαριασμού ή της εταιρικής κάρτας και η μόνη φορά που είχε εξασφαλίσει πρόσβαση ο Σ.Γ. στην υπηρεσία Web Banking μετά τις 2/3/19, ήταν στις 28/5/19, μια μέρα πριν ενημερώσει την Τράπεζα. Παρόλο που όταν ειδοποιηθήκατε στις 29/5/19 και διορθώθηκε ο αριθμός διαβατηρίου του Μ.Κ. έτσι ώστε τα στοιχεία του Μ.Κ. να μην παρουσιάζονται στο Web Banking του Σ.Γ., εντούτοις οι υπάλληλοι της Τράπεζας δεν προχώρησαν και στη διόρθωση της διευθύνσεως του Μ.Κ.. Αποτέλεσμα αυτού, όταν στις 9/8/19 εκδόθηκε νέα κάρτα στο όνομα του Μ.Κ., αυτή αποστάληκε στη διεύθυνση του Σ.Γ. Ο Σ.Γ. σας ενημέρωσε για ακόμη μια φορά στις 26/8/19, για την παραλαβή τώρα της κάρτας του Μ.Κ.. Τότε, προχωρήσατε σε ακύρωση της κάρτας και διόρθωση της διεύθυνσης του Μ.Κ. Ζητήσατε από τον Σ.Γ. να σας επιστρέψει την κάρτα πίσω, εντούτοις μέχρι και τις 9 Οκτωβρίου, 2019, η κάρτα δεν είχε επιστραφεί.

Ως αναφέρεται ανωτέρω, η Τράπεζα ενημερώθηκε από τον Σ.Γ. για πρώτη φορά στις 29/5/19 και για δεύτερη φορά στις 26/8/19. Το περιστατικό καταχωρίστηκε στο σχετικό σύστημα της Τράπεζας και ενημερώθηκε το γραφείο της Υπεύθυνης Προστασίας Δεδομένων της Τράπεζας στις 28/8/19

οπότε τότε ενεργοποιήθηκε ο μηχανισμός χειρισμού πιθανών παραβιάσεων προσωπικών δεδομένων. Κατόπιν διερεύνησης και αξιολόγησης του περιστατικού σε συνεργασία με άλλα αρμόδια τμήματα της Τράπεζας, υποβλήθηκε η Γνωστοποίηση στο γραφείο της Επιτρόπου την 20/9/19 την οποία χαρακτηρίσατε ως «Πλήρη». Ζητήθηκαν περαιτέρω διευκρινίσεις από το Γραφείο μου με επιστολές ημερ. 24/9/19 και 15/10/19 οι οποίες απαντήθηκαν με αντίστοιχες επιστολές σας ημερ. 9/10/19 και 4/11/19. Την 16/12/19 εξέδωσα εκ πρώτης όψεως απόφαση, σύμφωνα με την οποία κατέληγα ότι, με βάση τα μέχρι τις 16/12/19 δεδομένα, φαίνεται να υπήρξε παραβίαση εκ μέρους της Τράπεζας των **Άρθρων 32 παρ. 1(β) και 33 παρ. 1 του ΓΚΠΔ 2016/679** και κληθήκατε να προβάλετε τους λόγους για τους οποίους πιστεύετε ότι δεν θα πρέπει να επιβληθεί οποιοδήποτε διορθωτικό μέτρο ή διοικητική κύρωση, καθώς και όπως με πληροφορήσετε για τον κύκλο εργασιών της Ελληνικής Τράπεζας για το προηγούμενο οικονομικό έτος. Την 17/1/20 εκθέσατε τους μετριαστικούς παράγοντες, αλλά και νέα διαφοροποιημένα δεδομένα, τα οποία ενσωματώθηκαν στα αρχικά γεγονότα, ως αυτά αναφέρθηκαν από εσάς.

9. Νομική Πτυχή

Το **Άρθρο 4 του ΓΚΠΔ 2016/679**, ορίζει ότι «δεδομένα προσωπικού χαρακτήρα» είναι «*κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (υποκείμενο των δεδομένων)»*. Στο ίδιο άρθρο επίσης ορίζεται ως 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»*. Περαιτέρω, ως υπεύθυνος επεξεργασίας ορίζεται οποιοσδήποτε (το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας) που, *«μόνος ή από κοινού με άλλον, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα»*. Στο ίδιο άρθρο ορίζεται η παραβίαση δεδομένων προσωπικού χαρακτήρα ως *«η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία»*.

Οι αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα ορίζονται στο **Άρθρο 5 παρ. 1 του ΓΚΠΔ 2016/679**. Στο **εδάφιο στ) του Άρθρου 5**, αναφέρεται συγκεκριμένα ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να *«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»)*. Περαιτέρω, στην παράγραφο 2 του ίδιου άρθρου, αναφέρεται ότι ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 («λογοδοσία»).

Το **Άρθρο 24 του ΓΚΠΔ 2016/679** αναφέρεται στην ευθύνη του υπεύθυνου επεξεργασίας να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό και εκεί όπου χρειάζεται, τα μέτρα αυτά να επανεξετάζονται και επικαιροποιούνται. Όταν δικαιολογείται σε σχέση με τις δραστηριότητες επεξεργασίας, τα εφαρμοστέα μέτρα, περιλαμβάνουν και την εφαρμογή κατάλληλων πολιτικών. Η τήρηση δε εγκεκριμένων κωδίκων δεοντολογίας όπως αναφέρεται στο Άρθρο 40 ή εγκεκριμένου μηχανισμού πιστοποίησης όπως αναφέρεται στο Άρθρο 42 του ΓΚΠΔ 2016/679, δύναται να χρησιμοποιηθεί ως στοιχείο για την απόδειξη της συμμόρφωσης με τις υποχρεώσεις του υπευθύνου επεξεργασίας.

Στο **Άρθρο 29** αναφέρεται επίσης ότι *«κάθε πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, επεξεργάζεται τα εν λόγω δεδομένα μόνον κατ' εντολή του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους*

μέλους.», ενώ ομοίως στο **Άρθρο 32 παρ. 4** αναφέρεται ότι *«Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία λαμβάνουν μέτρα ώστε να διασφαλίζεται ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα τα επεξεργάζεται μόνο κατ' εντολή του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους.»*

Σύμφωνα με το **Άρθρο 32 παρ. 1(β) του ΓΚΠΔ 2016/679**, θα πρέπει ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία να *«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»* λαμβάνοντας υπόψη τους κινδύνους *«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.»* (**Άρθρο 32 παρ. 2**).

Περαιτέρω, σύμφωνα με το **Άρθρο 33 παρ. 1 του ΓΚΠΔ 2016/679**, σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας πρέπει να *«γνωστοποιεί αμελλητί και, αν είναι δυνατό, **εντός 72 ωρών** από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή που είναι αρμόδια σύμφωνα με το άρθρο 55, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση.»* Σύμφωνα με την αιτιολογική σκέψη (85) *«…Εάν μια τέτοια γνωστοποίηση δεν μπορεί να επιτευχθεί εντός 72 ωρών, η γνωστοποίηση θα πρέπει να συνοδεύεται από αιτιολογία η οποία αναφέρει τους λόγους της καθυστέρησης και οι πληροφορίες μπορούν να παρέχονται σταδιακά χωρίς αδικαιολόγητη καθυστέρηση.»* Σχετικό είναι και το **Άρθρο 33 παρ. 4** του Κανονισμού το οποίο αναφέρει ότι *«Σε περίπτωση που και εφόσον δεν είναι δυνατόν να παρασχεθούν οι πληροφορίες ταυτόχρονα, μπορούν να παρέχονται σταδιακά χωρίς αδικαιολόγητη καθυστέρηση.»*

Σύμφωνα με το **Άρθρο 34 παρ. 3 του ΓΚΠΔ 2016/679** *«Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα **ενδέχεται να θέσει σε υψηλό κίνδυνο** τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων.»* Εξαίρεση υπάρχει στην περίπτωση που ο υπεύθυνος επεξεργασίας (α) εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας τέτοιας φύσεως που να καθιστούν μη κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, (β) έλαβε στη συνέχεια μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει ο αναφερόμενος στην παράγραφο 1 υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και (γ) η ανακοίνωση προϋποθέτει δυσανάλογες προσπάθειες. Σε μια τέτοια περίπτωση, η ανακοίνωση μπορεί να γίνει δημόσια ή με τέτοιο τρόπο ώστε τα υποκείμενα των δεδομένων να ενημερωθούν με εξίσου αποτελεσματικό τρόπο.

Στο **Άρθρο 38 του ΓΚΠΔ 2016/679**, μεταξύ άλλων, αναφέρεται ότι *«Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία διασφαλίζουν ότι ο υπεύθυνος προστασίας δεδομένων συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα.»* αλλά και *«στηρίζουν τον υπεύθυνο προστασίας δεδομένων στην άσκηση των καθηκόντων που αναφέρονται στο άρθρο 39 παρέχοντας απαραίτητους πόρους για την άσκηση των εν λόγω καθηκόντων και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας, καθώς και πόρους απαραίτητους για τη διατήρηση της εμπειρογνωσίας του.»*

9.1. Κατευθυντήριες Γραμμές – Λήψη Γνώσης

Σε ότι αφορά **στο θέμα «γνώσης»** και το κατά πόσο έχει αποκτήσει ή όχι γνώση της παραβίασης ο ΥΠΔ, σχετική κατεύθυνση δίνεται μέσα από τις «Κατευθυντήριες γραμμές» που εξέδωσε το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων σχετικά με την γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα, την 3 Οκτωβρίου, 2017 και αναθεωρήθηκαν την 6 Φεβρουαρίου, 2018, όπου αναφέρεται ότι:

«Το ακριβές χρονικό σημείο όπου ένας υπεύθυνος επεξεργασίας μπορεί να θεωρείται ότι αποκτά «γνώση» μιας συγκεκριμένης παραβίασης θα εξαρτάται από τις περιστάσεις της συγκεκριμένης παραβίασης. Σε ορισμένες περιπτώσεις, θα προκύπτει με σχετική σαφήνεια από την αρχή ότι έχει διαπραχθεί παραβίαση, ενώ, σε άλλες, ενδέχεται να χρειάζεται κάποιος χρόνος για να διαπιστωθεί εάν τα δεδομένα προσωπικού χαρακτήρα έχουν τεθεί σε κίνδυνο. Ωστόσο, η έμφαση θα πρέπει να δίνεται στην έγκαιρη ανάληψη δράσης για τη διερεύνηση ενός περιστατικού, ώστε να διαπιστωθεί κατά πόσο τα δεδομένα προσωπικού χαρακτήρα έχουν παραβιαστεί και, σε τέτοια περίπτωση, να λαμβάνονται διορθωτικά μέτρα και να γίνεται γνωστοποίηση, εάν απαιτείται. … Αφού ενημερώθηκε πρώτα για πιθανή παραβίαση από πρόσωπο, έναν οργανισμό μέσων ενημέρωσης ή άλλη πηγή ή όταν έχει εντοπίσει ο ίδιος ένα περιστατικό ασφάλειας, ***ο υπεύθυνος επεξεργασίας μπορεί να διενεργήσει έρευνα μικρής χρονικής διάρκειας για να διαπιστώσει εάν έχει όντως διαπραχθεί παραβίαση.*** *Κατά τη διάρκεια αυτής της περιόδου έρευνας, ο υπεύθυνος επεξεργασίας δεν μπορεί να θεωρείται ότι έχει αποκτήσει «γνώση».* ***Ωστόσο, αναμένεται ότι η αρχική έρευνα θα πρέπει να ξεκινά το συντομότερο δυνατό και να εξακριβώνεται με εύλογο βαθμό βεβαιότητας εάν έχει σημειωθεί παραβίαση· στη συνέχεια, μπορεί να ακολουθήσει πιο ενδελεχής έρευνα. Μόλις ο υπεύθυνος επεξεργασίας αποκτήσει γνώση, μια γνωστοποιήσιμη παραβίαση πρέπει να γνωστοποιείται αμελλητί και, ει δυνατόν, το αργότερο εντός 72 ωρών.*** *Κατά τη διάρκεια αυτής της περιόδου, ο υπεύθυνος επεξεργασίας θα πρέπει να αξιολογεί τον πιθανό κίνδυνο για τα πρόσωπα, ώστε να προσδιορίζει εάν έχει ενεργοποιηθεί η απαίτηση για γνωστοποίηση, καθώς και τις ενέργειες που απαιτούνται για την αντιμετώπιση της παραβίασης.»*

«Παρότι ο ΓΚΠΔ επιτρέπει σε ορισμένο βαθμό την υποβολή γνωστοποιήσεων με καθυστέρηση, το γεγονός αυτό δεν θα πρέπει να οδηγεί στο συμπέρασμα ότι πρόκειται για κάτι που συμβαίνει τακτικά.»

9.2 Κατευθυντήριες Γραμμές - Αξιολόγηση κινδύνου και υψηλού κινδύνου

Σύμφωνα με τις «Κατευθυντήριες Γραμμές» γνωστοποίηση παραβίασης δεν απαιτείται να γίνεται σε όλες τις περιστάσεις. Ως αναφέρεται:

- *Απαιτείται γνωστοποίηση στην αρμόδια εποπτική αρχή, εκτός εάν η παραβίαση δεν ενδέχεται να επιφέρει* ***κίνδυνο*** *για τα δικαιώματα και τις ελευθερίες των προσώπων.*
- *Η ανακοίνωση μιας παραβίασης στο πρόσωπο πρέπει να γίνεται μόνο εάν η παραβίαση ενδέχεται να επιφέρει* ***υψηλό κίνδυνο*** *για τα δικαιώματα και τις ελευθερίες του.*

Σε ότι αφορά το θέμα της μη ανακοίνωσης της παραβίασης προς τον υποκείμενο των δεδομένων με βάση τις εξαιρέσεις του Άρθρου 34 παρ.3, οι Κατευθυντήριες Γραμμές διευκρινίζουν ότι σε μια τέτοια περίπτωση *«οι υπεύθυνοι επεξεργασίας θα πρέπει να μπορούν να αποδεικνύουν στην εποπτική αρχή ότι πληρούν μία ή περισσότερες από αυτές τις προϋποθέσεις. Θα πρέπει επίσης να λαμβάνεται υπόψιν ότι, ενώ μπορεί αρχικά να μην απαιτείται γνωστοποίηση εάν δεν υπάρχει κανένας κίνδυνος για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, αυτό το δεδομένο μπορεί να αλλάξει με την πάροδο του χρόνου και ο κίνδυνος θα πρέπει να αξιολογείται εκ νέου. Εάν ένας υπεύθυνος επεξεργασίας αποφασίσει να μην ανακοινώσει μια παραβίαση στο πρόσωπο, το άρθρο 34 παράγραφος 4 εξηγεί ότι η εποπτική αρχή μπορεί να του ζητήσει να το πράξει, εάν θεωρεί ότι η παραβίαση είναι πιθανό να επιφέρει υψηλό κίνδυνο για τα πρόσωπα. Εναλλακτικά, ενδέχεται να θεωρήσει ότι οι προϋποθέσεις του άρθρου 34 παράγραφος 3 έχουν ικανοποιηθεί, περίπτωση στην οποία δεν απαιτείται ανακοίνωση στα πρόσωπα. Εάν η εποπτική αρχή αποφασίσει ότι η απόφαση για τη μη ανακοίνωση στα υποκείμενα των δεδομένων δεν είναι δεόντως αιτιολογημένη, ενδέχεται να εξετάσει το ενδεχόμενο να ασκήσει τις εξουσίες που έχει στη διάθεσή της και να επιβάλει κυρώσεις.»*

Είναι ευθύνη του υπεύθυνου επεξεργασίας, να αξιολογήσει τον κίνδυνο που θα μπορούσε να προκύψει από το συμβάν, έτσι ώστε να μπορεί να προβεί σε αποτελεσματικές ενέργειες για τον περιορισμό και την αντιμετώπιση της παραβίασης, αλλά και να βοηθηθεί να προσδιορίσει εάν απαιτείται γνωστοποίηση στην εποπτική αρχή και, εάν είναι απαραίτητο, ανακοίνωση στα ενδιαφερόμενα πρόσωπα

Υψηλός κίνδυνος, υφίσταται όταν η παραβίαση ενδέχεται να οδηγήσει σε σωματική, υλική ή ηθική βλάβη για τα πρόσωπα τα δεδομένων των οποίων έχουν παραβιαστεί και εξαρτάται από παράγοντες όπως (α) το είδος της παραβίασης, (β) τη φύση, ευαισθησία και όγκο των δεδομένων, (γ) την ευκολία ταυτοποίησης των προσώπων, (δ) την σοβαρότητα των συνεπειών για τα πρόσωπα, (ε) τα ειδικά χαρακτηριστικά του προσώπου, (στ) τα ειδικά χαρακτηριστικά του υπεύθυνου επεξεργασίας και (ζ) τον αριθμό των επηρεαζόμενων προσώπων. Οι πιο πάνω παράγοντες θα πρέπει να εξετάζονται συνδυαστικά. Για παράδειγμα, παραβιάσεις που αφορούν δεδομένα υγείας, έγγραφα ταυτότητας ή οικονομικά δεδομένα, **όπως στοιχεία πιστωτικών καρτών**, μπορούν και από μόνα τους να προκαλέσουν βλάβη, αλλά, εάν χρησιμοποιηθούν συνδυαστικά, θα μπορούσαν να χρησιμοποιηθούν για την υποκλοπή ταυτότητας. Ένας συνδυασμός δεδομένων προσωπικού χαρακτήρα παρουσιάζει συνήθως μεγαλύτερη ευαισθησία από ένα μόνο δεδομένο προσωπικού χαρακτήρα. Όσο σοβαρότερες και πιθανότερο είναι να προκύψουν συνέπειες στα δικαιώματα και στις ελευθερίες των προσώπων, τόσο ψηλότερος είναι και ο κίνδυνος που προκύπτει. Περαιτέρω καθοδήγηση προς τον σκοπό αξιολόγησης της σοβαρότητας μιας παραβίασης, παρέχει ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)[1].

9.3 Κατευθυντήριες Γραμμές - Γνωστοποίηση Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα

Σε ότι αφορά στην αποστολή Γνωστοποίησης Παραβίασης Δεδομένων προς τις Εποπτικές Αρχές, συμφώνως των προνοιών του **Άρθρου 33 παρ.1**, στις Κατευθυντήριες Γραμμές αναφέρονται τα πιο κάτω:

«… ο ΓΚΠΔ αναγνωρίζει ότι οι υπεύθυνοι επεξεργασίας δεν θα έχουν πάντα όλες τις απαραίτητες πληροφορίες σχετικά με μια παραβίαση εντός 72 ωρών από τη στιγμή που απέκτησαν γνώση αυτής, καθώς οι πλήρεις και ολοκληρωμένες λεπτομέρειες του περιστατικού ενδέχεται να μην είναι πάντα διαθέσιμες κατά τη διάρκεια αυτής της αρχικής περιόδου. Ως εκ τούτου, ***επιτρέπει τη σταδιακή γνωστοποίηση****. Αυτό είναι πιο πιθανό να συμβαίνει στην περίπτωση παραβιάσεων με πιο περίπλοκο χαρακτήρα, όπως ορισμένα περιστατικά κυβερνοασφάλειας όπου, για παράδειγμα, ενδέχεται να απαιτείται διεξοδική εγκληματολογική έρευνα ώστε να διαπιστωθούν πλήρως η φύση της παραβίασης και ο βαθμός στον οποίο τα δεδομένα προσωπικού χαρακτήρα έχουν τεθεί σε κίνδυνο. Συνεπώς, σε πολλές περιπτώσεις, ο υπεύθυνος επεξεργασίας θα πρέπει να διεξάγει περαιτέρω έρευνα και να δίνει συνέχεια με πρόσθετες πληροφορίες που θα αποκτά σε μεταγενέστερο στάδιο.* ***Αυτό επιτρέπεται εφόσον ο υπεύθυνος επεξεργασίας αιτιολογεί την καθυστέρηση, σύμφωνα με το άρθρο 33 παράγραφος 1****. Η ΟΕ29 θεωρεί ότι, όταν ο υπεύθυνος επεξεργασίας ενημερώνει για πρώτη φορά την εποπτική αρχή, θα πρέπει να ενημερώνει επίσης την εποπτική αρχή εάν ο ίδιος δεν διαθέτει ακόμη όλες τις απαιτούμενες πληροφορίες και ότι θα παράσχει περισσότερες λεπτομέρειες σε μεταγενέστερο στάδιο. Η εποπτική αρχή θα πρέπει να συμφωνήσει όσον αφορά τον τρόπο και τον χρόνο με τον οποίο θα πρέπει να παρέχονται οι πρόσθετες πληροφορίες.* *Το γεγονός αυτό δεν εμποδίζει τον υπεύθυνο επεξεργασίας από το να παρέχει περαιτέρω πληροφορίες σε οποιοδήποτε άλλο στάδιο, εάν λάβει γνώση πρόσθετων σχετικών λεπτομερειών για την παραβίαση οι οποίες πρέπει να παρασχεθούν στην εποπτική αρχή.*
Η απαίτηση γνωστοποίησης θα πρέπει να εστιάζει στο να ενθαρρύνει τους υπευθύνους επεξεργασίας να ενεργούν άμεσα σε περίπτωση παραβίασης, να την περιορίζουν και, εάν είναι δυνατόν, να ανακτούν τα δεδομένα προσωπικού χαρακτήρα που έχουν τεθεί σε κίνδυνο, καθώς και ζητούν σχετικές συμβουλές από την εποπτική αρχή. Η γνωστοποίηση στην εποπτική αρχή εντός των πρώτων 72 ωρών μπορεί να παράσχει στον υπεύθυνο επεξεργασίας τη δυνατότητα να βεβαιωθεί ότι οι αποφάσεις σχετικά με την ενημέρωση ή μη των προσώπων είναι ορθές.»

«Θα πρέπει επίσης να είναι σαφές ότι, ***μετά την αρχική γνωστοποίηση, ένας υπεύθυνος επεξεργασίας θα μπορούσε να ενημερώνει την εποπτική αρχή εάν, στο πλαίσιο έρευνας παρακολούθησης, προκύψουν στοιχεία ότι το περιστατικό ασφάλειας ήταν περιορισμένο και στην πραγματικότητα δεν συνέβη παραβίαση. Αυτές οι πληροφορίες θα μπορούσαν στη συνέχεια να προστεθούν στις πληροφορίες που***

[1] ENISA, Συστάσεις για μια μεθοδολογία αξιολόγησης της σοβαρότητας των παραβιάσεων δεδομένων προσωπικού χαρακτήρα, https://www.enisa.europa.eu/publications/dbn-severity

έχουν ήδη παρασχεθεί στην εποπτική αρχή και το περιστατικό να καταγραφεί, συνεπώς, ως μη παραβίαση. *Δεν προβλέπεται κύρωση για την αναφορά συμβάντος που εν τέλει προκύπτει ότι δεν συνιστά παραβίαση.»*

«Το άρθρο 33 παράγραφος 1 καθιστά σαφές ότι ***όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση. Το γεγονός αυτό, σε συνδυασμό με την προσέγγιση της σταδιακής γνωστοποίησης, συνεπάγεται την αναγνώριση ότι ένας υπεύθυνος επεξεργασίας ενδέχεται να μην είναι πάντα σε θέση να γνωστοποιήσει μια παραβίαση εντός του συγκεκριμένου χρονικού διαστήματος και ότι μπορεί να γίνει αποδεκτή μια καθυστερημένη γνωστοποίηση.***
Αυτό μπορεί να συμβαίνει όταν, για παράδειγμα, ένας υπεύθυνος επεξεργασίας έρχεται αντιμέτωπος με πολλαπλές, παρεμφερούς φύσεως παραβιάσεις της εμπιστευτικότητας σε σύντομο χρονικό διάστημα, οι οποίες επηρεάζουν μεγάλο αριθμό υποκειμένων των δεδομένων κατά τον ίδιο τρόπο. Ένας υπεύθυνος επεξεργασίας θα μπορούσε να αποκτήσει γνώση μιας παραβίασης και, ενώ έχει ξεκινήσει να τη διερευνά, και πριν από τη γνωστοποίηση, να εντοπίσει κι άλλες παρεμφερείς παραβιάσεις, οι οποίες οφείλονται σε διαφορετικές αιτίες. *Ανάλογα με τις περιστάσεις, ο υπεύθυνος επεξεργασίας ενδέχεται να χρειαστεί κάποιο χρόνο για να διαπιστώσει την έκταση των παραβιάσεων και, αντί να γνωστοποιήσει κάθε παραβίαση ξεχωριστά, διαμορφώνει μια ουσιαστική γνωστοποίηση η οποία αφορά διάφορες πολύ παρεμφερείς παραβιάσεις, με πιθανώς διαφορετικές αιτίες. Το γεγονός αυτό θα μπορούσε να έχει ως αποτέλεσμα τη γνωστοποίηση στην εποπτική αρχή με καθυστέρηση μεγαλύτερη των 72 ωρών αφότου ο υπεύθυνος επεξεργασίας απέκτησε για πρώτη φορά γνώση αυτών των παραβιάσεων.»*

9.4 Κατευθυντήριες Γραμμές - Ο ρόλος του Υπεύθυνου Προστασίας Δεδομένων

Σύμφωνα και πάλι με τις «Κατευθυντήριες Γραμμές» ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ), μεταξύ άλλων, έχει καθήκον να παρέχει συμβουλές και πληροφορίες για την προστασία των δεδομένων στον υπεύθυνο επεξεργασίας, να συνεργάζεται με την εποπτική αρχή και να λειτουργεί ως σημείο επαφής για την εποπτική αρχή και τα υποκείμενα των δεδομένων. Διαδραματίζει επίσης σημαντικό ρόλο ως προς την αποτροπή μιας παραβίασης ή την προετοιμασία για την αντιμετώπιση μιας παραβίασης, παρέχοντας συμβουλές και παρακολουθώντας τη συμμόρφωση κατά τη διάρκεια μιας παραβίασης (δηλαδή κατά τη γνωστοποίηση στην εποπτική αρχή) και κατά τη διάρκεια οποιασδήποτε μεταγενέστερης έρευνας από την εποπτική αρχή. **Ο υπεύθυνος προστασίας δεδομένων πρέπει να ενημερώνεται άμεσα σχετικά με την ύπαρξη παραβίασης και να συμμετέχει στη διαδικασία διαχείρισης και γνωστοποίησης της παραβίασης**.

10. Σκεπτικό/Σχόλια

(α) Σύμφωνα με τις Κατευθυντήριες Γραμμές, ο ΓΚΠΔ επιτρέπει την σταδιακή γνωστοποίηση περιστατικού παραβίασης, στην περίπτωση που ο υπεύθυνος επεξεργασίας δεν έχει όλες τις απαραίτητες πληροφορίες σχετικά με την παραβίαση και εντός του χρονικού πλαισίου που ορίζει το **Άρθρο 33 παρ. 1**, των 72 ωρών από την στιγμή που απέκτησε γνώση γι' αυτό, ιδίως όταν πρόκειται για περίπλοκες περιπτώσεις (π.χ. περιστατικό κυβερνοασφάλειας) ή/και όταν έρχεται αντιμέτωπος με πολλαπλές, παρεμφερούς φύσεως παραβιάσεις της εμπιστευτικότητας σε σύντομο χρονικό διάστημα, οι οποίες επηρεάζουν μεγάλο αριθμό υποκειμένων των δεδομένων κατά τον ίδιο τρόπο.

Στην παρούσα περίπτωση, είχε Γνωστοποιηθεί το Περιστατικό της Παραβίασης στο Γραφείο μου στις 20/9/19, ένα μήνα δηλαδή μετά που το Γραφείο του Υπεύθυνου Προστασίας Δεδομένων της Τράπεζας έλαβε γνώση για το συμβάν, και σχεδόν τέσσερεις μήνες μετά που η Τράπεζα ειδοποιήθηκε για πρώτη φορά από τον Σ.Γ., δηλαδή στις 28/5/19. Αιτιολογήσατε την καθυστέρηση αυτή λόγω της πολυπλοκότητας του συμβάντος, η οποία είχε ως αποτέλεσμα να συμμετάσχουν στην έρευνα διάφορα τμήματα της Τράπεζας όπως η Υπηρεσία Ασφάλειας Πληροφοριών, το Κατάστημα της Τράπεζας στο οποίο εξυπηρετούνται οι πελάτες, το Γραφείο Προσωπικών Δεδομένων, το τμήμα Πληροφορικής, το Fraud Management Operations και η Μονάδα Διαχείρισης Λειτουργικών Κινδύνων, παρόλο που το περιστατικό αφορούσε σε δύο φυσικά πρόσωπα και μία νομική οντότητα συνδεδεμένη με ένα εξ αυτών.

Η Γνωστοποίηση χαρακτηρίστηκε ως «Πλήρης», δηλαδή ως τέτοια της οποίας η διερεύνηση είχε ολοκληρωθεί, και ο υπεύθυνος επεξεργασίας κατείχε όλες τις απαραίτητες πληροφορίες σχετικά με την παραβίαση. Το γεγονός αυτό (ότι η διερεύνηση είχε ολοκληρωθεί), ενισχύεται και από τον τρόπο με τον οποίο ο υπεύθυνος προστασίας δεδομένων απαντούσε στις σχετικές διευκρινίσεις που ζητήθηκαν από το Γραφείο μου με τις δύο επιστολές ημερ. 24/9/19 και 15/10/19. Σε καμία από τις δύο απαντήσεις της Τράπεζας δεν τέθηκαν ενώπιον μου τα νέα, διαφοροποιημένα στοιχεία τα οποία τέθηκαν στις 17/1/20, ούτε και αναφέρθηκε στο Γραφείο μου ότι η διερεύνηση του συμβάντος συνεχίζεται, με ενδεχόμενο να προκύψουν νέα δεδομένα σχετικά με τις συνθήκες υπό τις οποίες επεσυνέβη η παραβίαση. Σύμφωνα και με τις Κατευθυντήριες Γραμμές, συμπληρωματικά/σταδιακά στοιχεία θα μπορούσαν να προσκομιστούν εφόσον καταχωρείτο Αρχική Γνωστοποίηση, αιτιολογείτο η οποιαδήποτε καθυστέρηση της ολοκλήρωσης της έρευνας και ενημερώνετο η Εποπτική Αρχή για το γεγονός της απουσίας ολοκληρωμένης εικόνας σε σχέση με το περιστατικό. Η Εποπτική Αρχή θα έπρεπε να είχε συμφωνήσει όσον αφορά στον τρόπο και χρόνο με τον οποίο θα παρέχοντο οι πρόσθετες πληροφορίες.

Στην παρούσα περίπτωση, κάτι τέτοιο δεν είχε γίνει. Η Τράπεζα, όχι μόνο ξεπέρασε κατά πολύ το χρονικό περιθώριο των 72 ωρών που προβλέπει το **Άρθρο 33 παρ. 1**, αλλά ούτε τήρησε τις πρέπουσες διαδικασίες, ως αναφέρονται ανωτέρω, αγνοώντας τον ρόλο της Εποπτικής Αρχής. Ενεργώντας με τον τρόπο με τον οποίο ενήργησε η Ελληνική Τράπεζα, ενέκρινε από μόνη της παράταση χρόνου. Παραγνώρισε επίσης τον ρόλο του Υπεύθυνου Προστασίας Δεδομένων, εφόσον καθυστέρησε να ενεργοποιήσει τον μηχανισμό πληροφόρησης του για το εν λόγω συμβάν. Υπάρχει και η παραδοχή σας, αφού αναφέρατε ότι αναγνωρίζετε την ανάγκη της Τράπεζας για άμεση ανάληψη δράσης για διερεύνηση περιστατικών που αφορούν δεδομένα φυσικών προσώπων και για υποβολή σχετικής γνωστοποίησης στο Γραφείο μου εντός της προθεσμίας που καθορίζεται στο **Άρθρο 33 του ΓΚΠΔ 2016/679**, από το χρονικό σημείο που εξακριβώνεται με εύλογο βαθμό βεβαιότητας ότι έχει σημειωθεί παραβίαση προσωπικών δεδομένων.

Περαιτέρω, έστω και αν όπως λέχθηκε στις 17/1/20 τα οικονομικά δεδομένα που εκτέθηκαν προς τον Σ.Γ. αφορούσαν εταιρικούς λογαριασμούς συνδεδεμένους με τον Μ.Κ., είναι παραδεκτό εκ μέρους σας, ότι τουλάχιστον μέχρι και τις 20/9/19 που προβήκατε στην Γνωστοποίηση, αλλά ακόμη και μέχρι την 17/1/20 όπου διαφοροποιήσατε τα γεγονότα, είχατε την εντύπωση ότι τα δεδομένα στα οποία πλείστα είχε πρόσβαση ο Σ.Γ. αφορούσαν στο φυσικό πρόσωπο του Μ.Κ. Να λεχθεί επίσης, ότι δεν αποκλείστηκε το ενδεχόμενο ο Μ.Κ. να είχε πρόσβαση στα δεδομένα του Σ.Γ. Τουναντίον, στην Γνωστοποίηση Παραβίασης ημερ. 20/9/19 αναφέρεται ότι έχουν επηρεαστεί δύο φυσικά πρόσωπα, (δηλαδή τόσο ο Σ.Γ. όσο και Μ.Κ.), αλλά και στην επιστολή της Τράπεζας ημερ. 4/11/19 αναφέρεται ότι «*Τα εμπλεκόμενα πρόσωπα ως σας έχουμε ενημερώσει μέσω της γνωστοποίησης μπορούσαν να έχουν πρόσβαση στα στοιχεία,* [συνεπώς μπορούσαν να έχουν πρόσβαση ο ένας στα στοιχεία του άλλου], *αλλά δεν μπορούσαν για παράδειγμα να προβούν σε μεταφορές χρημάτων».*

(β) Σε ότι αφορά στα τεχνικά και οργανωτικά μέτρα τα οποία λαμβάνονται από την Τράπεζα έτσι ώστε να συμμορφώνεται με τις πρόνοιες **του Άρθρου 32 του ΓΚΠΔ 2016/679**, θα πρέπει να σημειώσω τα πιο κάτω:

Στις 16/4/19, λόγω λάθους υπαλλήλου της Τράπεζας, καταχωρίστηκε για πρώτη φορά ο αριθμός του νέου διαβατηρίου του Σ.Γ.. στα στοιχεία του πελάτη Μ.Κ.. Λόγω του ότι ήταν η πρώτη φορά που καταχωρείτο ο αριθμός αυτός στα δεδομένα της Τράπεζας, το σύστημα δεν εμφάνισε οποιαδήποτε προειδοποίηση. Την 2/5/19, κατά την επικαιροποίηση των στοιχείων του Σ.Γ., καταχωρίστηκε για δεύτερη φορά ο νέος αριθμός διαβατηρίου του Σ.Γ. στα δεδομένα της Τράπεζας. Αυτή την φορά το σύστημα εμφάνισε προειδοποιητικό μήνυμα. Η υπάλληλος της Τράπεζας βασίστηκε στην ορθότητα των εγγράφων που είχε στην κατοχή της και προχώρησε στην επιβεβαίωση της καταχώρησης. Στην επιβεβαίωση προχώρησε και δεύτερο άτομο της Τράπεζας, σύμφωνα με το four eye principle, το οποίο όμως αυτό άτομο, σύμφωνα με τα νέα δεδομένα τα οποία μας παρουσιάσατε κατά την 17/1/20, δεν λαμβάνει στο σύστημά του αντίστοιχο προειδοποιητικό μήνυμα ως αυτό που λαμβάνει ο πρώτος υπάλληλος.

Αν έτσι έχουν τα πράγματα, τότε σε τι αποσκοπεί η έγκριση ή όχι από δεύτερο υπάλληλο των ενεργειών του πρώτου, αφ' ης στιγμής δεν μπορεί να έχει γνώση του προειδοποιητικού μηνύματος που εμφανίζεται στην οθόνη του πρώτου υπαλλήλου; Πώς γίνεται τότε διπλός έλεγχος των δεδομένων; Η έκφραση από μόνη της four eye principle παραπέμπει σε οπτικό έλεγχο των πράξεων, από δύο πρόσωπα. Εάν το δεύτερο πρόσωπο απλά επιβεβαιώνει τις ενέργειες του πρώτου, χωρίς να γνωρίζει τι προηγήθηκε, τότε είναι άνευ ουσίας η εν λόγω επιβεβαίωση. Περαιτέρω να υπενθυμίσω ότι παραδεχθήκατε ότι καμία από τις δύο δικλείδες ασφαλείας του συστήματος δεν εμπόδισε το λάθος που έγινε, εφόσον ο υπάλληλος της Τράπεζας, λέτε, θα έπρεπε σύμφωνα με τις οδηγίες του Τμήματος Οργάνωσης και Διαδικασιών της Τράπεζας, να είχε διερευνήσει το λόγο παρουσίας του προειδοποιητικού μηνύματος, ούτως ώστε να εντοπίσει το λάθος που είχε γίνει από τη συνάδελφο της στις 16/4/19 και να αποφευχθούν τα όσα ακολούθησαν.

Αιτιολογήσατε την παραβίαση ότι ήταν αποτέλεσμα ανθρώπινου λάθους και απροσεξίας, κάτω από ασυνήθιστες συγκεκριμένες περιστάσεις, κατά την εφαρμογή των διαδικασιών της Τράπεζας κατά την καταχώρηση των στοιχείων στο σύστημα. Αυτό όμως δεν απέτρεψε επανάληψη παρόμοιου περιστατικού, το οποίο γνωστοποιήθηκε στην Εποπτική Αρχή την 15/11/19, με Αριθμό Γνωστοποίησης 57/19, σύμφωνα με το οποίο και πάλι πελάτης που είχε πρόσβαση στο Web Banking εμπορικής επωνυμίας, είχε δει στοιχεία κάρτας άλλης πελάτιδας, λόγω του ότι καταχωρίστηκε εκ λάθους ο αριθμός της εμπορικής επωνυμίας ως αριθμός ταυτότητας φυσικού προσώπου που αντιστοιχούσε στην άλλη πελάτιδα. Σύμφωνα περαιτέρω με τα **Άρθρα 29 και 32 παρ. 4 του ΓΚΠΔ 2016/679**, ο υπεύθυνος επεξεργασίας φέρει την ευθύνη πράξεων προσώπων που ενεργούν υπό την εποπτεία του και οφείλει να λαμβάνει μέτρα έτσι ώστε να διασφαλίζει ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του, επεξεργάζεται τα οποιαδήποτε προσωπικά δεδομένα μόνο κατ' εντολή του. Συνεπώς, δεν μπορεί να επικαλείστε το ανθρώπινο λάθος για απεμπόληση των ευθυνών σας, έχοντας υπόψιν επίσης ότι εσωγενείς κίνδυνοι μπορούν να αποβούν χειρότεροι από τους εξωγενείς.

Να σημειωθεί επίσης ότι παρόλο που ειδοποιηθήκατε από τον Σ.Γ. στις 28/5/19 για το γεγονός ότι στο σύστημα Web Banking, εμφανίζονταν όλα τα στοιχεία λογαριασμού του Μ.Κ. (έστω και αν εν τέλει φάνηκε ότι επρόκειτο για εταιρικό λογαριασμό), και λάβατε μέτρα για άρση αυτού του συμβάντος, εντούτοις δεν απετράπη νέο περιστατικό που συνέβη την 9/8/19, όταν δηλαδή εκδόθηκε η χρεωστική κάρτα του Μ.Κ. και αποστάληκε στην διεύθυνση του Σ.Γ., λόγω του ότι η κοινή διεύθυνση είχε παραμείνει αδιόρθωτη. Συνεπώς, ακόμη και τα άμεσα μέτρα τα οποία λήφθηκαν, δεν ήταν ικανοποιητικά για να αποτρέψουν το δεύτερο περιστατικό παραβίασης της ασφάλειας των δεδομένων.

(γ) Το υποκείμενο των δεδομένων δεν έχει ειδοποιηθεί για το εν λόγω συμβάν. Ο υπεύθυνος προστασίας δεδομένων, αιτιολόγησε την απόφαση αυτή στο γεγονός ότι (1) τα εμπλεκόμενα πρόσωπα δεν μπορούσαν να προβούν σε μη εξουσιοδοτημένες πράξεις που θα είχαν ως αποτέλεσμα πιθανή οικονομική ζημιά, (2) δεν υπήρχε το στοιχείο της ταυτότητας του υποκειμένου των δεδομένων και (3) λήφθηκαν άμεσα μέτρα αντιμετώπισης του συμβάντος, με την διόρθωση των στοιχείων. Έκρινε επίσης ότι η οποιαδήποτε επίπτωση στα δικαιώματα και ελευθερίες του υποκειμένου των δεδομένων, είναι μικρή. Δεν υπάρχει αμφιβολία όμως ότι ο Σ.Γ. είχε λάβει γνώση σωρείας οικονομικών δεδομένων εταιρείας που ανήκει στον Μ.Κ. καθώς και του ονόματος του Μ.Κ. ή/και ο Μ.Κ. είχε λάβει γνώση των οικονομικών δεδομένων του Σ.Γ.. Παρόλ' αυτά, λόγω του ότι δεν θα μπορούσαν τα μέρη να προβούν σε μη εξουσιοδοτημένες πράξεις που θα επέφεραν οικονομική ζημιά ο ένας στον άλλο, θα δεχτούμε με επιφύλαξη την απόφαση σας να μην ενημερώσετε τον Μ.Κ.

11. Κατάληξη

Λαμβάνοντας υπόψιν όλα τα ανωτέρω στοιχεία ως έχουν παρατεθεί, και με βάση τις εξουσίες που μου παρέχονται από τα **Άρθρα 58 και 83 του Κανονισμού (ΕΕ) 2016/679**, **άρθρο 24(β) του Νόμου 125(Ι)/2018,** καθώς και τις πρόνοιες του **άρθρου 43 περί των Γενικών Αρχών του Διοικητικού Δικαίου Νόμο του 1999,** καταλήγω ότι υπήρξε παράβαση εκ μέρους της Ελληνικής Τράπεζας μίας εκ των βασικών Αρχών που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα και δη του **Άρθρου 5, παρ.1 στ) του ΓΚΠΔ 2016/679**, αφού δεν κατάφερε να εγγυηθεί

την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα υποκειμένων των δεδομένων με την χρήση κατάλληλων τεχνικών και οργανωτικών μέτρων έτσι ώστε να διασφαλίζεται η ακεραιότητα και εμπιστευτικότητα αυτών, του **Άρθρου 32 παρ. 1(β) του ΓΚΠΔ 2016/679** εφόσον δεν εφάρμοσε τα κατάλληλα τεχνικά και οργανωτικά μέτρα τα οποία όφειλε να εφαρμόσει προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, διαθεσιμότητας και αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση, καθώς και παράβαση του **Άρθρου 33 παρ. 1**, εφόσον δεν ειδοποίησε την Εποπτική Αρχή εντός 72 ωρών από την στιγμή που απέκτησε γνώση του γεγονότος της παραβίασης, ως όφειλε.

Σύμφωνα με την **αιτιολογική σκέψη 148 του ΓΚΠΔ 2016/679**, προκειμένου να ενισχυθεί η επιβολή των κανόνων του Κανονισμού, κυρώσεις, συμπεριλαμβανομένων των διοικητικών προστίμων θα πρέπει να επιβάλλονται για κάθε παράβαση, επιπρόσθετα ή αντί των κατάλληλων μέτρων που επιβάλλονται από την Εποπτική Αρχή. Σε περίπτωση παράβασης ελάσσονος σημασίας ή αν το πρόστιμο που ενδέχεται να επιβληθεί θα αποτελούσε δυσανάλογη επιβάρυνση σε φυσικό πρόσωπο, θα μπορούσε να επιβληθεί επίπληξη αντί προστίμου. Θα πρέπει ωστόσο να λαμβάνονται δεόντως υπόψιν η φύση, η σοβαρότητα και η διάρκεια της παράβασης, ο εσκεμμένος χαρακτήρας της παράβασης, οι δράσεις που αναλήφθηκαν για τον μετριασμό της ζημιάς, ο βαθμός της ευθύνης ή τυχόν άλλες σχετικές προηγούμενες παραβάσεις, ο τρόπος με τον οποίο η εποπτική αρχή πληροφορήθηκε την παράβαση, η συμμόρφωση με τα μέτρα κατά του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, η τήρηση κώδικα δεοντολογίας και κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο.

Διαπιστώνοντας λοιπόν παράβαση των **Άρθρων 5 παρ. 1(στ), 32 παρ. 1(β) και 33 παρ. 1 του ΓΚΠΔ 2016/679** ως επεξηγείται ανωτέρω, βάσει των προνοιών του **Άρθρου 83 του ΓΚΠΔ**, στο μέτρο που εφαρμόζονται στη συγκεκριμένη περίπτωση, λαμβάνω υπόψιν τους πιο κάτω μετριαστικούς (1-10) και επιβαρυντικούς (11-16) παράγοντες:

(1) Τον περιορισμένο αριθμό υποκειμένων των δεδομένων των οποίων τα δεδομένα έχουν εκτεθεί (δύο στο σύνολο).
(2) Την ανυπαρξία δόλου εκ μέρους του υπεύθυνου επεξεργασίας, αφού η παραβίαση ήταν αποτέλεσμα ανθρώπινου λάθους.
(3) Το γεγονός ότι ο υπεύθυνος επεξεργασίας προέβαινε σε ενέργειες διόρθωσης των λαθών του, ευθύς μετά την ειδοποίηση γι' αυτά από το υποκείμενο των δεδομένων.
(4) Το ότι υπάρχει συνεργασία μεταξύ του υπεύθυνου επεξεργασίας και της Εποπτικής Αρχής.
(5) Το γεγονός ότι ο υπεύθυνος επεξεργασίας εφαρμόζει πολιτικές και κώδικες στον χώρο εργασίας όπως π.χ. Πολιτική Προστασίας Δεδομένων, Πλαίσιο Προστασίας Δεδομένων, Πολιτική Ασφάλειας Πληροφοριών, Πειθαρχικός Κώδικας, και Κώδικας Επαγγελματικής Συμπεριφοράς και Ηθικής, τους οποίους οι υπάλληλοι οφείλουν να γνωρίζουν και εφαρμόζουν.
(6) Το ότι υπήρξε παραδοχή λαθών τόσο για το θέμα των δικλείδων ασφαλείας του συστήματος, όσο και για την ανάγκη της Τράπεζας για άμεση ανάληψη δράσης για διερεύνηση περιστατικών και υποβολή σχετικής γνωστοποίησης στο Γραφείο μου εντός της προθεσμίας.
(7) Το γεγονός ότι πλείστα των δεδομένων του Μ.Κ. που εκτέθηκαν προς τον Σ.Γ., όπως φάνηκε εν τέλει, ανήκουν σε νομική οντότητα η οποία ήταν συνδεδεμένη με φυσικό πρόσωπο.
(8) Το ότι δεν πραγματοποιήθηκαν μη εξουσιοδοτημένες συναλλαγές, αφού απαιτείτο επιπρόσθετος κωδικός ασφάλειας – one time password και δεν υπήρξαν οικονομικές συνέπειες στα υποκείμενα των δεδομένων.
(9) Τον μεγάλο αριθμό καταχωρίσεων. Μόνο για το έτος 2019 έγιναν πέραν των 15000 καταχωρίσεων στο σύστημα της Τράπεζας.
(10) Το ότι ένα τραπεζικό ίδρυμα έχει αυξημένο βαθμό ευθύνης, έναντι οποιουδήποτε άλλου υπεύθυνου επεξεργασίας, για τήρηση τέτοιων μέτρων ασφαλείας ώστε να διαφυλάσσονται τα οικονομικά δεδομένα των πελατών του.

(11) Το ότι εντός του έτους 2019, γνωστοποιήθηκαν στην Εποπτική Αρχή, ακόμη 7 παραβιάσεις εμπιστευτικότητας δεδομένων των πελατών της Ελληνικής Τράπεζας, χωρίς όμως πάντα να αφορά στα ίδια περιστατικά όπως στην παρούσα περίπτωση.
(12) Το ότι αποκαλύφθηκαν οικονομικά δεδομένα και παραβιάστηκε η εμπιστευτικότητα τους.
(13) Την μη τήρηση της πρέπουσας διαδικασίας και την μεγάλη καθυστέρηση στην υποβολή Γνωστοποίησης Παραβίασης με βάση το Άρθρο 33 παρ. 1 του ΓΚΠΔ 2016/679.
(14) Το γεγονός ότι παρόλο που υπήρχαν δικλείδες ασφαλείας, αυτές δεν ήταν ικανές να αποτρέψουν την παραβίαση.
(15) Το γεγονός ότι παρατηρούνται συχνά περιστατικά παραβίασης που οφείλονται σε ανθρώπινο λάθος υπαλλήλων της Τράπεζας.
(16) Τέλος, το γεγονός ότι η Τράπεζα έλαβε γνώση για τις παραβιάσεις και αντιλήφθηκε τα λάθη τα οποία έγιναν, αφότου ειδοποιήθηκε και τις δύο φορές από ένα εκ των δύο επηρεαζόμενων προσώπων.

Έχοντας υπόψιν τα ανωτέρω, καθώς και το γεγονός ότι οι μετριαστικοί παράγοντες είναι κατά πολύ περισσότεροι από τους επιβαρυντικούς, αποφασίζω όπως μη επιβάλω διοικητικό πρόστιμο αυτή την φορά.

Παρόλα αυτά, δίδεται εντολή προς την Ελληνική Τράπεζα, όπως θεσπίσει τέτοια μέτρα ασφαλείας και πρακτικές, ουτώς ώστε να καθίστανται οι πράξεις επεξεργασίας σύμφωνες με τις διατάξεις του ΓΚΠΔ 2016/679, ως αυτές έχουν επεξηγηθεί με την παρούσα Απόφαση.

Εντέλλεται επίσης η Ελληνική Τράπεζα, όπως σε διάστημα τριών 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