

ΑΠΟΦΑΣΗ 38/2022

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνεδρίασε σε σύνθεση Ολομέλειας, μέσω τηλεδιασκέψεως, την Τρίτη 21-07-2022, μετά από πρόσκληση του Προέδρου της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν ο Πρόεδρος της Αρχής, Κωνσταντίνος Μενουδάκος και τα τακτικά μέλη της Αρχής, Κωνσταντίνος Λαμπρινουδάκης, ως εισηγητής, Σπυρίδων Βλαχόπουλος, Χαράλαμπος Ανθόπουλος Χρήστος Καλλονιάτης, Αικατερίνη Ηλιάδου και το αναπληρωματικό μέλος Μαρία Ψάλλα, σε αντικατάσταση του τακτικού μέλους Γρηγορίου Τσόλια, ο οποίος παρόλο που εκλήθη νομίμως εγγράφως, δεν παρέστη λόγω κωλύματος. Στη συνεδρίαση παρέστησαν οι Σπυρίδων Παπαστεργίου και Λεωνίδα Ρούσσοι, Ειδικοί Επιστήμονες, Πληροφορικοί, ως βοηθοί εισηγητή και με εντολή Προέδρου η Ειρήνη Παπαγεωργοπούλου ως Γραμματέας, υπάλληλος του τμήματος διοικητικών υποθέσεων της Αρχής.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Υποβλήθηκε στην Αρχή ένα σύνολο καταγγελιών και γνωστοποιήσεων περιστατικών παραβίασης προσωπικών δεδομένων που σχετίζονται με περιστατικά μη εξουσιοδοτημένης αντικατάστασης κάρτας sim συνδρομητή (sim swar) αλλά και άλλων διαδικασιών (π.χ. εκτροπής κλήσεων, έκδοσης νέων αριθμών τηλεφώνων) από τρίτους, μη κατόχους των εν λόγω συνδέσεων.

Αρχικά, υποβλήθηκαν οι: α) Η υπ' αριθμ. πρωτ. Γ/ΕΙΣ/4807/10-7-2020 καταγγελία, β) οι υπ' αριθμ. Γ/ΕΙΣ/7103/16-10-2020, Γ/ΕΙΣ/7255/22-10-2020, Γ/ΕΙΣ/7299/23-10-

2020,Γ/ΕΙΣ/7300/23-10-2020 και Γ/ΕΙΣ/7301/23-10-2020 γνωστοποιήσεις περιστατικών παραβίασης.

Η Αρχή, στο πλαίσιο της εξέτασης των υποθέσεων αυτών, απέστειλε στην εταιρεία παροχής υπηρεσιών κινητής τηλεφωνίας Vodafone – ΠΑΝΑΦΟΝ Α.Ε.Ε.Τ. (εφεξής «υπεύθυνος επεξεργασίας» ή «Vodafone») το υπ' αριθμ. πρωτ. Γ/ΕΞ/7771/11-11-2020 έγγραφο, με το οποίο ζητήθηκαν οι απόψεις της αναφορικά με τις σχετικές καταγγελίες, τα γνωστοποιηθέντα περιστατικά παραβίασης αλλά και τον γενικότερο τρόπο αντιμετώπισης των εν λόγω θεμάτων. Συγκεκριμένα, ζητήθηκε:

α) Περιγραφή των πολιτικών που εφαρμόζονταν ως προς τη διαδικασία ακύρωσης και αντικατάστασης κάρτας SIM από συνδρομητή, πριν την διαπίστωση των σχετικών περιστατικών παραβίασης.

β) Περιγραφή των αλλαγών/τροποποιήσεων που πραγματοποιήθηκαν στις εν λόγω πολιτικές και διαδικασίες μετά τη διαπίστωση των ανωτέρω περιστατικών παραβίασης.

γ) Περιγραφή των πολιτικών και των σχετικών οδηγιών που εφαρμόζονται σήμερα από τα σημεία εξυπηρέτησης των συνδρομητών για τη διαδικασία ακύρωσης και αντικατάστασης κάρτας SIM.

δ) Γνωστοποίηση αν έχουν διαπιστώσει και άλλα παρόμοια περιστατικά μετά την εφαρμογή των νέων πολιτικών και πέρα από αυτά που έχουν υποβληθεί στην Αρχή.

Η εταιρία απάντησε στα ανωτέρω ζητήματα με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/8392/07-12-2020 έγγραφο σύμφωνα με το οποίο τα μέτρα που εφαρμόστηκαν από την εταιρεία για την αποτελεσματική ταυτοποίηση συνδρομητών σε περιπτώσεις έκδοσης νέας κάρτας SIM ή αντικατάστασης κάρτας SIM διακρίνονται σε 4 χρονικές περιόδους.

1^η περίοδος: Πολιτικές που εφαρμόζονταν από την εταιρεία μέχρι τον Απρίλιο 2020.

Στο διάστημα αυτό οι διαδικασίες που ακολουθούνται από την εταιρεία είναι οι ακόλουθες:

(α) Στην περίπτωση που το σχετικό αίτημα υποβάλλεται αυτοπροσώπως από τον συνδρομητή, εντός καταστήματος της εταιρείας, διενεργείται από τους αρμοδίους

υπαλλήλους επιστάμενος έλεγχος για την επιβεβαίωση της ταυτότητας του αιτούντος. Ειδικότερα:

- a. Κατά τη διαδικασία της ταυτοποίησης του αιτούντος γίνονται αποδεκτά μόνο πρωτότυπα δικαιολογητικά (δελτίο ταυτότητας/διαβατήριο) και όχι αντίγραφα αυτών (ούτε επικυρωμένα αντίγραφα).
- b. Ελέγχεται ότι ο εμφανισθείς αιτών είναι ο ίδιος με αυτόν που απεικονίζεται στην φωτογραφία του δικαιολογητικού ταυτοποίησης.
- c. Ελέγχεται σε κάθε περίπτωση ότι η εκτιμώμενη από τους υπαλλήλους ηλικία του εμφανισθέντος/αιτούντος ταιριάζει με την ηλικία γέννησης που αναγράφεται στο δικαιολογητικό ταυτοποίησης.
- d. Ελέγχεται και επαληθεύεται ότι ο αριθμός του δικαιολογητικού ταυτοποίησης και η αναγραφόμενη σε αυτό ημερομηνία γέννησης ταυτίζονται με τα αντίστοιχα στοιχεία, που υπάρχουν στα συστήματα της εταιρείας.
- e. Ελέγχεται επισταμένως το δικαιολογητικό ταυτοποίησης για τυχόν ενδείξεις πλαστότητας.

(β) Στην περίπτωση που το σχετικό αίτημα υποβάλλεται εντός καταστήματος της εταιρείας από τρίτο πρόσωπο με χρήση εξουσιοδότησής από τον συνδρομητή, ομοίως διενεργούνται από τους αρμοδίους υπαλλήλους επιστάμενοι έλεγχοι.

Ειδικότερα:

- a. Ελέγχεται ότι η προσκομισθείσα εξουσιοδότηση είναι ειδική (και όχι γενική) και ότι αναφέρει ρητά ότι παρέχει στον εξουσιοδοτούμενο το δικαίωμα να ζητήσει την αντικατάσταση της κάρτας SIM συγκεκριμένου MSISDN.
- b. Ελέγχεται ότι τα αναγραφόμενα στην εξουσιοδότηση στοιχεία εξουσιοδοτούντος/εξουσιοδοτούμενου ταυτίζονται:
 - ο Τα στοιχεία του εξουσιοδοτούντος (ονοματεπώνυμο, αριθμός δικαιολογητικού ταυτοποίησης, ημερομηνία γέννησης κλπ) με αυτά που υπάρχουν στα συστήματα της εταιρείας
 - ο Τα στοιχεία του εξουσιοδοτούμενου με αυτά που αναγράφονται στο προσκομιζόμενο δικαιολογητικό ταυτοποίησής του (δελτίο ταυτότητας/διαβατήριο).
- c. Ελέγχεται ότι η προσκομισθείσα εξουσιοδότηση εξακολουθεί να ισχύει (η εξουσιοδότηση μπορεί να χρησιμοποιηθεί μια μόνο φορά και ισχύει για 6

μήνες από την ημερομηνία υπογραφής της) και ότι αμφότερα τα προσκομιζόμενα έγγραφα (εξουσιοδότηση και δικαιολογητικό ταυτοποίησης του εξουσιοδοτούμενου) δεν εμφανίζουν ενδείξεις πλαστότητας.

Η εξουσιοδότηση απαιτείται να φέρει πρωτότυπη θεώρηση γνησίου υπογραφής του εξουσιοδοτούντος από οιαδήποτε δημόσια ή δημοτική αρχή, από τράπεζα, από συμβολαιογράφους και από δικηγόρους. Σε περίπτωση ηλεκτρονικής εξουσιοδότησης (εκδοθείσας μέσω του gov.gr με χρήση των κωδικών Taxisnet) επιβεβαιώνεται η γνησιότητα της ηλεκτρονικής εξουσιοδότησης μέσω εισόδου στο <https://dilosi.services.gov.gr/> * είτε με χρήση του κωδικού επαλήθευσης του εγγράφου, είτε χρησιμοποιώντας το QR code.

(γ) Στην περίπτωση που το σχετικό αίτημα υποβάλλεται στο τηλεφωνικό κέντρο της εταιρείας, ομοίως διενεργούνται από τους αρμοδίους υπαλλήλους επιστάμενοι έλεγχοι. Ειδικότερα:

- a. Αρχικά ο αιτών ταυτοποιείται τηλεφωνικά κι ενημερώνεται ότι θα χρειαστεί να απευθυνθεί σε κατάσταση της εταιρείας, προκειμένου να διεκπεραιωθεί το αίτημά του.
- b. Στην περίπτωση που ο αιτών ενημερώσει ότι δεν επιθυμεί ή δεν δύναται να μεταβεί σε κάποιο κατάσταση της εταιρείας είτε λόγω των ειδικών συνθηκών της πανδημίας κορονοϊού (COVID19) είτε επειδή στην περιοχή του δεν λειτουργεί κατάσταση της εταιρείας, εξετάζονται οι προβαλλόμενοι λόγοι αντικατάστασης της SIM και ενημερώνεται ο αιτών ότι υπάρχει δυνατότητα αποστολής με συστημένη επιστολή μη ενεργοποιημένης κάρτας SIM μέσω εταιρείας ταχυμεταφοράς (courier). Επίσης ο αιτών ενημερώνεται ότι στην περίπτωση αυτή μόνο ο ίδιος (με επίδειξη αποδεικτικού ταυτοπροσωπίας) θα μπορεί να παραλάβει την αποσταλείσα μη ενεργοποιημένη κάρτα SIM από τον αρμόδιο υπάλληλο της εταιρείας ταχυμεταφοράς.

2^η περίοδος: Πολιτικές που εφαρμόζονταν από την εταιρεία από τον Απρίλιο 2020 μέχρι τον Οκτώβριο 2020

Μετά τη διαπίστωση των ανωτέρω περιστατικών παραβίασης, ήτοι τον Απρίλιο του 2020, η εταιρεία προχώρησε σε τροποποιήσεις των υφιστάμενων διαδικασιών

αντικατάστασης κάρτας SIM από συνδρομητή. Ειδικότερα από τις 27/04/2020 τροποποιήθηκαν οι ανωτέρω διαδικασίες και συγκεκριμένα:

- a. Θεσπίστηκε το βήμα της τηλεφωνικής επικοινωνίας με τον αιτούντα συνδρομητή / κάτοχο της SIM, προκειμένου να επιβεβαιωθεί το υποβληθέν αίτημα στις περιπτώσεις αιτήματος μέσω εξουσιοδότησης στα καταστήματα και αιτήματος μέσω τηλεφωνικού κέντρου.
- b. Θεσπίστηκε η υποχρέωση του αιτούντος συνδρομητή να συμπληρώσει (μέσω του gov.gr) σχετική υπεύθυνη δήλωση και να αποστείλει είτε την υπεύθυνη δήλωση είτε τον εκδοθέντα κωδικό, προκειμένου να διενεργηθεί έλεγχος αυτής στην περίπτωση αιτήματος μέσω τηλεφωνικού κέντρου.
- c. Στις μη αυτοπρόσωπες παρουσίες, θεσπίστηκε η υποχρέωση αποστολής της κάρτας SIM μέσω συστημένης αλληλογραφίας και δεν πραγματοποιείται ενεργοποίηση άλλης κάρτας SIM που τυχόν έχει στην κατοχή του ο συνδρομητής. Επίσης, η διαδικασία ενεργοποίησης γίνεται τηλεφωνικά, στη σύνδεση για την οποία ζητείται η αντικατάσταση της κάρτας SIM.

Παράλληλα με τις προαναφερθέντες τροποποιήσεις λήφθηκαν και τα κάτωθι επιπρόσθετα μέτρα:

- a. Πραγματοποιήθηκε ενημέρωση και εκπαίδευση των υπευθύνων και των υπαλλήλων του τηλεφωνικού κέντρου της εταιρείας με σαφή επισήμανση της προσοχής που πρέπει να επιδεικνύουν στους κινδύνους τους οποίους εγκυμονεί η διαδικασία αντικατάστασης SIM και στην συνακόλουθη ανάγκη πλήρους συμμόρφωσης και εφαρμογής των ανωτέρω διαδικασιών.
- b. Αναρτήθηκε σχετικό ενημερωτικό υλικό στην εσωτερική ιστοσελίδα (intranet) των καταστημάτων της εταιρείας, με σαφή επισήμανση της προσοχής που πρέπει να επιδεικνύουν στους κινδύνους τους οποίους εγκυμονεί η διαδικασία αντικατάστασης SIM και στην συνακόλουθη ανάγκη πλήρους συμμόρφωσης και εφαρμογής των ανωτέρω διαδικασιών.

3^η περίοδος: Πολιτικές που εφαρμόζονταν από την εταιρεία από το Νοέμβριο 2020 μέχρι τον Ιούλιο 2021

Παρά τις νέες ως άνω πολιτικές, που τέθηκαν σε ισχύ τον Απρίλιο του 2020, παρατηρήθηκαν και νέα περιστατικά, εξαιτίας των οποίων οι εφαρμοζόμενες

πολιτικές βελτιώθηκαν εκ νέου για την καταπολέμηση της συγκεκριμένης απάτης. Ειδικότερα, από τις 30-10-2020 διακόπηκε η παροχή δυνατότητας αντικατάστασης καρτών sim από το τηλεφωνικό κέντρο της εταιρείας (με τους αιτούντες να κατευθύνονται σε κάποιο από τα καταστήματα της εταιρείας). Σε περίπτωση δε που η επίσκεψη από τον συνδρομητή σε κάποιο κατάστημα της εταιρείας δεν ήταν εφικτή, η αντικατάσταση κάρτας sim πραγματοποιείται μόνο μέσω αποστολής της νέας κάρτας sim με συστημένη επιστολή προς τον αιτούντα συνδρομητή και με παράλληλη αποστολή ενημερωτικού SMS στον τηλεφωνικό αριθμό στον οποίο αφορά το αίτημα αντικατάστασης.

Περαιτέρω, στις 10-11-2020 βελτιστοποιήθηκε και η διαδικασία αντικατάστασης καρτών sim στα καταστήματα της εταιρείας μέσω της πρόβλεψης επιπλέον βήματος ασφαλείας. Συγκεκριμένα, η επιβεβαιωτική εξερχόμενη κλήση προς τον τηλεφωνικό αριθμό που αφορά το αίτημα αντικατάστασης κάρτας sim (που πραγματοποιείται μόνο σε περιπτώσεις αιτήματος με εξουσιοδότηση) επεκτάθηκε και στις περιπτώσεις αιτήματος υποβαλλόμενου αυτοπροσώπως από τον κάτοχο του επίμαχου τηλεφωνικού αριθμού.

4^η περίοδος: Επιπλέον μέτρα τα οποία εφαρμόστηκαν μετά τον Ιούλιο 2021

Η εταιρία θέσπισε επιπλέον μέτρα, τα οποία είναι τα ακόλουθα: (α) μη δυνατότητα αλλαγής κάρτας από τα ψηφιακά κανάλια σε περίπτωση απώλειας ή κλοπής και εξυπηρέτηση μόνο από καταστήματα και (β) μετά την αντικατάσταση κάρτας SIM πραγματοποιείται φραγή εισερχομένων sms για διάστημα 2 ωρών.

Με το με αριθμ. πρωτ. Γ/ΕΞΕ/701/15-03-2022 έγγραφο, η Αρχή κάλεσε την εταιρία, ενώπιον της στη συνεδρίαση της την Τετάρτη 22-03-2022, για να δώσει περαιτέρω διευκρινίσεις και να εκθέσει διεξοδικά τις απόψεις της επί των περιστατικών παραβίασης και των συναφών καταγγελιών. Επιπλέον, με την ανωτέρω κλήση, η εταιρία ενημερώθηκε ότι απαιτούνται διευκρινήσεις και αναφορικά με τις με αρ. πρωτ. Γ/ΕΙΣ/5508/19-07-17 και Γ/ΕΙΣ/2224/31-03-2021 καταγγελίες, που αφορούν στο ίδιο ζήτημα, και για τις η εταιρία ενημερώθηκε με τα με αρ. πρωτ. Γ/ΕΞΕ/1614/29-06-2021 και Γ/ΕΞ/9729/04-12-2018, αντίστοιχα, έγγραφα της Αρχής και στα οποία απάντησε με τα με αρ. πρωτ. Γ/ΕΙΣ/234/14-01-2019, Γ/ΕΙΣ/4721/15-07-2021 υπομνήματα, αντίστοιχα. Η εταιρία παρέστη και υπέβαλε αίτημα αναβολής, το οποίο έγινε δεκτό και η εξέταση της υπόθεσης αναβλήθηκε για τη συνεδρίαση της 3-

5-2022, κατά την οποία για την εταιρία παρέστησαν οι Χαλκιαδάκης Εμμανουήλ, Δικηγόρος, ΑΜ, Απόστολος Βόρρας, Δικηγόρος, ΑΜ ..., Εμμανουήλ Δημογεροντάκης, Δικηγόρος, ΑΜ και ο Α, Υπεύθυνος Προστασίας Δεδομένων της εταιρείας και οι οποίοι υποστήριξαν όσα με το ανωτέρω έγγραφό της είχε εκθέσει εγγράφως, αλλά και έλαβε προθεσμία για την υποβολή υπομνήματος, το οποίο και κατέθεσε με τον με αρ. πρωτ. Γ/ΕΙΣ/7738/06-06-2022 μήνυμα ηλεκτρονικού ταχυδρομείου. Σε συνέχεια του εν λόγω υπομνήματος η εταιρία υπέβαλε στις 6/7/2022 συμπληρωματικά στοιχεία.

Με τα ανωτέρω, η εταιρία αναφέρει ότι από τον Φεβρουάριο του έτους 2018, είχε πραγματοποιηθεί ένας προκαταρκτικός έλεγχος των διαδικασιών εξυπηρέτησης πελατών, συμπεριλαμβανομένης και της διαδικασίας ταυτοποίησης των συνδρομητών. Η αξιολόγηση αυτή έγινε στο πλαίσιο μιας αρχικής εκτίμησης του κινδύνου στο πλαίσιο της οποίας καταγράφηκαν οι σχετικές δραστηριότητες επεξεργασίας, τα εμπλεκόμενα πληροφοριακά συστήματα, ο τύπος των προσωπικών δεδομένων, η νομική βάση της επεξεργασίας, καθώς και τα τεχνικά και οργανωτικά μέτρα που έχουν ληφθεί για τη διασφάλιση ενός επαρκούς επιπέδου προστασίας των προσωπικών δεδομένων. Από την εκπονηθείσα μελέτη διαπιστώθηκε ότι τα τεχνικά και οργανωτικά μέτρα που εφαρμόζονταν για τη διασφάλιση της ασφάλειας της διαδικασίας ταυτοποίησης συνδρομητών (customer identity verification procedure), είναι εξαιρετικά αποτελεσματικά, καθώς μέχρι και τον Φεβρουάριο του έτους 2020 δεν είχε εντοπισθεί κανένα περιστατικό SIM swap. Στο υπόμνημα σημειώνεται, ότι τα πρώτα περιστατικά SIM swap στην Εταιρεία εντοπίστηκαν το μήνα Φεβρουάριο, ήτοι συνέπεσαν με την αφετηρία της πανδημίας covid-19 και των επιβληθέντων περιοριστικών μέτρων, τα οποία είχαν ως αποτέλεσμα, μεταξύ άλλων, τη ραγδαία αύξηση των τραπεζικών συναλλαγών και των φαινομένων ηλεκτρονικής απάτης.

Στο πλαίσιο της αντιμετώπισης του φαινομένου SIM swap fraud, τον Μάρτιο του έτους 2020, η εταιρία προέβη στην εκπόνηση μιας αναλυτικής μελέτης εκτίμησης αντικτύπου καθώς και στη λήψη επιπρόσθετων μέτρων αντιμετώπισης του φαινομένου. Σημειώνεται ότι για την εκπόνηση της συγκεκριμένης μελέτης λήφθηκαν υπόψη τα ακόλουθα:

- Η νέα μεθοδολογία ηλεκτρονικών απατών, η οποία επηρέαζε εμμέσως και την αύξηση του κινδύνου για τα δικαιώματα των υποκειμένων στο πλαίσιο της

διαδικασίας αντικατάστασης κάρτας SIM (μέσω: α. της αύξησης της πιθανότητας επέλευσης του κινδύνου, β. της έμμεσης αύξησης της σοβαρότητας των επιπτώσεων για τα υποκείμενα των δεδομένων)

- Τα αποτελέσματα των συναντήσεων εργασίας με την ομάδα Data Privacy του Vodafone Group, στο πλαίσιο των οποίων συζητήθηκαν περιστατικά SIM swap fraud που είχαν διαπιστωθεί σε άλλες χώρες του εξωτερικού. Επίσης, στο πλαίσιο των συγκεκριμένων συναντήσεων αναλύθηκε η μεθοδολογία των εγκληματικών ενεργειών και πραγματοποιήθηκε μια πρώιμη αξιολόγηση των εν δυνάμει πρόσθετων μέτρων ασφαλείας, που θα μπορούσαν να υιοθετηθούν.
- Τα αποτελέσματα από την ανάλυση διεθνών βιβλιογραφικών αναφορών σχετικά με περιστατικά SIM swap fraud, τα οποία λαμβάνουν χώρα σε παγκόσμια κλίμακα.
- Τα περιστατικά παραβίασης προσωπικών δεδομένων συνδρομητών της εταιρίας από κακόβουλους που εκμεταλλεύθηκαν τη δυνατότητα αντικατάστασης κάρτας SIM προσποιούμενοι είτε τον κάτοχο της κάρτας SIM ή κάποιον εξουσιοδοτημένο από το νόμιμο συνδρομητή.
- Την αύξηση των τραπεζικών συναλλαγών και των φαινομένων ηλεκτρονικής απάτης σε συνδυασμό με την εξάπλωση της πανδημίας covid-19 και τα σχετικά περιοριστικά μέτρα.

Αποτέλεσμα της συγκεκριμένης μελέτης ήταν η λήψη των ακόλουθων μέτρων:

- Προσθήκη περαιτέρω δικλίδων ασφαλείας στη διαδικασία αντικατάστασης κάρτας SIM με εξουσιοδότηση.
 - i. η επιβεβαίωση της γνησιότητας της ηλεκτρονικής εξουσιοδότησης (εκδοθείσας μέσω του gov.gr με χρήση των κωδικών Taxisnet) μέσω εισόδου στο <https://dilosi.services.gov.gr/> είτε με χρήση του κωδικού επαλήθευσης του εγγράφου, είτε χρησιμοποιώντας το QR code.
 - ii. η τηλεφωνική επικοινωνία με τον αιτούντα συνδρομητή/κάτοχο της SIM, για την οποία ζητείται αντικατάσταση, να πραγματοποιείται σε τηλέφωνο επικοινωνίας του συνδρομητή, που έχει δηλωθεί από τον τελευταίο και υπάρχει αποθηκευμένο στα συστήματα της εταιρίας, σε

περίπτωση που ο τηλεφωνικός αριθμός για τον οποίο ζητείται η αντικατάσταση SIM είναι απενεργοποιημένος.

- Προσθήκη περαιτέρω δικλίδων ασφαλείας στη διαδικασία αντικατάστασης κάρτας SIM μέσω τηλεφωνικού κέντρου. Μετά την ολοκλήρωση της τηλεφωνικής ταυτοποίησης, ζητείται από τον αιτούντα συνδρομητή να ολοκληρώσει τη διαδικασία εντός καταστήματος της Εταιρείας.
- Εναλλακτικά, δυνατότητα αποστολής μη ενεργοποιημένης κάρτας SIM μέσω Εταιρείας ταχυμεταφοράς (courier). Δυνατότητα παραλαβής έχει μόνο ο αιτών με επίδειξη αποδεικτικού ταυτοπροσωπίας, ενώ η ενεργοποίηση προτείνεται να πραγματοποιηθεί τηλεφωνικά, εφόσον ολοκληρωθούν τα κάτωθι βήματα:
 - i. αποστολή σχετικής υπεύθυνης δήλωσης (μέσω gov.gr) ή του εκδοθέντα κωδικού, προκειμένου να διενεργηθεί έλεγχος αυτής,
 - ii. κλήση από τον αιτούντα συνδρομητή/κάτοχο της SIM στο τηλεφωνικό κέντρο της Εταιρείας (χωρίς απόκρυψη τηλεφωνικού αριθμού) και πλήρης ταυτοποίηση,
 - iii. κλήση της εταιρίας προς τον αιτούντα συνδρομητή/κάτοχο της SIM, προκειμένου να επιβεβαιωθεί το υποβληθέν αίτημα. Η ως άνω τηλεφωνική επικοινωνία θα πραγματοποιείται στον τηλεφωνικό αριθμό για τον οποίο ζητείται η αντικατάσταση SIM και στην περίπτωση που αυτό είναι απενεργοποιημένο σε τηλέφωνο επικοινωνίας του συνδρομητή, που έχει δηλωθεί από τον τελευταίο και υπάρχει στα συστήματα της Εταιρείας. Ειδικά στους συνδρομητές καρτοκινητής, εφόσον το τηλέφωνο για το οποίο ζητείται η αντικατάσταση SIM είναι απενεργοποιημένο (και δεν υπάρχει κανένα άλλο τηλέφωνο επικοινωνίας στα συστήματα της εταιρίας) προτείνεται να παράσχει ο αιτών πληροφορίες σε σχέση με το πότε πραγματοποίησε την τελευταία ανανέωση χρόνου ομιλίας και με το ποσό που αυτή αφορούσε.

Τον Οκτώβριο 2020, η εταιρία προέβη εκ νέου σε επικαιροποίηση της από 2/3/2020 Μελέτης Εκτίμησης Αντικτύπου. Συγκεκριμένα, εισηγήθηκε τη λήψη πρόσθετων μέτρων ασφαλείας αναφορικά με τη διαδικασία αντικατάστασης κάρτας

SIM από τον αιτούντα συνδρομητή/κάτοχο SIM, τα οποία τελικά υιοθετήθηκαν και εφαρμόστηκαν. Ειδικότερα, εισηγήθηκε:

- Τη σαφή επισήμανση προς τους υπευθύνους και τους υπαλλήλους καταστημάτων της εταιρίας για την προσοχή που πρέπει να επιδεικνύουν κατά τη διαδικασία της ταυτοπροσωπίας δεδομένου μάλιστα ότι η χρήση μάσκας προστασίας δυσχεραίνει τον έλεγχο ταυτοπροσωπίας.
- Την προσθήκη επιπλέον δικλίδας ασφαλείας κατά τη διαδικασία αντικατάστασης κάρτας SIM από τον αιτούντα συνδρομητή/ κάτοχο της SIM, εντός καταστήματος της εταιρίας: επιβεβαιωτική εξερχόμενη κλήση προς τον τηλεφωνικό αριθμό που αφορά το αίτημα αντικατάστασης κάρτας SIM.
- Κατάργηση της δυνατότητας αντικατάστασης κάρτας SIM μέσω τηλεφωνικού κέντρου (τμήμα εξυπηρέτησης πελατών) της εταιρίας. Οι αιτούντες συνδρομητές θα πρέπει να επισκεφθούν κάποιο κατάστημα της εταιρίας και να υποβάλουν αυτοπροσώπως το αίτημά τους. Εναλλακτικά, προτείνεται η αποστολή της νέας κάρτας SIM μόνο μέσω συστημένης επιστολής με παράλληλη αποστολή ενημερωτικού SMS στον τηλεφωνικό αριθμό τον οποίο αφορά το αίτημα αντικατάστασης.

Τέλος, τον Ιούνιο 2021, η εταιρία προέβη εκ νέου σε επικαιροποίηση της από 2/3/2020 Μελέτης Εκτίμησης Αντικτύπου με αποτέλεσμα την υιοθέτηση και εφαρμογή των ακόλουθων μέτρων:

- Προσθήκη επιπλέον δικλίδων ασφαλείας κατά τη διαδικασία αντικατάστασης κάρτας SIM:
 - i. αποστολή μηνύματος συναίνεσης (SMS consent) στον αριθμό για τον οποίο έγινε το αίτημα αντικατάστασης κάρτας SIM, προκειμένου ο αιτών συνδρομητής/κάτοχος της SIM να επιβεβαιώσει το αίτημα,
 - ii. μετά την ολοκλήρωση κάθε αιτήματος αντικατάστασης κάρτας SIM αυτόματη ενεργοποίηση φραγής εισερχομένων SMS για χρονικό διάστημα δύο (2) ωρών.

Επίσης, τον Αύγουστο 2021, η εταιρεία προέβη σε επέκταση της χρονικής διάρκειας της φραγής εισερχομένων SMS από δύο (2) σε τέσσερις (4) ώρες, μέτρο το οποίο ισχύει μέχρι και σήμερα. Παράλληλα, η εταιρία επισημαίνει ότι έχει ήδη

υλοποιήσει ένα σύνολο ενεργειών εκπαίδευσης, ενημέρωσης και ευαισθητοποίησης του προσωπικού της. Ειδικότερα, αναφέρεται ότι η εταιρία από τις αρχές του έτους 2020 εκκίνησε τις διαδικασίες υλοποίησης: α) Προγράμματος ενημέρωσης και ευαισθητοποίησης του προσωπικού και β) Προγράμματος εκπαίδευσης του προσωπικού στις νέες διαδικασίες.

Ως προς τα περιστατικά παραβίασης για τα οποία κλήθηκε η εταιρία σε ακρόαση δόθηκαν διευκρινήσεις για δεκατέσσερις (14) από τις εξεταζόμενες υποθέσεις. Συγκεκριμένα επισημάνθηκαν τα ακόλουθα:

- Η υπ' αριθμ. πρωτ. Γ/ΕΙΣ/4807/10-7-2020 καταγγελία σχετίζεται με το περιστατικό που έχει γνωστοποιηθεί στην Αρχή με την υπ' αριθμ. πρωτ. Γ/ΕΙΣ/7103/16-10-2020 γνωστοποίηση περιστατικού παραβίασης.
- Για πέντε (5) περιστατικά τα οποία περιλαμβάνονται στην υπ' αριθμ. Γ/ΕΙΣ/7103/16-10-2020 γνωστοποίηση περιστατικού παραβίασης, η εταιρεία έχει κληθεί σε παροχή στοιχείων, τα οποία έχει παράσχει προς την ΑΔΑΕ. Ακολούθως έχει λάβει χώρα ακρόαση ενώπιον της ΑΔΑΕ και εκκρεμεί η έκδοση απόφασης.
- Για τρία (3) περιστατικά τα οποία περιλαμβάνονται στην υπ' αριθμ. Γ/ΕΙΣ/7103/16-10-2020 γνωστοποίηση περιστατικού παραβίασης, η εταιρεία έχει κληθεί σε παροχή στοιχείων, τα οποία έχει παράσχει προς την ΑΔΑΕ. Εκκρεμεί ενδεχόμενη κλήση της εταιρείας σε ακρόαση.
- Για την υπ' αριθμ. Γ/ΕΙΣ/7255/22-10-2020 γνωστοποίηση περιστατικού παραβίασης, η εταιρεία έχει κληθεί σε παροχή στοιχείων, τα οποία έχει παράσχει προς την ΑΔΑΕ. Εκκρεμεί ενδεχόμενη κλήση της εταιρείας σε ακρόαση.
- Για την υπ' αριθμ. Γ/ΕΙΣ/7299/23-10-2020 γνωστοποίηση περιστατικού παραβίασης, η εταιρεία έχει κληθεί σε παροχή στοιχείων, τα οποία έχει παράσχει προς την ΑΔΑΕ. Ακολούθως, έχει λάβει χώρα κλήση της εταιρείας σε ακρόαση ενώπιον της ΑΔΑΕ με καταληκτική ημερομηνία υποβολής υπομνήματος την 08-07-2022.
- Για την υπ' αριθμ. Γ/ΕΙΣ/7300/23-10-2020 γνωστοποίηση περιστατικού παραβίασης, η εταιρεία έχει κληθεί σε παροχή στοιχείων, τα οποία έχει

παράσχει προς την ΑΔΑΕ. Ακολούθως έχει λάβει χώρα ακρόαση ενώπιον της ΑΔΑΕ και εκκρεμεί η έκδοση απόφασης.

- Για την υπ' αριθμ. Γ/ΕΙΣ/7301/23-10-2020 γνωστοποίηση περιστατικού παραβίασης, η εταιρεία έχει κληθεί σε παροχή στοιχείων, τα οποία έχει παράσχει προς την ΑΔΑΕ. Ακολούθως έλαβε χώρα ακρόαση και μας επιδόθηκε η απόφαση της ΑΔΑΕ, η οποία επιβάλλει στην εταιρεία διοικητική κύρωση.
- Η με αρ. πρωτ. Γ/ΕΙΣ/5508/19-07-17 καταγγελία δεν συνιστά περιστατικό SIM swap fraud. Εν προκειμένω, υπήρξε απάτη στο πλαίσιο σύναψης νέας σύμβασης με την εταιρία. Η μεθοδολογία διαφέρει ουσιωδώς ως προς τις λοιπές υποθέσεις. Η υπόθεση εξετάζεται ήδη από την Ελληνική Δικαιοσύνη.

Συνοπτικά αναφέρεται ότι:

- για έξι (6) περιστατικά έχει λάβει χώρα ακρόαση ενώπιον της ΑΔΑΕ και εκκρεμεί η έκδοση απόφασης,
- για τέσσερα (4) περιστατικά, η εταιρεία έχει κληθεί σε παροχή στοιχείων, τα οποία έχει παράσχει προς την ΑΔΑΕ. Εκκρεμεί ενδεχόμενη κλήση της εταιρείας σε ακρόαση,
- για ένα (1) περιστατικό, έχει λάβει χώρα κλήση της εταιρείας σε ακρόαση ενώπιον της ΑΔΑΕ με καταληκτική ημερομηνία υποβολής υπομνήματος την 08-07-2022,
- για ένα (1) περιστατικό, επιδόθηκε η απόφαση της ΑΔΑΕ, η οποία επιβάλλει στην εταιρεία διοικητική κύρωση,
- μία καταγγελία δεν συνιστά περιστατικό SIM swap fraud, και
- μία καταγγελία σχετίζεται με ένα κοινοποιημένο περιστατικό παραβίασης.

Επιπλέον, η εταιρία αναφέρει ότι από τα ως άνω πραγματικά περιστατικά, σε συνδυασμό με τις περιεχόμενες στις γνωστοποιήσεις σχετικές πληροφορίες, προκύπτει ότι στις περισσότερες των υποθέσεων ακολουθήθηκε ορθώς η τότε ισχύουσα διαδικασία της Εταιρείας από τους αρμόδιους υπαλλήλους. Παρά ταύτα οι κακόβουλοι κατάφεραν μέσω προσκόμισης πλαστών εγγράφων να ολοκληρώσουν τις παράνομες πράξεις. Μόνο σε δύο περιπτώσεις διαπιστώνεται μη πιστή εφαρμογή των διαδικασιών της εταιρίας, καθώς δεν εφαρμόστηκε το επιπλέον μέτρο

ασφαλείας που είχε ληφθεί κατά τον χρόνο τέλεσης του περιστατικού από την εταιρία, ήτοι το μέτρο *«της τηλεφωνικής επικοινωνίας με τον αιτούντα συνδρομητή/κάτοχο της SIM για την οποία ζητείται αντικατάσταση να πραγματοποιείται σε τηλέφωνο επικοινωνίας του συνδρομητή, που έχει δηλωθεί από τον τελευταίο και υπάρχει αποθηκευμένο στα συστήματα της εταιρίας, σε περίπτωση που ο τηλεφωνικός αριθμός για τον οποίο ζητείται η αντικατάσταση SIM είναι απενεργοποιημένος.»*

Κατά τα λοιπά, στο σύνολο των υπόλοιπων περιπτώσεων τηρήθηκαν τα μέτρα ασφαλείας και οι διαδικασίες που είχαν θεσπισθεί και τεθεί σε εφαρμογή κατά τον χρόνο εκείνο.

Η εταιρία σημειώνει ότι οι κακόβουλοι δρούσαν συστηματικά, προμελετημένα και οργανωμένα, με την προσκόμιση και χρήση πλαστών εγγράφων στις περισσότερες των περιπτώσεων, με αποτέλεσμα να υπερβαίνουν τα οργανωτικά μέτρα ασφαλείας και τις λογικές υποψίες των υπαλλήλων της εταιρίας. Επιπλέον, αναφέρεται ότι η πρόκληση υποψιών δεν είναι αναμενόμενη όσον αφορά στον μέσο υπάλληλο παροχής υπηρεσιών κινητής τηλεφωνίας, καθόσον, παρά τη σχετική του εκπαίδευση, είναι αντικειμενικά λιγότερο εξοικειωμένος με απατηλές παραστάσεις ως προς την ταυτότητα προσώπων εμφανιζόμενων ως αντισυμβαλλομένων. Πολύ περισσότερο κρίνεται ως μη αναμενόμενη η πρόκληση αντίστοιχων υποψιών στους υπαλλήλους της εταιρίας, όταν οι εμφανιζόμενοι: α) είχαν πλήρη γνώση των προσωπικών δεδομένων/προσωπικών στοιχείων του συνδρομητή, τα οποία ανέφεραν σε υπαλλήλους της Εταιρείας, β) προσκόμιζαν πλαστά έγγραφα ταυτοπροσωπίας.

Τέλος, η εταιρία εγείρει ζήτημα ως προς την εφαρμογή της αρχής **ne bis in idem**, καθότι κάποια από τα περιστατικά ελέγχονται ήδη και από την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (εφεξής «ΑΔΑΕ»). Ειδικότερα, η εταιρία κάνει αναφορά στην απόφαση **122/2012** της ΑΠΔΠΧ σχετικά με την εφαρμογή εν λόγω αρχής σε περιπτώσεις επιβολής κυρώσεων από δύο διοικητικές αρχές για τα αυτά πραγματικά περιστατικά. Ειδικότερα: *«Επί του θέματος αυτού η Αρχή, κατά πλειοψηφία, κρίνει ότι όταν για τα αυτά (ή ουσιωδώς όμοια) πραγματικά περιστατικά, που ενέχουν προσβολή των αυτών ή και διαφόρων εννόμων αγαθών, και τα οποία αναφέρονται στα αυτά υπαίτια πρόσωπα (ταυτότητα πράξεων και*

παραβατών), έχει επιληφθεί και εξέδωσε απόφαση η πρώτη αρμόδια αρχή, η δε κρίση της είναι επί της ουσίας της υποθέσεως, τότε δεν είναι δυνατόν να επιληφθεί της κρίσεως αυτών για ενδεχόμενη επιβολή κυρώσεων η δεύτερη αρμόδια αρχή. Συνεπώς, στη συγκεκριμένη περίπτωση αν έχει επιληφθεί το ΕΣΡ και κρίνει επί της ουσίας πραγματικά περιστατικά, τα οποία αποτελούν περιεχόμενο τηλεοπτικής ή ραδιοφωνικής εκπομπής, τα οποία συνιστούν ενδεχομένως και προσβολή του δικαιώματος στην προστασία των προσωπικών δεδομένων, τότε η ΑΠΔΠΧ όταν καλείται να επιληφθεί ως δεύτερο αρμόδιο όργανο, δεν είναι δυνατόν να ασκήσει την κυρωτική αρμοδιότητά της προβαίνοντας σε σχετική έρευνα, διαπίστωση της παράβασης και επιβολή κυρώσεων, αλλά υποχρεούται να προβεί στη διαπίστωση ότι για τα αυτά (ή ουσιωδώς όμοια) πραγματικά περιστατικά υπάρχει επί της ουσίας κρίση του ΕΣΡ και οφείλει να απόσχει της εξετάσεως των πραγματικών αυτών περιστατικών.

Αν και κατά τη γνώμη τριών μελών η αρχή *ne bis in idem* δεν καλύπτει απλώς τη σύμπτωση των αυτών πραγματικών περιστατικών και υπαιτίων προσώπων (ταυτότητα πράξεως και παραβάτου) αλλά εφαρμόζεται μόνον στην περίπτωση που τα αυτά πραγματικά περιστατικά αποτελούν προσβολή του αυτού εννόμου αγαθού και εξυπηρετούνται οι αυτοί σκοποί προστασίας του κοινωνικού συνόλου, και συνεπώς εφόσον η Αρχή έχει ως αποστολή την προστασία των προσωπικών δεδομένων, καθ'εαυτών και όχι της προσωπικότητας εν γένει, εξακολουθεί να διατηρεί την αρμοδιότητα επιβολής κυρώσεων καίτοι το ΕΣΡ, κατά τον έλεγχο των ραδιοτηλεοπτικών εκπομπών, έχει αρμοδιότητα επιβολής κυρώσεων για προσβολή του σεβασμού της αξίας του ανθρώπου και της προσωπικότητας εν γένει.»

Η εταιρία αναφέρει ότι αντίστοιχες νομολογιακές θέσεις έχουν διατυπωθεί και σε αποφάσεις του Συμβουλίου της Επικρατείας [Απόφαση 1091/2015 (ΣτΕ Τμήμα Δ'- Παραπομπή σε Επταμελή Σύμβαση), η οποία ταυτίζεται με την άποψη της πλειοψηφίας της ΑΠΔΠΧ, καθώς και η Απόφαση 2797/2015 (ΣτΕ Τμήμα Δ'), η οποία ακολουθεί την άποψη της μειοψηφίας της ΑΠΔΠΧ].

Δοσμένης λοιπόν της ιδιαίτερης φύσης της υπό κρίση υπόθεσης και των επί μέρους πτυχών της, η εταιρία διαπιστώνει ότι υφίσταται ταυτότητα της αντικειμενικής υπόστασης των περιστατικών που εξετάζονται από τις δυο Αρχές, τόσο από την ΑΠΔΠΧ όσο και από την ΑΔΑΕ, και παρατηρείται πλήρης ταύτιση των

πραγματικών περιστατικών ως προς το πεδίο ελέγχου των δύο Αρχών ως περιστατικά παραβίασης υπό το πρίσμα της εφαρμογής της αυτής νομοθεσίας (Νόμος 3471/2006 άρθρο 12 παράγραφος 5, ως έχει τροποποιηθεί και ισχύει) και για το λόγο τούτο η εταιρία εγείρει τον προβληματισμό της ως προς την εφαρμογή της αρχής ne bis in idem. Επιπλέον διαπιστώνει ότι η τυχόν επιβολή κυρώσεων από τις πιο πάνω Αρχές σε βάρος της εταιρίας δεν θα ήταν δυνατή με βάση τη γενική αρχή του διοικητικού δικαίου περί μη επιβολής σωρευτικών διοικητικών κυρώσεων για την ίδια πράξη (ne bis in idem).

Η Αρχή, μετά από εξέταση όλων των στοιχείων του φακέλου και αναφορά στα διαμειφθέντα της ακροαματικής διαδικασίας, αφού άκουσε τον εισηγητή και τις διευκρινίσεις των βοηθών εισηγητή και κατόπιν διεξοδικής συζήτησης,

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Από τις διατάξεις των άρθρων 51 και 55 του Γενικού Κανονισμού Προστασίας Δεδομένων (Κανονισμού (ΕΕ) 2016/679 – εφεξής, ΓΚΠΔ) και του άρθρου 9 του νόμου 4624/2019 (ΦΕΚ Α΄ 137) προκύπτει ότι η Αρχή έχει αρμοδιότητα να εποπτεύει την εφαρμογή των διατάξεων του ΓΚΠΔ, του νόμου αυτού και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων.
2. Σύμφωνα με το άρθρο 4 παρ. 1 του 7ου Πρωτοκόλλου της Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου (Ε.Σ.Δ.Α.), το οποίο κυρώθηκε με το άρθρο πρώτο του Ν. 1705/1987 (ΦΕΚ 89 Α΄), «*κανένας δεν μπορεί να διωχθεί ή καταδικασθεί ποινικά από τα δικαστήρια του ίδιου Κράτους για μία παράβαση για την οποία ήδη αθωώθηκε ή καταδικάστηκε με αμετάκλητη απόφαση σύμφωνα με το νόμο και την ποινική δικονομία του Κράτους αυτού*». Με την εν λόγω διάταξη καθιερώνεται η αρχή non bis in idem, η οποία όπως γίνεται παγίως δεκτό από τη νομολογία του ΕΔΔΑ, του ΔΕΕ αλλά και του ΣτΕ, εφαρμόζεται όχι μόνο επί ποινικών κυρώσεων αλλά και στις περιπτώσεις που από τη σχετική νομοθεσία προβλέπεται η επιβολή σοβαρών διοικητικών κυρώσεων, όπως είναι τα πρόστιμα μεγάλου ύψους. Βασική προϋπόθεση για την εφαρμογή της αρχής non bis in idem, κατά τη Νομολογία του ΣτΕ, είναι **να έχει επιβληθεί κύρωση** στο

πλαίσιο διοικητικής διαδικασίας, η οποία να έχει **οριστικοποιηθεί**, είτε λόγω μη άσκησης ενδίκου βοηθήματος είτε λόγω απόρριψης του ασκηθέντος ενδίκου βοηθήματος (ΣτΕ 951/2018, 4309/2015). Εν προκειμένω, όπως προκύπτει από το υπόμνημα της καταγγελλόμενης εταιρίας, από την ΑΔΑΕ έχουν επιβληθεί σε βάρος της κυρώσεις μόνο σε δύο περιπτώσεις (Β, Γ), κατά των οποίων η καταγγελλόμενη δηλώνει ήδη ότι προτίθεται να προσφύγει ενώπιον του αρμόδιου Δικαστηρίου. Συνεπώς, δεν συντρέχει περίπτωση επιβολής οριστικοποιημένης κύρωσης εκ μέρους της ΑΔΑΕ, η οποία να εμποδίζει την εξέταση των υπό κρίση καταγγελιών από την Αρχή, κατ' εφαρμογή της αρχής non bis in idem. Ανεξαρτήτως αυτού, οι εξεταζόμενες στην παρούσα υπόθεση παραβιάσεις συνιστούν προσβολή έννομου αγαθού διαφορετικού εκείνου που θίγεται με τις παραβάσεις, για τις οποίες έχουν επιβληθεί κυρώσεις στην εταιρία από την ΑΔΑΕ και οι οποίες αφορούν αποκλειστικά στην εφαρμογή ή μη των πολιτικών των υπευθύνων επεξεργασίας (αρ. 12 παρ. 3 εδ. γ ν.3471/06) και όχι, εκτός αυτού, στην αποτελεσματικότητα των μέτρων που περιγράφονται σε αυτές και που ακολουθούνται βάσει αυτών και που εν τέλει καίτοι εφαρμόστηκαν δεν ήταν επαρκή ώστε να αποτρέψουν τα διαπιστωμένα περιστατικά παραβιάσεων των δεδομένων του συνδρομητή. ... Συνεπώς, και για το λόγο αυτό δεν έχει εφαρμογή στην προκειμένη περίπτωση η αρχή non bis in idem σύμφωνα με την πρόσφατη Νομολογία του ΣτΕ (βλ. ΣτΕ 433/2021, 1771/2019, 3473/2017), με την οποία γίνεται δεκτό ότι *είναι δυνατή η επιβολή στον ίδιο παραβάτη για τα ίδια πραγματικά περιστατικά δύο διοικητικών κυρώσεων από διαφορετικά διοικητικά όργανα ή ανεξάρτητες διοικητικές αρχές, αν η επιβολή τους αποβλέπει στην προστασία ιδιαιτέρως σημαντικών και διαφορετικών εννόμων αγαθών διότι τυχόν αδυναμία επιβολής της μιας από τις δύο διοικητικές κυρώσεις κατ' εφαρμογή της αρχής non bis in idem, εφόσον έχει ήδη επιβληθεί και οριστικοποιηθεί η μια από αυτές θα καθιστούσε ανενεργή την υποχρέωση που έχουν από το Σύνταγμα διαφορετικά κρατικά όργανα να προστατεύουν τους διγομένους στα ατομικά τους δικαιώματα* (ΣτΕ 433/2021, 3473/2017) και ότι η αρχή αυτή ούτε απαγορεύει την σωρευτική επιβολή κυρώσεων κατ' επίκληση διατάξεων που τελούν σε αληθή κατ' ιδέαν συρροή ούτε επιβάλλει «ενότητα διαδικασίας» (in a via), και, ακριβώς για τον λόγο αυτό δεν **μπορεί να θεωρηθεί**

ότι απαγορεύει να επιβληθούν οι κυρώσεις αυτές από διαφορετικές αρχές με ανεξάρτητες και αυτοτελείς διαδικασίες (ΣΤΕ 1771/2019).

3. Σύμφωνα με το άρθρο 4 του ΓΚΠΔ, ως δεδομένα προσωπικού χαρακτήρα ορίζεται «κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο» και ως υπεύθυνος επεξεργασίας ορίζεται «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», ενώ ως εκτελών την επεξεργασία ορίζεται «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας».
4. Στο ίδιο άρθρο ορίζεται η παραβίαση δεδομένων προσωπικού χαρακτήρα ως «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».
5. Σύμφωνα με το άρθρο 5 παρ. 3 του ΓΚΠΔ ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωσή του με τις αρχές της επεξεργασίας που καθιερώνονται στην παράγραφο 1 του ίδιου άρθρου, στις οποίες συμπεριλαμβάνεται η νομιμότητα, αντικειμενικότητα και διαφάνεια της επεξεργασίας σύμφωνα με το άρθρο 5 παρ. 1 στοιχ. α', και η εμπιστευτικότητα και ακεραιότητα των δεδομένων σύμφωνα με το άρθρο άρθρο 5 παρ. 1 στοιχ. στ'. Με άλλα λόγια, με τον ΓΚΠΔ υιοθετήθηκε ένα μοντέλο συμμόρφωσης με κεντρικό πυλώνα την εν λόγω αρχή της λογοδοσίας, ήτοι ο υπεύθυνος επεξεργασίας υποχρεούται να σχεδιάζει, εφαρμόζει και εν γένει λαμβάνει τα αναγκαία μέτρα και πολιτικές, προκειμένου η επεξεργασία των δεδομένων να είναι σύμφωνη με τις σχετικές νομοθετικές προβλέψεις και, επιπλέον, οφείλει να αποδεικνύει ο ίδιος και ανά πάσα στιγμή τη συμμόρφωσή του με τις αρχές του άρθρου 5 παρ. 1 ΓΚΠΔ.

6. Σύμφωνα με το άρθρο 12 παρ. 5, του ν.3471/06 «σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών γνωστοποιεί αμελλητί την παραβίαση στην Α.Π.Δ.Π.Χ. Η γνωστοποίηση ... περιλαμβάνει κατ' ελάχιστον περιγραφή της φύσης της παραβίασης δεδομένων προσωπικού χαρακτήρα και των σημείων επαφής από τα οποία μπορούν να αποκτηθούν περισσότερες πληροφορίες. Περιγράφονται επίσης οι συνέπειες της παραβίασης και τα μέτρα που προτάθηκαν ή λήφθηκαν από τον φορέα για την αντιμετώπιση της παραβίασης.».
7. Σύμφωνα με το άρθρο 12 παρ. 1 του παραπάνω νόμου, «ο φορέας παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να λαμβάνει τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα, προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του, καθώς και η ασφάλεια του δημοσίου δικτύου ηλεκτρονικών επικοινωνιών. Τα μέτρα αυτά, εφόσον είναι αναγκαίο, λαμβάνονται από κοινού με τον φορέα παροχής του δημοσίου δικτύου ηλεκτρονικών επικοινωνιών, πρέπει δε να εγγυώνται επίπεδο ασφαλείας ανάλογο προς τον υπάρχοντα κίνδυνο, λαμβανομένων υπόψη αφ' ενός των πλέον προσφάτων τεχνικών δυνατοτήτων αφ' ετέρου δε του κόστους εφαρμογής τους.».
8. Σύμφωνα με το άρθρο 12 παρ. 3 του ν.3471/06, «... με τα μέτρα του παρόντος άρθρου κατ' ελάχιστον: α) εξασφαλίζεται ότι πρόσβαση σε δεδομένα προσωπικού χαρακτήρα μπορεί να έχει μόνον εξουσιοδοτημένο προσωπικό για νομίμως εγκεκριμένους σκοπούς, β) προστατεύονται τα αποθηκευμένα ή διαβιβασθέντα δεδομένα προσωπικού χαρακτήρα από τυχαία ή παράνομη καταστροφή, τυχαία απώλεια ή αλλοίωση και από μη εξουσιοδοτημένη ή παράνομη επεξεργασία, συμπεριλαμβανομένης της αποθήκευσης, πρόσβασης ή αποκάλυψης και γ) διασφαλίζεται η εφαρμογή πολιτικής ασφαλείας σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα.».
9. Σύμφωνα με την παράγραφο 6 του ίδιου άρθρου, «όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να έχει δυσμενείς επιπτώσεις στα δεδομένα προσωπικού χαρακτήρα ή την ιδιωτική ζωή του συνδρομητή ή άλλου ατόμου, ο φορέας ενημερώνει αμελλητί για την παραβίαση αυτή και τον θιγόμενο συνδρομητή ή το θιγόμενο άτομο. Η ενημέρωση του προηγούμενου εδαφίου

περιλαμβάνει κατ' ελάχιστον περιγραφή της φύσης της παραβίασης δεδομένων προσωπικού χαρακτήρα και των σημείων επαφής από τα οποία μπορούν να αποκτηθούν περισσότερες πληροφορίες, καθώς και συστάσεις που δύνανται να περιορίσουν ενδεχόμενα δυσμενή αποτελέσματα της παραβίασης δεδομένων προσωπικού χαρακτήρα.».

10. Περαιτέρω, στην παράγραφο 7 του άρθρου αυτού ορίζεται ότι «η ενημέρωση του θιγόμενου συνδρομητή ή του θιγόμενου ατόμου για την παραβίαση δεδομένων προσωπικού χαρακτήρα δεν είναι αναγκαία, εάν ο φορέας έχει αποδείξει κατά ικανοποιητικό τρόπο στις αρμόδιες αρχές, ότι έχει εφαρμόσει τα κατάλληλα τεχνολογικά μέτρα προστασίας και ότι τα μέτρα αυτά εφαρμόστηκαν για τα δεδομένα που αφορούσε η παραβίαση της ασφάλειας. Αυτά τα τεχνολογικά μέτρα προστασίας πρέπει, κατ' ελάχιστον, να περιλαμβάνουν ασφαλή κρυπτογράφηση των δεδομένων, ώστε να μην είναι δυνατή η μη εξουσιοδοτημένη πρόσβαση. Αν ο φορέας δεν έχει προβεί σε ενημέρωση σύμφωνα με την παράγραφο 6 του παρόντος άρθρου, οι αρμόδιες αρχές, αφού εξετάσουν τις πιθανές δυσμενείς επιπτώσεις της παραβίασης, δύνανται να του ζητήσουν να το πράξει.».
11. Αναφορικά με τα περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα που έχουν καταγραφεί και παρατίθενται στο Παράρτημα προκύπτουν οι ακόλουθες τρεις κατηγορίες παραβάσεων:
 - A. Δεν εφαρμόστηκε η τρέχουσα πολιτική και τα μέτρα που σχετίζονται με την διαδικασία αντικατάστασης της κάρτας SIM. Συγκεκριμένα, έχουν καταγραφεί τρία (3) περιστατικά για την 1η περίοδο, τρία (3) περιστατικά για την 2η περίοδο και 2 περιστατικά για την 4η περίοδο.
 - B. Τα μέτρα που εφαρμόζονταν σχετικά με τον έλεγχο ταυτοποίησης των πελατών κατά τη διαδικασία αντικατάστασης της κάρτας SIM δεν ήταν επαρκή ώστε να εμποδίσουν την εκμετάλλευση αδυναμιών στην υπάρχουσα πολιτική και την παραβίαση προσωπικών δεδομένων. Συγκεκριμένα, έχουν καταγραφεί οκτώ (8) περιστατικά για την 1η περίοδο και δύο (2) περιστατικά για την 2η περίοδο.
 - Γ. Τα μέτρα που εφαρμόζονταν σχετικά με τον έλεγχο ταυτοποίησης των πελατών κατά την διαδικασία εξυπηρέτησης αιτήσεων για άλλες υπηρεσίες

(πχ. εκτροπή κλήσεων, έκδοση νέων αριθμών τηλεφώνων συνδρομητή) δεν ήταν αποτελεσματικά ώστε να εμποδίσουν την εκμετάλλευση αδυναμιών στην υπάρχουσα πολιτική και την παραβίαση προσωπικών δεδομένων. Συγκεκριμένα, έχουν καταγραφεί δύο (2) περιστατικά για την 2η περίοδο, δύο (2) περιστατικά για την 3η περίοδο και τρία (3) περιστατικά για την 4η περίοδο.

Λαμβάνοντας υπόψη την προαναφερθείσα κατηγοριοποίηση των περιστατικών διαπιστώνονται τα ακόλουθα:

- I. Από την αξιολόγηση των περιστατικών που ανήκουν στις τρεις κατηγορίες (Α, Β και Γ) προκύπτει ότι τα μέτρα ασφάλειας που εφαρμόζονταν στις αντίστοιχες χρονικές περιόδους δεν ήταν τα ενδεδειγμένα προκειμένου να εξασφαλιστεί σε επαρκές επίπεδο η ασφάλεια των προσφερόμενων υπηρεσιών καθώς και η ασφάλεια του δημοσίου δικτύου ηλεκτρονικών επικοινωνιών (άρθρο 12, παρ.1 του ν. 3471/06). Σημειώνεται ότι το επίπεδο ασφαλείας πρέπει να είναι ανάλογο προς τον υπάρχοντα κίνδυνο, λαμβανομένων υπόψη αφ' ενός των πλέον προσφάτων τεχνικών δυνατοτήτων αφ' ετέρου δε του κόστους εφαρμογής τους. Στην προκειμένη περίπτωση, παρά το γεγονός ότι η εταιρία φαίνεται να ενήργησε προκειμένου να αντιμετωπίσει τις προσεγγίσεις που ακολουθούν οι κακόβουλοι και να περιορίσει την εμφάνιση σχετικών περιστατικών, η αναθεώρηση των ισχυουσών πολιτικών και η υιοθέτηση των πρόσθετων μέτρων δεν στάθηκε ικανή να εμποδίσει την εμφάνιση νέων περιστατικών.
- II. Επιπρόσθετα διαπιστώνεται ότι περιστατικά, τα οποία εμφανίζονται κυρίως τη 3^η και 4^η χρονική περίοδο, σχετίζονται με την εκμετάλλευση αδυναμιών στη διαδικασία ταυτοποίησης των πελατών σε διάφορες υπηρεσίες (π.χ. διαδικασία σύνδεσης ενός αριθμού με έναν άλλο, διαδικασία εκτροπής κλήσης από έναν αριθμό σε άλλο αριθμό, διαδικασία αντικατάστασης της κάρτας SIM). Το γεγονός αυτό εγείρει επιπλέον ζητήματα σχετικά με την ασφάλεια τόσο των προσφερόμενων υπηρεσιών όσο και του δημοσίου δικτύου ηλεκτρονικών επικοινωνιών (άρθρο 12, παρ.1 του ν. 3471/06).
- III. Από την ανάλυση των περιστατικών που ανήκουν στην πρώτη (1) κατηγορία κρίνεται ότι υπήρχαν περιπτώσεις όπου οι πολιτικές που ίσχυαν στις

αντίστοιχες χρονικές περιόδους δεν εφαρμόστηκαν (άρθρο 12, παρ.3, εδ.γ του ν. 3471/06). Σημειώνεται ότι περιστατικά μη εφαρμογής της υπάρχουσας πολιτικής και των ισχυόντων μέτρων εμφανίζονται σε όλες τις περιόδους.

Από τις ανωτέρω διαπιστώσεις προκύπτουν δύο κατηγορίες παραβιάσεων.

Συγκεκριμένα:

1. Από την πρώτη και δεύτερη διαπίστωση (I, II ανωτέρω) προκύπτει ότι η εταιρία εφάρμοζε στις τέσσερις διαδοχικές χρονικές περιόδους πολιτικές οι οποίες ήταν ελλιπείς (άρθρο 12 παρ. 1, ν. 3471/2006).
2. Από τη τρίτη διαπίστωση (III ανωτέρω) προκύπτει ότι υπήρχαν περιπτώσεις μη εφαρμογής των ισχυουσών πολιτικών της εταιρίας (άρθρο 12 παρ. 3 εδ. γ, ν. 3471/2006).

Επίσης, παρατηρήθηκαν περιπτώσεις (τουλάχιστον πέντε) στις οποίες τα περιστατικά δεν γνωστοποιήθηκαν αμελλητί στην Αρχή (σημειώθηκαν αποκλίσεις μεταξύ του χρόνου κατά τον οποίο έγινε γνωστό το περιστατικό στον υπεύθυνο επεξεργασίας και του χρόνου υποβολής της γνωστοποίησής του στην Αρχή, της τάξεως από 2-3 μήνες έως και πέραν του εξαμήνου).

Βάσει των ανωτέρω, η Αρχή κρίνει ομόφωνα ότι σύμφωνα με το άρθρο 12 του ν. 3471/2006, συντρέχουν οι προϋποθέσεις επιβολής σε βάρος των υπευθύνων επεξεργασίας, με βάση αφενός το άρθρο 13 του ν. 3471/2006, σε συνδυασμό με το άρθρο 21 παρ. 1 στοιχ. β' του ν. 2472/1997 και με το άρθρο του 84 ν. 4624/2019, και αφετέρου το άρθρο 58 παρ. 2 εδ. θ' του Κανονισμού και το άρθρο 15 παρ. 6 του ν. 4624/2019, της διοικητικής κύρωσης, που αναφέρεται στο διατακτικό της παρούσας, η οποία κρίνεται ανάλογη με τη βαρύτητα της παράβασης.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Επιβάλλει, στην εταιρία το αποτελεσματικό, αναλογικό και αποτρεπτικό διοικητικό χρηματικό πρόστιμο που αρμόζει στην συγκεκριμένη περίπτωση σύμφωνα με τις ειδικότερες περιστάσεις αυτής, ύψους εκατόν πενήντα χιλιάδων ευρώ

(150.000,00) ευρώ, για τις ως άνω διαπιστωθείσες παραβιάσεις του άρθρου 12 του ν. 3471/2006.

Ο Πρόεδρος

Η Γραμματέας

Κων/νος Μενουδάκος

Ειρήνη Παπαγεωργοπούλου