ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Αθήνα, 02-12-2022
Αριθ. Πρωτ.: 3093

ΑΠΟΦΑΣΗ 39/2022

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 Λεωνίδας Ρούσσος, 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 swap) αλλά και άλλων διαδικασιών (π.χ. εκτροπής κλήσεων, έκδοσης νέων αριθμών τηλεφώνων) από τρίτους, μη κατόχους των εν λόγω συνδέσεων.

Πιο συγκεκριμένα, αρχικά, υποβλήθηκαν οι με αρ. πρωτ. Γ/ΕΙΣ/2649/13-04-2020, Γ/ΕΙΣ/2662/14-04-2020, Γ/ΕΙΣ/2663/14-04-2020, Γ/ΕΙΣ/2806/24-04-2020, Γ/ΕΙΣ/2896/27-04-2020, Γ/ΕΙΣ/3012/04-05-2020, Γ/ΕΙΣ/3127/08-05-2020,

Γ/ΕΙΣ/3128/08-05-2020, Γ/ΕΙΣ/3142/11-05-2020, Γ/ΕΙΣ/3143/11-05-2020, Γ/ΕΙΣ/3209/12-05-2020, Γ/ΕΙΣ//3244/13-05-2020, Γ/ΕΙΣ/3246/13-05-2020, Γ/ΕΙΣ/3910/09-06-2020, Γ/ΕΙΣ/4348/23-06-2020, Γ/ΕΙΣ/4436/26-06-2020, Γ/ΕΙΣ/4584/02-07-2020, Γ/ΕΙΣ/4653/03-07-2020, Γ/ΕΙΣ/5173/03-07-2020, Γ/ΕΙΣ/5368/31-07-2020, Γ/ΕΙΣ/5468/05-08-2020, Γ/ΕΙΣ/5590/11-08-2020, Γ/ΕΙΣ/6471/24-09-2020, Γ/ΕΙΣ/7233/21-10-2020, Γ/ΕΙΣ/7254/22-10-2020, Γ/ΕΙΣ/7485/2-11-2020 καταγγελίες και γνωστοποιήσεις περιστατικών παραβίασης.

Η Αρχή, στο πλαίσιο της εξέτασης των υποθέσεων αυτών, απέστειλε στην εταιρεία παροχής υπηρεσιών κινητής τηλεφωνίας COSMOTE ΚΙΝΗΤΕΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ Α.Ε & ΟΤΕ ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ Α.Ε (εφεξής «Cosmote" ή «υπεύθυνος επεξεργασίας») το υπ' αριθμ. πρωτ. Γ/ΕΞ/7774/11-11-2020 έγγραφο, με το οποίο ζητήθηκαν οι απόψεις της αναφορικά με τις σχετικές καταγγελίες, τα γνωστοποιηθέντα περιστατικά παραβίασης αλλά και τον γενικότερο τρόπο αντιμετώπισής 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/8858/28-12-2020 έγγραφο. Σύμφωνα με αυτό, τα μέτρα που εφαρμόζονταν ανά χρονική περίοδο είναι τα παρακάτω.

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

Στο διάστημα αυτό για την αντικατάσταση κάρτας SIM στα υποκαταστήματα της εταιρείας η διαδικασία που ίσχυε προέβλεπε τα ακόλουθα:

a. Σε περίπτωση φυσικής παρουσίας του συνδρομητή στο κατάστημα, επίδειξη πρωτότυπου δικαιολογητικού ταυτοπροσωπίας.

b. Σε περίπτωση που στο κατάστημα εμφανίζονταν τρίτο πρόσωπο για να αιτηθεί την αντικατάσταση της κάρτας για λογαριασμό του συνδρομητή απαιτούνταν η επίδειξη εξουσιοδότησης του συνδρομητή προς το τρίτο πρόσωπο με βεβαίωση του γνησίου της υπογραφής του από ΚΕΠ ή Αστυνομικό Τμήμα, καθώς και επίδειξη πρωτότυπου δικαιολογητικού ταυτοπροσωπίας του εξουσιοδοτούμενου. Αντίγραφο της εξουσιοδότησης αρχειοθετούνταν για σκοπούς απόδειξης.

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

Ειδικότερα από τις 8.4.2020, τα αιτήματα αντικατάστασης κάρτας SIM εξυπηρετούνται μόνο με φυσική παρουσία του συνδρομητή στο κατάστημα. Αιτήματα που υποβάλλονται στο κατάστημα από τρίτο πρόσωπο με εξουσιοδότηση του συνδρομητή δεν ολοκληρώνονται. Σε περίπτωση υποβολής αιτήματος από τρίτον για λογαριασμό του συνδρομητή, η διαχείριση του αιτήματος γίνεται τηλεφωνικά από την Εξυπηρέτηση Πελατών, ως εξής: Ο εργαζόμενος του δικτύου καταστημάτων επικοινωνεί τηλεφωνικά με την Εξυπηρέτηση Πελατών και αναφέρει ότι έχει προσκομιστεί εξουσιοδότηση από τρίτο. Η αντικατάσταση της κάρτας γι’ αυτήν την περίπτωση πραγματοποιείται σύμφωνα με την υφιστάμενη διαδικασία της Εξυπηρέτησης Πελατών και όχι από το δίκτυο καταστημάτων. Συγκεκριμένα, εφαρμόζονται τα παρακάτω μέτρα ασφάλειας: Πραγματοποιείται τηλεφωνική ταυτοποίηση του συνδρομητή της τηλεφωνικής σύνδεσης για την οποία υπάρχει αίτημα αντικατάστασης κάρτας SIM με σκοπό την επιβεβαίωση του αιτήματος. Εάν όντως επιβεβαιωθεί το αίτημα, η κάρτα SIM αποστέλλεται στον συνδρομητή μέσω courier και στη συνέχεια ενεργοποιείται.

3η περίοδος: **Πολιτικές που εφαρμόζονταν από την εταιρεία μετά τον Οκτώβριο 2020**

Συγκεκριμένα, από τις 19.10.2020 αποστέλλεται το παρακάτω ενημερωτικό μήνυμα στον αριθμό κινητού του πελάτη για τον οποίο υπάρχει αίτημα αντικατάστασης κάρτας SIM «Για τον αριθμό κινητού 697XXXXXX έχετε αιτηθεί την αντικατάσταση κάρτας sim. Σε περίπτωση που η αίτηση δεν έγινε από εσάς επικοινωνήστε άμεσα με το 13888»

Με το με αριθμ. πρωτ. Γ/ΕΞΕ/700/15-03-2022 έγγραφο, η Αρχή κάλεσε την εταιρία ενώπιόν της στη συνεδρίαση της την Τετάρτη 22-03-2022, για να δώσει περαιτέρω διευκρινίσεις και να εκθέσει, επιπλέον, διεξοδικά τις απόψεις της επί των περιστατικών παραβίασης και των συναφών, με αρ. πρωτ. Γ/ΕΙΣ/ 5626/25-07-17, Γ/ΕΙΣ/934/06-02-2021, Γ/ΕΙΣ/2274/01-04-2021, Γ/ΕΙΣ/3838/11-06-2021 καταγγελιών, για τις οποίες είχε ήδη υποβάλλει της απόψεις της, με τα με αρ. πρωτ. Γ/ΕΙΣ/8867/18-12-2019, Γ/ΕΙΣ/4369/01-07-2021, Γ/ΕΙΣ/5007/29-07-2021 και Γ/ΕΙΣ/6908/26-10-2021 υπομνήματα, αντίστοιχα, επί των οποίων απαιτούνταν διευκρινήσεις, καθώς και για την μ ε αρ. πρωτ. Γ/ΕΙΣ/1771/10-03-21 καταγγελία. 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 Α, Υποδιευθυντής Υποστήριξης & Εκπαίδευσης Δικτύων Πωλήσεων Ομίλου ΟΤΕ, Β, Υποδιευθυντής Residential Customer Service & Sales ΟΤΕ – COSMOTE, Ελένη Γέρουτση, Δικηγόρος, ΑΜ … και η Γ, Υπεύθυνη Προστασίας Δεδομένων του Ομίλου του ΟΤΕ και οι οποίοι απάντησαν στα ερωτήματα που της ετέθησαν, ενώ υποστήριξαν εκ νέου όσα η εταιρία είχε εκθέσει με το ανωτέρω έγγραφό της. Επιπλέον, η εταιρία υποστήριξε ότι η εξέταση των υποθέσεων από την Αρχή παραβιάζει την Αρχή της εκκρεμοδικίας και την αρχή ne bis in idem, καθότι η εταιρία ελέγχονταν για πολλά από τα ανωτέρω περιστατικά και από την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (εφεξής «ΑΔΑΕ»), για πολλά από τα οποία έχουν εκδοθεί Αποφάσεις ή/και Πορίσματα της ΑΔΑΕ, ενώ σε δύο από αυτές τις περιπτώσεις έχει επιβληθεί από την ΑΔΑΕ στην εταιρία διοικητικό πρόστιμο ύψους 30.000 ευρώ και 50.000 ευρώ αντίστοιχα.

Η εταιρία έλαβε προθεσμία για την υποβολή υπομνήματος, το οποίο και κατέθεσε με το με αρ. πρωτ. Γ/ΕΙΣ/7531/30-05-2022 μήνυμα ηλεκτρονικού ταχυδρομείου, στο οποίο επισυνάπτει τα Πορίσματα και τις Αποφάσεις της ΑΔΑΕ σε σχέση με είκοσι πέντε (25) περιστατικά παραβίασης, αλλά παρέχει και διευκρινήσεις αναφορικά με τις πολιτικές που εφαρμόζονταν σε κάθε περίοδο από την εταιρία.

Συμπληρώνει, δε, ότι κατά την 3η περίοδο αποστέλλεται και κωδικός ασφαλείας (one time password - otp) στον πελάτη μέσω SMS, προκειμένου να ολοκληρωθεί η ενεργοποίηση της νέας κάρτας SIM. Προσθέτει, ότι, από τις 8-2-2021, στην περίπτωση υποβολής αντικατάστασης της κάρτας sim στα καταστήματα, ενεργοποιείται ολική φραγή της παλιάς κάρτας για 6 ώρες και μετά ενεργοποιείται η νέα με φραγή εισερχομένων sms για 18 ώρες, ενώ αν αυτό πραγματοποιηθεί στην εξυπηρέτηση πελατών η φραγή της παλιάς κάρτας είναι διαρκής.

Στην περίπτωση τηλεφωνικού αιτήματος αντικατάστασης δίνονται πληροφορίες για τα στοιχεία ταυτοποίησης τα οποία επαληθεύονται και περιλαμβάνουν το ονοματεπώνυμο, το ΑΦΜ, το ΑΔΤ, το όνομα πατρός, την ημ/νία γέννησης, την δ/νση αποστολής λογαριασμού και το εισπρακτικό σημείο που εξοφλήθηκε ο τελευταίος λογαριασμός. Στην περίπτωση μη απάντησης της επιβεβαιωτικής εξερχόμενης κλήσης από την εξυπηρέτηση πελατών από τον «αιτούντα» στα στοιχεία που βρίσκονται δηλωμένα στο σύστημα ή σε περίπτωση που ο τελευταίος δεν διαθέτει άλλη σύνδεση στο δίκτυο της εταιρίας, τότε ενημερώνεται ότι πρέπει να μεταβεί σε κατάστημα για την ολοκλήρωση του αιτήματος.

Σύμφωνα με το εν λόγω υπόμνημα η διαδικασία ταυτοποίησης του συνδρομητή κατά την ενεργοποίηση της προώθησης κλήσεων ισχυροποιήθηκε από τον Μάρτιο 2021, καθώς ο συνδρομητής καθοδηγείται να πραγματοποιήσει ο ίδιος την εκτροπή από την συσκευή του, εφόσον είναι διαθέσιμη, διαφορετικά ακολουθείται η διαδικασία επαλήθευσης που περιεγράφηκε παραπάνω. Στην περίπτωση που ο συνδρομητής έχει ενεργοποιημένη προώθηση στην σύνδεση που πρόκειται να πραγματοποιηθεί η κλήση επιβεβαίωσης, τότε του προτείνονται η άρση της, η αποστολή ενυπόγραφου αιτήματος ηλεκτρονικού ταχυδρομείου και τέλος η μετάβασή του σε κατάστημα.

Η εταιρία, με το ανωτέρω υπόμνημά της, δήλωσε εξάλλου ότι επανεκτιμά σε τακτική και έκτακτη βάση το επίπεδο ασφάλειας των υφιστάμενων μέτρων, όπως έκανε και στις ανωτέρω περιπτώσεις, καθώς και ότι εφαρμόζει διαδικασία εκτίμησης κινδύνων ασφάλειας πληροφοριακών συστημάτων, ενώ το αμέσως επόμενο διάστημα πρόκειται να εφαρμοστεί ανάλογη διαδικασία και αναφορικά με την ασφάλεια και την προστασία των προσωπικών δεδομένων που επεξεργάζεται η εταιρία. Επικαλείται, ακόμα, την ανάγκη άμεσης και γρήγορης εξυπηρέτησης των συνδρομητών, προβάλλοντας ότι η φραγή της νέας κάρτας συνεπάγεται διακοπή των παρεχόμενων υπηρεσιών και δεν θα μπορούσε να εφαρμοστεί παρά μόνο κατασταλτικά και μάλιστα μετά την εμφάνιση επαρκούς όγκου περιστατικών και όχι προληπτικά, καθώς ζητούμενο είναι η στάθμιση της ασφάλειας με την ταχύτητα και την ποιότητα εξυπηρέτησης. Εξάλλου, διατείνεται ότι παρόμοια περιστατικά δεν είχαν εκδηλωθεί προγενέστερα και αυτό αποδεικνύει την επάρκεια των υφιστάμενων μέτρων, μέχρι τότε. Εντούτοις, υποστηρίζεται ότι το μέτρο των φραγών είχε προαποφασιστεί, αλλά εξαιτίας σύνθετης τεχνικής υλοποίησης καθυστέρησε να υλοποιηθεί.

Η εταιρία υποστηρίζει, εξάλλου, ότι καθώς μεγάλο μέρος των απατών διενεργείται με την προσκόμιση πλαστών δικαιολογητικών, οι υπάλληλοί της δεν έχουν την αρμοδιότητα να κρίνουν περί της πλαστότητας, η οποία ανήκει στις δικαστικές αρχές. Επικαλείται, τέλος και την δήλωση της ΑΔΑΕ περί αναρμοδιότητάς της σχετικά με τέτοιου είδους ελέγχους. Δήλωσε, τέλος, η εταιρία, ότι από τον Οκτώβριο του 2020, δεν έχει εκδηλωθεί κανένα άλλο παρόμοιο περιστατικό.

Εν κατακλείδι, η εταιρία επικαλείται την αρχή της αναλογικότητας και της επιείκειας αναφορικά με τις κυρώσεις που επιβάλλονται και από την ΑΔΑΕ, προβάλλει τον ισχυρισμό ότι έχει γνωστοποιήσει όλα τα περιστατικά ως όφειλε, ότι δεν υπήρχε δόλος, ότι έλαβε μέτρα, αλλά και την συγκυρία τέλεσης των εν λόγων απατών εν μέσω μέτρων κατά της πανδημίας.

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 καταδικάσθηκε 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, ΣτΕ 4309/2015). Εν προκειμένω, όπως προκύπτει από το υπόμνημα της καταγγελλόμενης εταιρίας, από την ΑΔΑΕ επιβληθεί σε βάρος της κυρώσεις μόνο σε δύο περιπτώσεις (Δ, Ε), 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 θιγομένους 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» (una 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 ιδίου 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 παράνομή καταστροφή, τυχαία απώλεια ή αλλοίωση και από μη εξουσιοδοτημένη ή παράνομή επεξεργασία, συμπεριλαμβανομένης της αποθήκευσης, πρόσβασης ή αποκάλυψης και γ) διασφαλίζεται η εφαρμογή πολιτικής ασφάλειας 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 άτοκο. 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 εφαρμόσθηκαν 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 τρείς κατηγορίες περιστατικών, εν σχέση με τις πολιτικές που βρίσκονταν σε εφαρμογή:

    1. Δεν εφαρμόστηκε η τρέχουσα πολιτική και τα μέτρα που σχετίζονται με την διαδικασία αντικατάστασης της κάρτας SIM. Συγκεκριμένα, έχουν καταγραφεί εννέα (9) περιστατικά για την 1η περίοδο, επτά (7) περιστατικά για την 2η περίοδο και δύο (2) περιστατικά για την 3η περίοδο.

    2. Τα μέτρα που εφαρμόζονταν σχετικά με τον έλεγχο ταυτοποίησης των πελατών κατά την 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 εννέα (9) περιστατικά για την 1η περίοδο, επτά (7) περιστατικά για την 2η περίοδο και δύο (2) περιστατικά για την 3η περίοδο.

    3. Τα μέτρα που εφαρμόζονταν σχετικά με τον έλεγχο ταυτοποίησης των πελατών κατά την διαδικασία εξυπηρέτησης άλλων αιτήσεων υπηρεσιών (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 ένα (1) περιστατικό για την 1η περίοδο, ένα (1) περιστατικό για την 2η περίοδο και τρία (3) περιστατικά για την 3η περίοδο.

    Λαμβάνοντας υπόψη την προαναφερθείσα κατηγοριοποίηση των περιστατικών διαπιστώνονται τα ακόλουθα:

    I. Από την ανάλυση των περιστατικών που ανήκουν στις τρεις κατηγορίες (Α, Β και Γ) προκύπτει ότι τα μέτρα ασφάλειας που εφαρμόζονταν στις αντίστοιχες 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.

Επίσης 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 η ύπαρξη περιστατικών που εκμεταλλεύτηκαν αδυναμίες 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 αξιολόγηση των περιστατικών που ανήκουν στην πρώτη (Α) κατηγορία διαπιστώνεται ότι υπήρχαν περιπτώσεις όπου οι πολιτικές που είχαν οριστεί τις αντίστοιχες περιόδους δεν εφαρμόστηκαν (άρθρο 12, παρ.3, εδ.γ του ν. 3471/06).

Από τις ανωτέρω διαπιστώσεις προκύπτουν δύο (2) κατηγορίες παραβιάσεων. Συγκεκριμένα:

1. Από την πρώτη και δεύτερη διαπίστωση (I, II ανωτέρω) προκύπτει ότι η εταιρία εφάρμοζε σε διάφορες χρονικές περιόδους πολιτικές οι οποίες ήταν ελλιπείς (άρθρο 12 παρ. 1, ν. 3471/2006).

2. Από την τρίτη διαπίστωση (III ανωτέρω) προκύπτει ότι υπήρχαν περιπτώσεις που οι ισχύουσες πολιτικές δεν εφαρμόζονταν (άρθρο 12 παρ. 3 εδ. γ, ν. 3471/2006).

Επίσης, παρατηρήθηκαν περιπτώσεις (τουλάχιστον οκτώ) όπου 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 έναν έως τρεις μήνες).

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**