ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 29-05-2019

Αριθ. Πρωτ.: Γ/ΕΞ/3834/29-05-2019

Α Π Ο Φ Α Σ Η 14/2019

(Τμήμα)

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνεδρίασε σε σύνθεση Τμήματος στην έδρα της την 06-02-2019 και ώρα 10:00 μετά από πρόσκληση του Προέδρου της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν ο Αναπληρωτής Πρόεδρος, Γ. Μπατζαλέξης, κωλυομένου του Προέδρου της Αρχής, Κ. Μενουδάκου, και τα αναπληρωματικά μέλη της Αρχής Ε. Παπακωνσταντίνου και Π. Ροντογιάννης, ως εισηγητής, σε αντικατάσταση των τακτικών μελών Κ. Λαμπρινουδάκη και Αντ. Συμβώνη αντίστοιχα, οι οποίοι, αν και εκλήθησαν νομίμως εγγράφως, δεν παρέστησαν λόγω κωλύματος. Το τακτικό μέλος της Αρχής Χ. Ανθόπουλος και το αναπληρωματικό του μέλος Γρ. Τσόλιας, αν και εκλήθησαν νομίμως εγγράφως, δεν παρέστησαν λόγω κωλύματος. Παρούσες χωρίς δικαίωμα ψήφου ήταν η Γ. Παναγοπούλου, ειδική επιστήμονας ελέγκτρια, ως βοηθός εισηγητή, η οποία αποχώρησε μετά τη συζήτηση της υπόθεσης και πριν από τη διάσκεψη και τη λήψη απόφασης και η Ε. Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Η Αρχή έλαβε τη με αρ. πρωτ. Γ/ΕΙΣ/8105/12-10-2018 γνωστοποίηση περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα από τη «Βιοϊατρική Διαγνωστικό Κέντρο Α.Ε» (εφεξής «υπεύθυνος επεξεργασίας») που περιγράφει την εκ παραδρομής αποστολή αποτελεσμάτων ιατρικών εξετάσεων εξεταζόμενου σε

τρίτο πρόσωπο. Το κανάλι αποστολής δεν προσδιορίστηκε με σαφήνεια, ενδέχεται η αποστολή να πραγματοποιήθηκε μέσω μηνύματος ηλεκτρονικού ταχυδρομείου ή μέσω τηλεομοιοτυπίας (φαξ).

Σχετικά η Αρχή έχει εκδώσει παλαιότερα την απόφαση 164/2014 με την οποία είχε απευθύνει αυστηρή προειδοποίηση στον υπεύθυνο επεξεργασίας για τήρηση των επιταγών του άρθρου 10 του ν. 2472/1997 για το απόρρητο και την ασφάλεια της επεξεργασίας, κατόπιν καταγγελίας ότι αποτελέσματα εξετάσεων αίματος ενδέχεται να εστάλησαν μέσω ηλεκτρονικού ταχυδρομείο σε τρίτο πρόσωπο.

Στη συνέχεια, η Αρχή με τη με αρ. πρωτ. Γ/ΕΞ/8686/02-11-2018 κλήση κάλεσε τον υπεύθυνο επεξεργασίας να παραστεί στη συνεδρίαση του Τμήματος της Αρχής την 21-11-2018, προκειμένου να συζητηθεί το ανωτέρω ζήτημα.

Κατά την ακρόαση της 21-11-2018 παρέστησαν εκ μέρους του υπευθύνου επεξεργασίας οι Α, Οικονομικός Διευθυντής και Β Σύμβουλος Πληροφορικής, ενώ από τη Δικηγορική εταιρεία Νίκος Κανελλόπουλος – Χ. Ζέρβα και Συνεργάτες, η οποία έχει ορισθεί ως υπεύθυνος προστασίας δεδομένων του υπευθύνου επεξεργασίας, παραστάθηκαν οι Χαρά Ζέρβα και Ήρα Χιόνη. Αφού αναπτύχθηκαν προφορικά οι απόψεις των παρισταμένων, στη συνέχεια υπεβλήθη εκ μέρους του υπευθύνου επεξεργασίας το με αρ. πρωτ. Γ/ΕΙΣ/9631/31-10-2018 υπόμνημα.

Στο υπόμνημα αναφέρεται ότι το συγκεκριμένο περιστατικό αφορά μεμονωμένη περίπτωση ανθρωπίνου λάθους, με ασήμαντες συνέπειες, αφού έγινε αποστολή μέσω φαξ αποτελέσματος εξετάσεων σε λάθος παραλήπτη που είχε το ίδιο ονοματεπώνυμο. Περιγράφονται επίσης στο σύνολό τους οι διαδικασίες που εφαρμόζονται για την αποστολή των αποτελεσμάτων ιατρικών εξετάσεων μέσω ηλεκτρονικού ταχυδρομείου, λαμβάνοντας υπόψη τις συστάσεις που απηύθυνε η Αρχή με την απόφαση 64/2014.

Η Αρχή, μετά από εξέταση των στοιχείων του φακέλου, την ακροαματική διαδικασία και αφού άκουσε τον εισηγητή και τη βοηθό εισηγητή, η οποία αποχώρησε μετά τη συζήτηση της υπόθεσης και πριν από τη διάσκεψη και τη λήψη απόφασης, μετά από διεξοδική συζήτηση

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟΝ ΝΟΜΟ

1. Ο ΓΚΠΔ, ο οποίος αντικατέστησε την Οδηγία 95/56/ΕΚ, είναι σε εφαρμογή

από τις 25 Μαΐου 2018. Το άρθρο 4 του ΓΚΔΠ 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*».

2. Οι αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα ορίζονται στο άρθρο 5 παρ. 1 του ΓΚΔΠ – μεταξύ αυτών, όπως επισημαίνεται στο άρθρο 5 παρ. 1 στοιχ. στ' αυτού, τα δεδομένα προσωπικού χαρακτήρα 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»).

3. Σύμφωνα με το άρθρο 32 του ΓΚΠΔ, «*λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά*

περίπτωση: (…) *δ) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας*». Εξάλλου, στην παράγραφο 2 αυτού, αναφέρεται ότι «*κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας λαμβάνονται ιδίως υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία».*

4. Αναφορικά με τη περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα, ο ΓΚΠΔ ορίζει συγκεκριμένες υποχρεώσεις για τους υπευθύνους επεξεργασίας. Συγκεκριμένα, στο άρθρο 33 αυτού, ορίζεται ότι σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην αρμόδια[1] εποπτική αρχή, 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.

Στην παράγραφο 3 του άρθρου 33 ορίζεται ότι η γνωστοποίηση αυτή κατ' ελάχιστο: α) περιγράφει τη φύση της παραβίασης δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων, όπου είναι δυνατό, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων των δεδομένων, καθώς και των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων δεδομένων προσωπικού χαρακτήρα, β) ανακοινώνει το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες, γ) περιγράφει τις ενδεχόμενες συνέπειες της παραβίασης των δεδομένων προσωπικού χαρακτήρα, δ) περιγράφει τα ληφθέντα ή τα προτεινόμενα προς λήψη μέτρα από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της. Σε περίπτωση που και εφόσον δεν είναι δυνατόν να παρασχεθούν οι πληροφορίες ταυτόχρονα, μπορούν να παρέχονται σταδιακά χωρίς

[1] Λαμβάνοντας υπόψη το άρθρο 55 του ΓΚΔΠ περί των αρμοδιοτήτων των εποπτικών αρχών, αρμόδια για το εν λόγω περιστατικό είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

αδικαιολόγητη καθυστέρηση.

Σύμφωνα με το άρθρο 34 του ΓΚΔΠ, 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. Σε αυτήν την ανακοίνωση περιγράφεται με σαφήνεια η φύση της παραβίασης των δεδομένων προσωπικού χαρακτήρα και περιέχονται τουλάχιστον οι πληροφορίες και τα μέτρα που αναφέρονται στο άρθρο 33 παράγραφος 3 στοιχεία β), γ) και δ) (πβλ. ανωτέρω). Η ανακοίνωση στο υποκείμενο των δεδομένων δεν απαιτείται, εάν πληρείται οποιαδήποτε από τις ακόλουθες προϋποθέσεις: α) ο υπεύθυνος επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, και τα μέτρα αυτά εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση δεδομένα προσωπικού χαρακτήρα, κυρίως μέτρα που καθιστούν μη κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, όπως η κρυπτογράφηση, β) ο υπεύθυνος επεξεργασίας έλαβε στη συνέχεια μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, γ) προϋποθέτει δυσανάλογες προσπάθειες (οπότε και, στην περίπτωση αυτή, γίνεται αντ' αυτής δημόσια ανακοίνωση ή υπάρχει παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο).

5. Στην προκειμένη περίπτωση από τα στοιχεία του φακέλου της υπόθεσης προκύπτει ότι ο υπεύθυνος επεξεργασίας συμμορφώθηκε με τις υποχρεώσεις των υπευθύνων επεξεργασίας οι οποίες απορρέουν από τα προαναφερθέντα άρθρα 33 και 34 του ΓΚΠΔ αναφορικά με τη διαχείριση περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα, δεδομένου ότι:

α) υπέβαλε τη σχετική γνωστοποίηση στην Αρχή, εντός εβδομήντα δύο (72) ωρών από τη στιγμή που έλαβε γνώση του περιστατικού,

β) η γνωστοποίηση συνολικά, όπως αυτή συμπληρώθηκε, παρέχει όλες τις πληροφορίες που απαιτούνται βάσει του άρ. 33 του ΓΚΔΠ,

γ) προέβη αμέσως σε αξιολόγηση των κινδύνων για το επηρεαζόμενο υποκείμενο των δεδομένων λόγω του περιστατικού και πραγματοποίησε ενημέρωση αυτού, σύμφωνα με τα όσα προβλέπονται σχετικώς στο άρ. 34 του ΓΚΠΔ.

7. Ενόψει των ανωτέρω δεν φαίνεται να υπάρχει κάποιο ζήτημα σε σχέση με τη

διαχείριση του συγκεκριμένου μεμονωμένου περιστατικού όπως επίσης και με την προσαρμογή του υπευθύνου στις συστάσεις της απόφασης 64/2014.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή κρίνει ότι για την περίπτωση που εξετάστηκε δεν απαιτείται να ασκήσει κάποια από τις προβλεπόμενες στο άρθρο 58 παρ. 2 του ΓΚΠΔ διορθωτικές εξουσίες της.

Ο Αναπληρωτής Πρόεδρος	**Η Γραμματέας**
Γεώργιος Μπατζαλέξης	**Ειρήνη Παπαγεωργοπούλου**