ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Αθήνα, 7 Ιουλίου 2026

Αριθμ. Πρωτ: Γ/ΕΞΕ/3051

ΑΠΟΦΑΣΗ 13/2026

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνεδρίασε σε σύνθεση Τμήματος μέσω τηλεδιασκέψεως την 11/03/2026 μετά από πρόσκληση του εκτελούντος χρέη Προέδρου Αναπληρωτή Προέδρου της, Γεωργίου Μπατζαλέξη, παραιτηθέντος του προέδρου της Κων/νου Μενουδάκου, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν ο Γεώργιος Μπατζαλέξης, Αναπληρωτής Πρόεδρος, το αναπληρωματικό μέλος Μαρία Ψάλλα, σε αναπλήρωση του τακτικού μέλους, Γρηγορίου Τσόλια, ο οποίος απουσίασε λόγω κωλύματος, αν και είχε προσκληθεί νομίμως εγγράφως, και το αναπληρωματικό μέλος, Δημοσθένης Βουγιούκας, ως εισηγητής, κατ' άρθρα 3 περ. β' και 8 παρ. 2 του Κανονισμού Λειτουργίας της Αρχής. Στη συνεδρίαση παρέστησαν επίσης, με εντολή του Αναπληρωτή Προέδρου, η Φωτεινή Καρβέλα, νομική ελέγκτρια – δικηγόρος και ο Λεωνίδας Ρούσσος, πληροφορικός ελεγκτής, ως βοηθοί εισηγητή και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών υποθέσεων της Αρχής, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Υποβλήθηκε στην Αρχή η με αριθμ. πρωτ. Γ/ΕΙΣ/6821/02-09-2024 γνωστοποίηση περιστατικού παραβίασης δεδομένων από το Γενικό Νοσοκομείο Θεσσαλονίκης Γ. Γεννηματάς «Ο Άγιος Δημήτριος» (εφεξής «Υπεύθυνος Επεξεργασίας») , με αντικείμενο την εκ παραδρομής ανάρτηση των αριθμών τηλεφώνου, των παθήσεων και των προγραμματισμένων επεμβάσεων των υποκειμένων της λίστας χειρουργείου από τις 03/05/2024 έως τουλάχιστον και τις 29/8/2024 στην ιστοσελίδα του Νοσοκομείου και στο διαδίκτυο.

Επίσης, υποβλήθηκε στην Αρχή η με αριθμ. πρωτ. Γ/ΕΙΣ/7588/02-10-2024 αναφορά πολίτη

σχετικά με το εν λόγω περιστατικό παραβίασης. Συγκεκριμένα, σύμφωνα με την ως άνω αναφορά, κατά την αναζήτηση συγκεκριμένου, αγνώστου στον ίδιο, αριθμού κινητού τηλεφώνου, το οποίο τον καλούσε, στην μηχανή αναζήτησης Google στις 29/08/2024, εμφανίστηκε ως αποτέλεσμα ένα έγγραφο κειμένου (της μορφής .pdf) που περιεχόταν στην ιστοσελίδα του ανωτέρω Νοσοκομείου (που προφανώς περιελάμβανε και το προς αναζήτηση κινητό), στο οποίο αναφέρονταν τηλέφωνα επικοινωνίας ασθενών (σταθερά και κινητά), παθήσεις καθώς και προγραμματισμένες επεμβάσεις τους. Ο πολίτης παραθέτει την διεύθυνση URL στην οποία ήταν προσβάσιμο το εν λόγω αρχείο[1].

Όπως αναφέρει, την ίδια ημέρα ενημέρωσε το Νοσοκομείο μέσω μηνύματος ηλεκτρονικού ταχυδρομείου, το οποίο και επισυνάπτει στην καταγγελία, έχοντας προηγουμένως αντιμετωπίσει αρκετή δυσκολία εντοπισμού ηλεκτρονικών διευθύνσεων, καθώς άλλες διευθύνσεις ηλεκτρονικού ταχυδρομείου εμφανίζονταν στην σελίδα επικοινωνίας του Νοσοκομείου 'https://www.oagiosdimitrios.gr/epikoinonia-general/stoicheiaepikoinonias/' και άλλες στους συνδέσμους των διευθύνσεων, ενώ ορισμένοι σύνδεσμοι δεν λειτουργούσαν. Επίσης, όπως ανέφερε, δεν υπήρχε κάποια αναφορά στα στοιχεία του Υπεύθυνου Προστασίας Δεδομένων (εφεξής ΥΠΔ) του Νοσοκομείου στην ιστοσελίδα του Νοσοκομείου.

Όπως αναφέρει ο πολίτης, το συγκεκριμένο αρχείο αποσύρθηκε από την σελίδα του Νοσοκομείου λίγες ώρες αργότερα, ενώ βρισκόταν αναρτημένο από τον Μάιο του 2024, ωστόσο μέχρι την ημέρα της αναφοράς δεν είχε λάβει ενημέρωση από το Νοσοκομείο για τις ενέργειες στις οποίες αυτό προέβη σε συνέχεια της εν λόγω αναφοράς, παρόλο που το προέτρεψε να το πράξει. Συγκεκριμένα, όπως αναφέρει ο πολίτης, το Νοσοκομείο δεν είχε ενημερώσει τους ασθενείς που περιέχονταν στο εν λόγω αρχείο, σύμφωνα με πληροφόρηση που είχε από υποκείμενο των δεδομένων που περιλαμβανόταν στη λίστα, ούτε ατομικά, αλλά ούτε και με κάποια ανάρτηση σε κάποιο ηλεκτρονικό μέσο.

Όπως αναφέρει, στο εν λόγω αρχείο περιέχονταν στοιχεία όπως είδος πάθησης και προγραμματισμένης επέμβασης, καθώς και αριθμοί κινητών και σταθερών τηλεφώνων ασθενών και σε κάποιες περιπτώσεις συνοδών, ενώ δεν περιέχονταν ονοματεπώνυμα ασθενών. Ωστόσο, όπως αναφέρει ο πολίτης, είναι εύκολη η ταύτιση αριθμών με

[1] …

συνδρομητή, στις περιπτώσεις που περιέχονται σε καταλόγους τηλεπικοινωνιακών παρόχων ή οι ασθενείς έχουν από μόνοι τους δημοσιοποιήσει το τηλέφωνο τους για οποιαδήποτε χρήση, ενώ πραγματοποιήθηκε και δοκιμαστική αναζήτηση στο διαδίκτυο από τον ίδιο, κατά την οποία προέκυψαν τα πλήρη στοιχεία ασθενών.

Στο αρχείο αναφέρονται ημερομηνίες προγραμματισμένου χειρουργείου. Το αρχείο περιλαμβάνει 235 σελίδες, με 12 περίπου ασθενείς ανά σελίδα, δηλαδή περιέχει συνολικά στοιχεία για: 235 x 12 = 2820 ασθενείς. Το αρχείο περιλαμβανόταν στην ευρετηρίαση (indexing) της ιστοσελίδας από την Google από την στιγμή της ανάρτησής του και για αρκετούς μήνες, τουλάχιστον έως και την ημερομηνία της αναφοράς και κάθε αναζήτηση στοιχείου που περιεχόταν σε αυτήν επέστρεφε το συνολικό αρχείο. Όπως αναφέρει και ο πολίτης, ενδεχομένως να είχε αναρτηθεί από κάποιον υπάλληλο, για το διαμοιρασμό του πίνακα των προγραμματισμένων χειρουργείων σε προσωπικό του Νοσοκομείου, αλλά εκ των πραγμάτων ήταν προσβάσιμο και σε κάθε τρίτο στο διαδίκτυο.

Στην καταγγελία του αναφέρει επίσης, ότι, επειδή πρόκειται για δεδομένα υγείας, που δυνητικά θα μπορούσαν να χρησιμοποιηθούν από τρίτους (πχ ασφαλιστικές εταιρείες για άρνηση ασφάλισης, ιδιωτικές κλινικές για προώθηση επεμβάσεων σε συντομότερο χρόνο, σε σχέση με τον αναφερόμενο στον πίνακα, επιτήδειους για την υπεξαίρεση χρημάτων κτλ), και επειδή το Νοσοκομείο δεν του είχε απαντήσει έως την στιγμή της αναφοράς του στην Αρχή, ο πολίτης υπέβαλε μια σειρά ερωτημάτων προς την Αρχή και την κάλεσε να ελέγξει αν έχουν γίνει από τον Υπεύθυνο Επεξεργασίας οι προβλεπόμενες από το Νόμο ενέργειες, αναφορικά με τα κάτωθι:

• την αξιολόγηση του περιστατικού ασφαλείας (αν ελέγχθηκε πόσοι απέκτησαν πρόσβαση στο αρχείο με μεταφόρτωση από την σελίδα και τι αντίκτυπο έχει η διαρροή των στοιχείων αυτών για μεγάλο αριθμό πολιτών).

• τα μέτρα πρόληψης που ελήφθησαν.

• αν ενημερώθηκε η Αρχή.

• αν ενημερώθηκαν οι θιγόμενοι.

• αν υπάρχει ΥΠΔ στον φορέα (και απλά λείπουν μέχρι και σήμερα τα στοιχεία επικοινωνίας στην ιστοσελίδα). Η Αρχή απέστειλε στον Υπεύθυνο Επεξεργασίας το με αριθμ. πρωτ. Γ/ΕΞ/3113/11-11-2024 έγγραφο της, με το οποίο τον κάλεσε να της παράσχει διευκρινίσεις

σχετικά με:

α) τους λόγους για τους οποίους προέκυψε η δημόσια ανάρτηση των στοιχείων που αναφέρονται,

β) την ανταπόκρισή του στην επικοινωνία του πολίτη που προέβη στην αναφορά,

γ) τα στοιχεία ορισμού και επικοινωνίας του ΥΠΔ,

δ) την απόφαση του Υπεύθυνου Επεξεργασίας για ενημέρωση ή μη των υποκειμένων των δεδομένων τα οποία αφορά η παραβίαση (άρθρο 34 του ΓΚΠΔ) και σε θετική απάντηση τον τρόπο και το περιεχόμενο ενημέρωσης των υποκειμένων των δεδομένων,

ε) την γνωστοποίηση του περιστατικού στην Αρχή (άρθρο 34 του ΓΚΠΔ).

Ο Υπεύθυνος Επεξεργασίας απάντησε με το με αρ. πρωτ. Γ/ΕΙΣ/8933/19-11-2024 έγγραφο στα ανωτέρω ερωτήματα και συγκεκριμένα ότι:

α) Η ανάρτηση ήταν προϊόν ανθρωπίνου λάθους. Παρά την εφαρμογή διαδικασίας κωδικοποίησης (ψευδωνυμοποίησης) των προσωπικών δεδομένων, εντοπίστηκε σφάλμα κατά την διαγραφή των τηλεφωνικών αριθμών πριν από την ανάρτηση της λίστας, η οποία ήταν αναρτημένη την χρονική περίοδο από 03-05-2024 έως 10-05-2024.

β) Η Διοίκηση του Νοσοκομείου προέβη σε διερεύνηση του περιστατικού, προκειμένου να εντοπιστούν τα αίτια του σφάλματος και να υιοθετηθούν πρόσθετα μέτρα ασφάλειας. Εξετάστηκε, ειδικότερα, η δυνατότητα αυτοματοποίησης της διαδικασίας ανωνυμοποίησης των στοιχείων λίστας χειρουργείων μέσω του υφιστάμενου πληροφοριακού συστήματος, προς αποκλεισμό της πιθανότητας ανθρωπίνου λάθους. Με την ολοκλήρωση της εν λόγω διαδικασίας, το Νοσοκομείο θα προβεί στην ενημέρωση του πολίτη για την εν λόγω καταγγελία.

γ) Το Νοσοκομείο δήλωσε ότι τα στοιχεία επικοινωνίας του ΥΠΔ του βρίσκονταν αναρτημένα σε συγκεκριμένη διεύθυνση που παρέπεμπε στα εξωτερικά ιατρεία του, ενώ υπάρχει η δυνατότητα επικοινωνίας μαζί του μέσω κατάλληλης διεύθυνσης ηλεκτρονικής αλληλογραφίας του νοσοκομείου.

δ) Το Νοσοκομείο προέβη σε γνωστοποίηση του περιστατικού παραβίασης, ενώ κατόπιν εκτίμησης κινδύνου, κρίθηκε ότι το περιστατικό δεν ενείχε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και, συνεπώς, δεν κρίθηκε απαραίτητη η

ενημέρωση των υποκειμένων.

Εν συνεχεία, η Αρχή απέστειλε το με αρ. πρωτ. Γ/ΕΞΕ/788/06-03-2025 έγγραφο στον Υπεύθυνο Επεξεργασίας, με το οποίο τον κάλεσε:

α) να τεκμηριώσει τον ακριβή χρόνο λήξης του περιστατικού, δεδομένου ότι στην υπ' αριθμ. πρωτ. Γ/ΕΙΣ/6821/02-09-2024 γνωστοποίηση περιστατικού παραβίασης δεδομένων δηλώνει ως χρόνο λήξης του περιστατικού την «10/5/2024 15:00μμ», ενώ τα εν λόγω δεδομένα βρίσκονταν αναρτημένα τουλάχιστον έως και τις 29/8/2024, οπότε και υποβλήθηκε η υπ' αριθμ. πρωτ. Γ/ΕΙΣ/7588/02-10-2024 αναφορά.

β) να προσδιορίσει τον αριθμό των προσβάσεων (μεταφορτώσεων) των συγκεκριμένων δεδομένων που βρίσκονταν διαθέσιμα στην ιστοσελίδα του από μοναδικές διαδικτυακές διευθύνσεις (IP addresses).

γ) να επικαιροποιήσει τα στοιχεία του ΥΠΔ που έχει γνωστοποιήσει στην Αρχή, διότι διαφέρουν από αυτά που ανέφερε στις υπ' αριθμ. πρωτ. Γ/ΕΙΣ/8933/19-11-2024 διευκρινίσεις του.

δ) να διευκρινίσει εάν και με ποιο τρόπο ήταν διαθέσιμα τα στοιχεία επικοινωνίας του ΥΠΔ στην ιστοσελίδα του κατά το χρόνο αναφοράς του πολίτη και πότε έγινε η συμπερίληψή τους στην πρώτη σελίδα της ιστοσελίδας του.

ε) να προσκομίσει την απάντησή του στο φυσικό πρόσωπο που του ανέφερε την εν λόγω διαρροή.

στ) να περιγράψει τον τρόπο επεξεργασίας των λιστών χειρουργείων (σύστημα που χρησιμοποιείται, ψευδωνυμοποίηση, ανάρτηση, μέτρα ασφάλειας), υποβάλλοντας τη σχετική τεκμηρίωση.

Ο Υπεύθυνος Επεξεργασίας απάντησε με το με αρ. πρωτ. Γ/ΕΙΣ/2166/14-03-2025 έγγραφο στα ανωτέρω ερωτήματα και συγκεκριμένα ότι:

α) Η πρόσβαση ήταν δυνατή μέσω σχετικού συνδέσμου στην ιστοσελίδα του Νοσοκομείου για την χρονική περίοδο από την Παρασκευή 3-5-2024 έως την Παρασκευή 10-05-2024, οπότε και ο σύνδεσμος ενημερώθηκε ώστε να παραπέμπει σε επόμενο αρχείο. Το αρχείο, όμως, ως οντότητα μορφής pdf, παρέμενε αρχειοθετημένο σε φάκελο με τα αρχεία που έχουν ανέβει έως τότε στην ιστοσελίδα, χωρίς απευθείας πρόσβαση μέσω αυτής, παρά μόνο

μέσω μηχανής αναζήτησης, με αναζήτηση συγκεκριμένων στοιχείων που περιλαμβάνονταν στο αρχείο αυτό. Η οριστική του διαγραφή έγινε μετά την ειδοποίηση του πολίτη.

β) Δεν είναι δυνατή η απάντηση μέσω στατιστικών του παρόχου υποστήριξης του χώρου φιλοξενίας της ιστοσελίδας του, καθότι έχει παρέλθει το τρίμηνο, μέχρι το οποίο διατηρούνταν σχετικά στοιχεία, μέσω του συγκεκριμένου πακέτου, ήτοι το WHFA της Nova.

γ) Η επικαιροποίηση των στοιχείων του ΥΠΔ του έγινε ενώπιον της Αρχής.

δ) Τα στοιχεία επικοινωνίας του ΥΠΔ δεν ήταν διαθέσιμα κατά τον χρόνο της αναφοράς του πολίτη, από παράλειψη κατά την αναβάθμιση της σχετικής σελίδας και των στοιχείων του ΥΠΔ. Συμπεριλήφθηκαν στην ιστοσελίδα για τα εξωτερικά ιατρεία καθώς και στην ιστοσελίδα που αναφέρεται στα γενικότερα στοιχεία επικοινωνίας του Υπεύθυνου Επεξεργασίας.

ε) Επισυνάπτεται η απάντηση προς το φυσικό πρόσωπο που τον ειδοποίησε για την διαρροή.

στ) Η διαδικασία της ανωνυμοποίησης των στοιχείων της λίστας χειρουργείου αυτοματοποιήθηκε μέσω του υφιστάμενου πληροφοριακού συστήματος προς αποκλεισμό της πιθανότητας του ανθρώπινου λάθους. Στην κατάλληλη διαδικτυακή διεύθυνση του Νοσοκομείου, στο σημείο της λίστας χειρουργείου, εμφανίζονται ανωνυμοποιημένα απευθείας από την εφαρμογή της λίστας χειρουργείων, τα στοιχεία χειρουργείου.

Κατόπιν τούτων, η Αρχή κάλεσε με την με αριθμ. πρωτ. Γ/ΕΞΕ/1786/22-05-2025 κλήση τον Υπεύθυνο Επεξεργασίας σε ακρόαση, προκειμένου να εκθέσει τις απόψεις του όσον αφορά το συγκεκριμένο περιστατικό στην από 11-06-2025 συνεδρίαση μέσω τηλεδιάσκεψης του Τμήματος της Αρχής. Στην ως άνω συνεδρίαση παρέστησαν μέσω τηλεδιάσκεψης εκ μέρους του υπευθύνου επεξεργασίας η Γεωργία Ζώη, δικηγόρος με ΑΜΔΣ…, η Α, Αναπληρώτρια Διοικήτρια του Γ.Ν.Θ.Γ. Γεννηματάς ο Άγιος Δημήτριος, οργανική μονάδα «Ο Άγιος Δημήτριος» και η Β, Προϊσταμένη Τμήματος Πληροφορικής, οι οποίες απάντησαν στις ερωτήσεις που τους ετέθησαν.

Μετά την εν λόγω ακρόαση δόθηκε στον Υπεύθυνο Επεξεργασίας προθεσμία προσκομίσεως υπομνήματος προς περαιτέρω υποστήριξη των ισχυρισμών του μέχρι την 20-06-2025.

Ακολούθως, ο Υπεύθυνος Επεξεργασίας υπέβαλε εμπροθέσμως το με αριθ. πρωτ. Γ/ΕΙΣ/5655/23-06-2025 υπόμνημά του, στο οποίο επανέλαβε τις θέσεις που είχε εκφράσει

στα ανωτέρω μνημονευόμενα διευκρινιστικά έγγραφά του, αλλά και συνόψισε τους ισχυρισμούς του κατά την απάντηση των ερωτημάτων που τέθηκαν στην ακρόαση. Αναλυτικότερα:

Ο Υπεύθυνος Επεξεργασίας αρχικά επανέλαβε ότι ενημερώθηκε για το περιστατικό από τον πολίτη ο οποίος υπέβαλε στη συνέχεια ενώπιον της Αρχής την με αριθμ. πρωτ. Γ/ΕΙΣ/7588/02-10-2024 αναφορά. Στην συνέχεια, ο Υπεύθυνος Επεξεργασίας περιέγραψε την διαδικασία της εβδομαδιαίας ανάρτησης στον ιστοχώρο του της λίστας χειρουργείων, η οποία περιελάμβανε τον αριθμό του περιστατικού, την ημερομηνία του χειρουργείου, την κατηγορία του περιστατικού, το χαρακτηρισμό του ως έκτακτου ή μη, την κλινική, την επέμβαση και το αποτέλεσμά της. Ο Υπεύθυνος Επεξεργασίας ανέφερε ότι ανέκαθεν εφαρμοζόταν διαδικασία κωδικοποίησης μέσω ψευδωνυμοποίησης των ονοματεπωνύμων των ασθενών, η οποία διενεργείτο από υπαλλήλους του γραφείου κίνησης του Νοσοκομείου, μέχρι και το τέλος του Αυγούστου του 2024.

Κατόπιν διερεύνησης του περιστατικού, διαπιστώθηκε ότι εκ παραδρομής, λόγω σφάλματος του αρμόδιου υπαλλήλου, δεν διαγράφηκαν οι τηλεφωνικοί αριθμοί από την λίστα της συγκεκριμένης εβδομάδος. Άμεσα ενημερώθηκε ο ΥΠΔ του Νοσοκομείου, ώστε να ειδοποιηθεί η Αρχή και να εκτιμηθεί ο κίνδυνος και οι συνέπειες του περιστατικού. Η συγκεκριμένη εκτίμηση, σύμφωνα με τους ισχυρισμούς του Υπευθύνου Επεξεργασίας, κατέδειξε ότι το κρίσιμο περιστατικό δεν συνεπαγόταν σημαντικό κίνδυνο για τις ελευθερίες και τα δικαιώματα των φυσικών προσώπων και συνεπώς δεν κρίθηκε απαραίτητη η ενημέρωση των υποκειμένων. Γνωστοποιήθηκε το περιστατικό στην Αρχή στις 02-09-2024, ενώ συμπεριλήφθηκε η εκτίμηση του κινδύνου στην γνωστοποίηση.

Στην συνέχεια, σύμφωνα με το υπόμνημα του Υπευθύνου Επεξεργασίας, η διαδικασία της ανάρτησης αυτοματοποιήθηκε, χωρίς να περιλαμβάνει ανθρώπινη παρέμβαση, ενώ πλέον έχει τεθεί σε παραγωγική λειτουργία η ενιαία Ψηφιακή Λίστα Χειρουργείων η οποία καταρτίζεται μέσω της πλατφόρμας της ΗΔΙΚΑ ΑΕ για λογαριασμό του Υπουργείου Υγείας και ενημερώνεται μέσω προγραμματιστικών διεπαφών (Application Programming Interfaces-APIs) από τα συστήματα των Νοσοκομείων.

Ως απάντηση στα ερωτήματα που τέθηκαν από τα μέλη του Τμήματος, ο Υπεύθυνος Επεξεργασίας παρείχε επιπλέον με το υπόμνημά του τις κάτωθι διευκρινίσεις:

Περί της μη ενημέρωσης των υποκειμένων, ανέφερε ότι αυτή δεν πραγματοποιήθηκε, διότι, κατά τον Υπεύθυνο Επεξεργασίας, δεν συνέτρεχε υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των επηρεαζόμενων φυσικών προσώπων, επειδή ο αριθμός τηλεφώνου δεν αποτελεί ευαίσθητο δεδομένο, αλλά απλό, ενώ η ταυτοποίηση των φυσικών προσώπων μόνο εμμέσως θα μπορούσε να πραγματοποιηθεί, εφόσον α) στην λίστα δεν περιλαμβάνονταν άλλα στοιχεία ταυτοποίησής τους, όπως πχ. ονοματεπώνυμα, β) η συγκεκριμένη λίστα δεν ήταν άμεσα προσβάσιμη από την σελίδα του νοσοκομείου, αλλά μόνο μέσω μηχανής αναζήτησης, γ) για να καταστεί δυνατή η ταυτοποίηση των υποκειμένων, θα έπρεπε κάποιος να κάνει αναζήτηση αυτών σε μηχανή αναζήτησης με βάση τους αριθμούς τηλεφώνου τους

Σχετικά με τα στοιχεία επικοινωνίας του ΥΠΔ, ο Υπεύθυνος Επεξεργασίας δήλωσε αυτά είναι αναρτημένα σε δύο θέσεις στον ιστότοπο του Νοσοκομείου, (στα εξωτερικά ιατρεία, και στα στοιχεία επικοινωνίας), ενώ δεν ήταν διαθέσιμα κατά τον χρόνο της αναφοράς του πολίτη, διότι σε μία από τις συνεχείς αναβαθμίσεις του λογισμικού ανάπτυξης του ιστοτόπου, τα στοιχεία του ΥΠΔ είχαν απαλειφθεί από τα στοιχεία επικοινωνίας του Νοσοκομείου.

Ο Υπεύθυνος Επεξεργασίας επίσης υποστήριξε ότι, βάσει του άρθρου 39 ν. 4619/2019, το ερευνώμενο περιστατικό αποτελεί ήσσονος βαρύτητας πράξη παραβίασης δεδομένων, με μικρή διάρκεια και σχετικά μικρό αριθμό υποκειμένων, τα οποία δεν υπέστησαν καμία ζημία, αφού η ταυτοποίησή τους απαιτούσε εξιδιασμένες ενέργειες και ήταν εξαιρετικά δυσχερής να επιτευχθεί. Το ερευνώμενο περιστατικό αποτελεί το μοναδικό περιστατικό σχετικό με το αντικείμενο της Αρχής, καθώς δεν υφίστανται σχετικές προηγούμενες παραβιάσεις του φορέα και δεν έχουν διαταχθεί εις βάρος του νοσοκομείου τα μέτρα της παρ. 2 του αρ. 58 του ΓΚΠΔ για την ίδια παράβαση. Για όλους τους ανωτέρω λόγους, ο Υπεύθυνος Επεξεργασίας ζήτησε να μην του επιβληθεί διοικητική κύρωση.

Η Αρχή, έπειτα από εξέταση των στοιχείων του φακέλου και όσων προέκυψαν από την ενώπιόν της ακροαματική διαδικασία και το υπόμνημα του υπευθύνου επεξεργασίας, αφού άκουσε τον εισηγητή και τις διευκρινίσεις από τους βοηθούς εισηγητή, οι οποίοι παρέστησαν χωρίς δικαίωμα ψήφου, κατόπιν διεξοδικής συζητήσεως,

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Από τις διατάξεις των άρθρων 51 και 55 του Κανονισμού (ΕΕ) 2016/679 για την προστασία προσωπικών δεδομένων (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 σημείο 12 του άρθρου 4 του ΓΚΠΔ, ως *«παραβίαση δεδομένων προσωπικού χαρακτήρα νοείται 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».*

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

4. Σύμφωνα με το άρθρο 4 στοιχ. 7 του ΓΚΠΔ, 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*».

5. Στο άρθρο 5 παρ. 1 του ΓΚΠΔ ορίζονται οι Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Σε αυτές περιλαμβάνεται η αρχή της ακεραιότητας και εμπιστευτικότητας (εδαφ. στ'), σύμφωνα με την οποία τα δεδομένα 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.

6. Σύμφωνα με το άρθρο 5 παρ. 2 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. Όπως προκύπτει από τη διάταξη αυτή, με τον ΓΚΠΔ υιοθετήθηκε ένα μοντέλο συμμόρφωσης με κεντρικό πυλώνα την εν λόγω αρχή της λογοδοσίας, σύμφωνα με την οποία 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.

7. Αναφορικά με την αρχή της διαφάνειας της επεξεργασίας, ο ΓΚΠΔ θέτει συγκεκριμένες υποχρεώσεις στους υπευθύνους επεξεργασίας ως προς την ενημέρωση που οφείλουν να παρέχουν στα υποκείμενα των δεδομένων. Ειδικότερα, σύμφωνα με το άρθρο 12 παρ. 1 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία που αναφέρεται πλην άλλων, στο άρθρο 13 –στο οποίο ορίζεται ότι «*όταν δεδομένα προσωπικού χαρακτήρα που αφορούν υποκείμενο των δεδομένων συλλέγονται από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας, κατά τη λήψη των δεδομένων προσωπικού χαρακτήρα, παρέχει στο υποκείμενο των δεδομένων όλες τις ακόλουθες πληροφορίες: α) την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας, β) τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, κατά περίπτωση, γ) τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία, (…)*» (βλ. παρ. 1 του άρθρου 13 του ΓΚΠΔ). Περαιτέρω, στην παράγραφο 2 του άρθρου 12 του ΓΚΠΔ προβλέπεται ότι «*ο υπεύθυνος επεξεργασίας διευκολύνει την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων (…)*». Στην υπό εξέταση περίπτωση, κατά το χρόνο επέλευσης του κρίσιμου περιστατικού παραβίασης και υποβολής της σχετικής αναφοράς, τα στοιχεία επικοινωνίας του ΥΠΔ δεν ήταν διαθέσιμα, όπως αναφέρει ο Υπεύθυνος Επεξεργασίας στο υπ’ αριθμ. πρωτ. Γ/ΕΙΣ/2166/14-03-2025 έγγραφό του και στο υπ’ αριθ. πρωτ. Γ/ΕΙΣ/5655/23-06-2025 υπόμνημά του, λόγω παράλειψης κατά την αναβάθμιση της σχετικής ιστοσελίδας. Συνεπώς, προκύπτει παραβίαση της υποχρέωσης του Υπευθύνου Επεξεργασίας να ενημερώνει τα υποκείμενα των δεδομένων, όπως επιτάσσει η αρχή της διαφάνειας.

8. Σύμφωνα με το άρθρο 32 παρ. 1 εδ. α και δ 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 της ψευδωνυμοποίησης δεδομένων προσωπικού χαρακτήρα, καθώς και διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας. Σύμφωνα με την παρ. 2 του ίδιου άρθρου, 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. Δεν απαιτείται τα μέτρα ασφάλειας να εξαλείφουν κάθε μορφή κινδύνου και η απλή επέλευση παραβίασης δεδομένων προσωπικού χαρακτήρα δεν συνιστά, αυτή καθαυτή, παράβαση του άρθρου 32 του ΓΚΠΔ. Η ανωτέρω ερμηνεία έχει επιβεβαιωθεί από το Δικαστήριο της Ευρωπαϊκής Ένωσης με την απόφασή του Agence nationale des recettes publiques de Bulgarie (14.12.2023, C-340/21, σκέψεις 29-31), με την οποία κρίθηκε ότι η αναφορά, στο άρθρο 32 παρ. 1 και 2 ΓΚΠΔ, σε «επίπεδο ασφάλειας κατάλληλο προς τον κίνδυνο» και σε «κατάλληλο επίπεδο ασφάλειας» καταδεικνύει ότι ο ΓΚΠΔ θεσπίζει καθεστώς διαχείρισης κινδύνων και δεν αποσκοπεί στην εξάλειψη των κινδύνων παραβίασης δεδομένων προσωπικού χαρακτήρα. Από τη διατύπωση των άρθρων 24 και 32 ΓΚΠΔ προκύπτει ότι οι διατάξεις αυτές επιβάλλουν στον υπεύθυνο επεξεργασίας την υποχρέωση υιοθέτησης τεχνικών και οργανωτικών μέτρων με σκοπό την αποτροπή, στο μέτρο του δυνατού, παραβιάσεων δεδομένων προσωπικού χαρακτήρα. Η καταλληλότητα των μέτρων αυτών πρέπει να αξιολογείται κατά περίπτωση, λαμβανομένων υπόψη των κριτηρίων που προβλέπονται στα ανωτέρω άρθρα, καθώς και των ειδικών αναγκών προστασίας των δεδομένων και των κινδύνων που απορρέουν από τη συγκεκριμένη επεξεργασία.

Στην υπό εξέταση περίπτωση, όπως αναφέρει ο Υπεύθυνος Επεξεργασίας στο υπ’ αριθμ.

πρωτ. Γ/ΕΙΣ/8933/19-11-2024 έγγραφό του και στο υπ' αριθ. πρωτ. Γ/ΕΙΣ/5655/23-06-2025 υπόμνημά του, η ανάρτηση της λίστας, όπως έλαβε χώρα, ήταν προϊόν ανθρωπίνου λάθους, διότι, παρά την εφαρμογή διαδικασίας κωδικοποίησης (ψευδωνυμοποίησης) των προσωπικών δεδομένων, εντοπίστηκε σφάλμα κατά την διαγραφή των τηλεφωνικών αριθμών πριν από την ανάρτηση της λίστας. Δεδομένης της φύσης των δεδομένων και του είδους της επεξεργασίας, δηλαδή των ειδικών αναγκών προστασίας στην συγκεκριμένη περίπτωση, ο υπεύθυνος επεξεργασίας όφειλε να είχε προβλέψει επιπλέον οργανωτικά και τεχνικά μέτρα, όπως, ενδεικτικά τον έλεγχο από δεύτερο πρόσωπο πριν τη δημοσίευση, την αυτοματοποίηση της διαδικασίας μέσω ειδικής εφαρμογής, την δοκιμαστική ανάρτηση σε άλλο περιβάλλον, δικλείδες, δηλαδή, προστασίας, απλές και γνωστές στην κοινότητα της κυβερνοασφάλειας. Η έλλειψη αυτή συνεπώς συνιστά παράβαση των θεμελιωδών προϋποθέσεων περί λήψης κατάλληλων οργανωτικών και τεχνικών μέτρων για την ασφάλεια της επεξεργασίας, σύμφωνα με το άρθρο 32 του ΓΚΠΔ.

9. Σύμφωνα με το άρθρο 33 παρ. 1 του ΓΚΠΔ, σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος, την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή 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.

Στην υπό εξέταση περίπτωση, η γνωστοποίηση στην Αρχή έλαβε χώρα εντός 96 ωρών από τη λήψη γνώσης του περιστατικού. Ειδικότερα, ο Υπεύθυνος Επεξεργασίας έλαβε γνώση του περιστατικού στις 29.8.2024 από την αναφορά πολίτη και γνωστοποίησε αυτό στην Αρχή στις 2.09.2024 (βλ. Γ/ΕΙΣ/6821/02.09.2024 γνωστοποίηση). Από τον ισχυρισμό του Υπευθύνου Επεξεργασίας στην ανωτέρω γνωστοποίηση ότι δεν γνωστοποίησε το περιστατικό στην Αρχή εντός της προθεσμίας των 72 ωρών που θέτει το άρθρο 33 παρ. 1 ΓΚΠΔ, διότι μεσολάβησε Σαββατοκύριακο και διότι από την αξιολόγηση/εκτίμηση του κινδύνου για τα δικαιώματα των επηρεαζόμενων φυσικών προσώπων στην οποία προέβη ο Υπεύθυνος Επεξεργασίας, αυτός συμπέρανε ότι επρόκειτο για χαμηλό κίνδυνο, προκύπτει παραβίαση του άρθρου 33 παρ. 1 και 32 του ΓΚΠΔ, αφενός διότι η μεσολάβηση Σαββατοκύριακου είναι αδιάφορη,

αφετέρου διότι η εσφαλμένη αντίληψη της φύσης της παραβίασης και του συνεπαγόμενου κινδύνου για τα δικαιώματα των επηρεαζόμενων φυσικών προσώπων καταδεικνύει έλλειψη των κατάλληλων μέτρων ασφάλειας της επεξεργασίας.

10. Σύμφωνα με το άρθρο 34 παρ. 1 του ΓΚΠΔ, 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. Στην προκειμένη περίπτωση, ο Υπεύθυνος Επεξεργασίας δεν ανακοίνωσε την παραβίαση στα επηρεαζόμενα φυσικά πρόσωπα, παρόλο που αυτή ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματά τους, λαμβανομένου υπόψη ότι αφορά προσωπικά δεδομένα τα οποία αφορούν στην υγεία τους και η παραβίαση της εμπιστευτικότητάς τους ενδέχεται να οδηγήσει σε υλική ζημία ή ηθική βλάβη για αυτά, η οποία μπορεί να συνίσταται σε εις βάρος τους διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια και βλάβη της φήμης τους.[2]

11. Σύμφωνα με το άρθρο 37 παρ. 1 του ΓΚΠΔ, «ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία ορίζουν υπεύθυνο προστασίας δεδομένων σε κάθε περίπτωση στην οποία: α) η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα (…)». Περαιτέρω, στην παρ. 7 του ιδίου άρθρου, αναφέρεται ότι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δημοσιεύουν τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων. Εξάλλου, όπως προαναφέρθηκε, τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων πρέπει να καθίστανται διαθέσιμα και στα υποκείμενα των δεδομένων. Αναφορικά με το ρόλο του υπευθύνου προστασίας δεδομένων, επισημαίνεται ότι, μεταξύ άλλων, όπως προβλέπεται στο άρθρο 38 παρ. 4 του ΓΚΠΔ, «τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν με τον υπεύθυνο προστασίας δεδομένων για κάθε ζήτημα σχετικό με την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα και με την άσκηση των δικαιωμάτων τους (…)».

Στην υπό εξέταση περίπτωση, κατά το χρόνο επέλευσης του κρίσιμου περιστατικού παραβίασης και υποβολής της σχετικής αναφοράς, τα στοιχεία επικοινωνίας του ΥΠΔ δεν ήταν διαθέσιμα, όπως αναφέρει ο Υπεύθυνος Επεξεργασίας στο υπ' αριθμ. πρωτ.

[2] Βλ. αιτ. σκ. 75 και 86 ΓΚΠΔ και Κατευθυντήριες Γραμμές 9/2022 του ΕΣΠΔ σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του ΓΚΠΔ, παρ. 102.

Γ/ΕΙΣ/2166/14-03-2025 έγγραφό του, λόγω παράλειψης κατά την αναβάθμιση της σχετικής ιστοσελίδας.

12. Κατόπιν των ανωτέρω, από τα στοιχεία του φακέλου, και από όσα προέκυψαν από την ακροαματική διαδικασία και το υποβληθέν υπόμνημα, η Αρχή διαπιστώνει τις εξής παραβάσεις εκ μέρους του Υπευθύνου Επεξεργασίας:

Α) Παράβαση του άρθρου 5 παρ. 1 στοιχ. στ' σε συνδυασμό με το άρθρο 32 παρ. 1 του ΓΚΠΔ αναφορικά με την ασφάλεια της επεξεργασίας.

Β) Παράβαση του άρθρου 33 παρ. 1 ΓΚΠΔ, αφού δεν γνωστοποιήθηκε εμπροθέσμως το περιστατικό παραβίασης στην Αρχή, ως όφειλε να πράξει ο Υπεύθυνος Επεξεργασίας.

Γ) Παράβαση του άρθρου 34 παρ. 1 ΓΚΠΔ, αφού ο Υπεύθυνος Επεξεργασίας δεν ανακοίνωσε την παραβίαση στα επηρεαζόμενα υποκείμενα των δεδομένων.

Δ) Παράβαση των άρθρων 12, 13 και 37 του ΓΚΠΔ, διότι ο Υπεύθυνος Επεξεργασίας δεν είχε αναρτημένα, ως όφειλε, τα στοιχεία επικοινωνίας του ΥΠΔ του, κατά την στιγμή του περιστατικού.

13. Με βάση τα ανωτέρω, η Αρχή κρίνει ότι συντρέχει περίπτωση άσκησης των εκ του άρθρου 58 παρ. 2 ΓΚΠΔ διορθωτικών εξουσιών της σε σχέση με τις διαπιστωθείσες παραβάσεις. Ειδικότερα, η Αρχή κρίνει ότι πρέπει, με βάση τις παραβάσεις που διαπιστώθηκαν, να επιβληθεί στον Υπεύθυνο Επεξεργασίας, κατ' εφαρμογή της διάταξης του άρθρου 58 παρ. 2 εδ. θ' ΓΚΠΔ, αποτελεσματικό, αναλογικό και αποτρεπτικό διοικητικό χρηματικό πρόστιμο, συμφώνως προς τα άρθρα 83 ΓΚΠΔ και 39 παρ. 1 και 2 του ν. 4624/2019 που αφορά στην επιβολή διοικητικών κυρώσεων στους φορείς του δημόσιου τομέα.

14. Περαιτέρω η Αρχή έλαβε υπόψη τα κριτήρια επιμέτρησης προστίμων που ορίζονται στο άρθρο 83 παρ. 2 του ΓΚΠΔ, την παράγραφο 5 του άρθρου αυτού που έχει εφαρμογή στον υπεύθυνο επεξεργασίας για την παράβαση των άρθρων 5 παρ. 1 στοιχ. στ,' 12 και 13 του ΓΚΠΔ και την παράγραφο 4 του άρθρου 83 ΓΚΠΔ, που έχει εφαρμογή για τις λοιπές παραβάσεις του Υπευθύνου Επεξεργασίας, και τις Κατευθυντήριες Γραμμές 04/2022 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων[3] για τον υπολογισμό των διοικητικών

[3] https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_en

προστίμων υπό τον ΓΚΠΔ, καθώς και τα πραγματικά δεδομένα της εξεταζόμενης υπόθεσης και ιδίως τα εξής:

I. Οι διαπιστωθείσες παραβάσεις των άρθρων 5 παρ. 1 στοιχ. στ', 12 και 13 του ΓΚΠΔ από τον Υπεύθυνο Επεξεργασίας υπάγονται, σύμφωνα με τις διατάξεις του άρθρου 83 παρ. 5 εδ. α' ΓΚΠΔ, στην ανώτερη προβλεπόμενη κατηγορία του συστήματος διαβάθμισης διοικητικών προστίμων.

II. Η παραβίαση προσωπικών δεδομένων σχετίζεται με τις κύριες δραστηριότητες του Υπευθύνου Επεξεργασίας, εφόσον αφορά στον προγραμματισμό των χειρουργικών επεμβάσεων που πραγματοποιούνται στο νοσοκομείο.

III. Ο αριθμός των επηρεαζόμενων προσώπων είναι υψηλός, καθώς ανέρχεται σε περίπου 2820 ασθενείς.

IV. Το περιστατικό είχε ως συνέπεια την αποκάλυψη προσωπικών δεδομένων που αφορούν σε δεδομένα υγείας και αποτελούν ειδική κατηγορία προσωπικών δεδομένων, των οποίων η παραβίαση μπορεί να επιφέρει σοβαρούς κινδύνους[4].

V. Η αδυναμία εφαρμογής της διαδικασίας ψευδωνυμοποίησης των δεδομένων πριν την ανάρτησή τους και η απουσία ενδεδειγμένων μέτρων όπως η έγκριση του συνόλου των προς ανάρτηση δεδομένων από εξουσιοδοτημένα στελέχη πριν την ανάρτησή τους, και ο έλεγχός τους μετά την συγκεκριμένη πράξη επεξεργασίας καταδεικνύουν πλημμέλειες στην εφαρμογή της πολιτικής ασφαλείας του Υπευθύνου Επεξεργασίας.

VI. Η παραβίαση δεν ανακοινώθηκε στα επηρεαζόμενα υποκείμενα των δεδομένων λόγω εσφαλμένης εκτίμησης του κινδύνου που προέκυψε από την παραβίαση.

VII. Δεν έχει διαπιστωθεί προηγούμενη αντίστοιχη παράβαση από τον Υπεύθυνο Επεξεργασίας.

VIII. Κατόπιν του περιστατικού, ενισχύθηκε η ασφάλεια του συστήματος του Υπευθύνου Επεξεργασίας με τη λήψη τόσο τεχνικών όσο και οργανωτικών μέτρων.

IX. Το περιστατικό γνωστοποιήθηκε με μικρή καθυστέρηση στην Αρχή.

[4] Βλ. συναφώς και τη Σκέψη 57 των Κατευθυντηρίων Γραμμών 4/2022 του ΕΣΠΔ

Η Αρχή κρίνει ότι, με βάση τις περιστάσεις που διαπιστώθηκαν και τα ανωτέρω κριτήρια, πρέπει να επιβληθούν στον Υπεύθυνο Επεξεργασίας οι αναφερόμενες στο διατακτικό κυρώσεις, οι οποίες αποτελούν αποτελεσματικό, αναλογικό και αποτρεπτικό μέτρο τόσο προς αποκατάσταση της συμμόρφωσης, όσο και για την τιμωρία της παράνομης συμπεριφοράς.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή, λαμβάνοντας υπόψη τα παραπάνω,

Α) Επιβάλλει, με βάση το άρθρο 58 παρ. 2 εδ. θ' του ΓΚΠΔ, στο Γενικό Νοσοκομείο Θεσσαλονίκης Γ. Γεννηματάς «Ο Άγιος Δημήτριος» διοικητικό πρόστιμο συνολικού ύψους 10.000 ευρώ, για την παραβίαση του άρθρου 5 παρ. 1 στοιχ. στ'. σε συνδυασμό με το άρθρο 32 παρ. 1 του Κανονισμού (ΕΕ) 2016/679.

Β) Επιβάλλει, με βάση το άρθρο 58 παρ. 2 εδ. θ' του ΓΚΠΔ, στο Γενικό Νοσοκομείο Θεσσαλονίκης Γ. Γεννηματάς «Ο Άγιος Δημήτριος» διοικητικό πρόστιμο συνολικού ύψους 2.000 ευρώ, για την παραβίαση του άρθρου 33 παρ. 1 του Κανονισμού (ΕΕ) 2016/679.

Γ) Επιβάλλει, με βάση το άρθρο 58 παρ. 2 εδ. θ' του ΓΚΠΔ, στο Γενικό Νοσοκομείο Θεσσαλονίκης Γ. Γεννηματάς «Ο Άγιος Δημήτριος» διοικητικό πρόστιμο συνολικού ύψους 10.000 ευρώ, για την παραβίαση του άρθρου 34 παρ. 1 του Κανονισμού (ΕΕ) 2016/679.

Δ) Επιβάλλει, με βάση το άρθρο 58 παρ. 2 εδ. θ' του ΓΚΠΔ, στο Γενικό Νοσοκομείο Θεσσαλονίκης Γ. Γεννηματάς «Ο Άγιος Δημήτριος» διοικητικό πρόστιμο συνολικού ύψους 3.000 ευρώ, για την παραβίαση των άρθρων 12 και 13 σε συνδυασμό με το άρθρο 37 του Κανονισμού (ΕΕ) 2016/679.

Ο εκτελών χρέη Προέδρου Αν. Πρόεδρος | **Η Γραμματέας**

Γεώργιος Μπατζαλέξης | **Ειρήνη Παπαγεωργοπούλου**