ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Αθήνα, 29-12-2021
Αριθ. Πρωτ.: 3028

ΑΠΟΦΑΣΗ 55/2021

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, συνήλθε, μετά από πρόσκληση του Προέδρου της, σε τακτική συνεδρίαση μέσω τηλεδιάσκεψης την 6-10-2021, σε συνέχεια της από 19-07-2021 έκτακτης συνεδρίασής της και εξ αναβολής της από 23-06-2021 συνεδρίασής της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Κωνσταντίνος Μενουδάκος, Πρόεδρος της Αρχής, τα τακτικά μέλη Σπυρίδων Βλαχόπουλος, Κωνσταντίνος Λαμπρινουδάκης, ως εισηγητής, και Χαράλαμπος Ανθόπουλος. Στη συνεδρίαση, χωρίς δικαίωμα ψήφου, παρέστησαν, με εντολή του Προέδρου, οι ελεγκτές Κωνσταντίνος Λιμνιώτης και Γεώργιος Ρουσόπουλος, ειδικοί επιστήμονες πληροφορικής, ως βοηθοί εισηγητή, και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του Τμήματος Διοικητικών Υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη τα παρακάτω:

Υποβλήθηκε στην Αρχή η υπ' αριθμ. πρωτ. Γ/ΕΙΣ/4545/01-07-2020 αναφορά, μέσω ηλεκτρονικού ταχυδρομείου, του Α, σύμφωνα με την οποία, κατά την προσπάθειά του να υποβάλει αίτηση στην πλατφόρμα tourism4all.gov.gr, διαπίστωσε πρόβλημα διαρροής προσωπικών δεδομένων τρίτων προσώπων. Ειδικότερα, εισάγοντας τα διαπιστευτήρια του (κωδικοί TAXISNET), εμφανίστηκαν στην οθόνη του στοιχεία αίτησης τρίτου ατόμου (που δεν έχει κάποια σχέση με τον ίδιο), τα οποία περιλάμβαναν ονοματεπώνυμο, Αριθμό Φορολογικού Μητρώου (ΑΦΜ), Αριθμό Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ), ταχυδρομική διεύθυνση, τηλέφωνο, διεύθυνση ηλεκτρονικού ταχυδρομείου (email), ενώ υπήρχαν και πεδία με τυχόν στοιχεία αναπηρίας και αν χρήζει φροντίδας τόσο για αιτούντα όσο και για τη σύζυγο. Προς απόδειξη επισυνάφθηκε στιγμιότυπο οθόνης (screenshot). Το εν

Λεωφ. Κηφισίας 1-3, 11523 Αθήνα
T: 210 6475 600 • E: contact@dpa.gr • www.dpa.gr

λόγω μήνυμα ηλεκτρονικού ταχυδρομείου απεστάλη στις … επίσης προς την ηλεκτρονική διεύθυνση tourism4all@mintour.gr η οποία αναγραφόταν στην εν λόγω πλατφόρμα.

Η Αρχή, διαπιστώνοντας ότι στην πολιτική προστασίας προσωπικών δεδομένων της πλατφόρμας αναφέρεται ότι *«…μπορείτε να απευθύνετε όλες τις ερωτήσεις ή τα αιτήματα σας σχετικά με την προστασία των Προσωπικών σας Δεδομένων που τηρούνται από το Υπουργείο Τουρισμού υπό την ιδιότητα του ως Υπεύθυνου Επεξεργασίας κατά τα ανωτέρω, στον Υπεύθυνο Προστασίας Δεδομένων του Υπουργείου Τουρισμού αποστέλλοντας e-mail: dpo@mintour.gov.gr...»* και καθώς δεν είχε υποβληθεί γνωστοποίηση περιστατικού παραβίασης, απέστειλε στις … μήνυμα ηλεκτρονικού ταχυδρομείου προς την εν λόγω διεύθυνση, το οποίο όμως μετά δύο ημέρες, επεστράφη ως ανεπίδοτο. Περαιτέρω, κατόπιν αναζήτησης στο μητρώο Υπευθύνων Προστασίας Δεδομένων που τηρεί η Αρχή, δεν βρέθηκε κατά την επίμαχη χρονική περίοδο ανακοίνωση στοιχείων επικοινωνίας του Υπεύθυνου Προστασίας Δεδομένων από το ως άνω Υπουργείο, ως όφειλε σύμφωνα με το άρθρο 37 παρ. 1 και 7 του Γενικού Κανονισμού Προστασίας Δεδομένων (Κανονισμός (ΕΕ) 2016/679 - εφεξής, ΓΚΠΔ) .

Ακολούθως, η Αρχή απέστειλε το υπ’ αριθμ. πρωτ. Γ/ΕΞ/4914/15-07-2020 έγγραφο στο Υπουργείο Τουρισμού, ενημερώνοντας για όλα τα ανωτέρω και ζητώντας τις απόψεις του επί των όσων περιγράφονται στην αναφορά του Α, ζητώντας ειδικότερα διευκρινίσεις ως προς τα εξής ζητήματα:

1) Σε ποιες ακριβώς ενέργειες προέβη, όταν έλαβε γνώση του εν λόγω περιστατικού, καθώς επίσης και εάν οι εν λόγω ενέργειες έχουν προβλεφθεί στο πλαίσιο κάποιας γενικότερης πολιτικής χειρισμού περιστατικών παραβίασης προσωπικών δεδομένων,

2) Πώς αξιολόγησε το εν λόγω περιστατικό βάσει των κινδύνων που μπορούν να επέλθουν εξ αυτού στα θιγόμενα πρόσωπα,

3) Αν έχει γίνει ορισμός Υπευθύνου Προστασίας Δεδομένων και αν η αναφερόμενη στην ιστοσελίδα διεύθυνση επικοινωνίας και άσκησης δικαιωμάτων (dpo@mintour.gov.gr) είναι λειτουργική.

Ακολούθως, λόγω μη λήψης έγγραφης απάντησης από το Υπουργείο μετά την πάροδο μηνών, η Αρχή απέστειλε σχετική υπόμνηση με το υπ' αριθμ. πρωτ. Γ/ΕΞΕ/534/01-02-2021 έγγραφο. Κατόπιν τούτου, το Υπουργείο απάντησε στην Αρχή με το υπ' αριθμ. πρωτ. … έγγραφο (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/1080/12-02-2021), στο οποίο αναφέρει τα εξής:

Α) Η υλοποίηση της ψηφιακής εφαρμογής για το πρόγραμμα «Τουρισμός για Όλους» αναπτύχθηκε σε συνεργασία με το Υπουργείο Ψηφιακής Διακυβέρνησης, το οποίο, μέσω του Κέντρου Διαλειτουργικότητας της Γενικής Γραμματείας Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης (εφεξής, ΓΓΠΣΔΔ), καθοδήγησε τη συνεργαζόμενη με το Υπουργείο Ψηφιακής Διακυβέρνησης ανάδοχη εταιρεία THREENITAS Α.Ε. για θέματα σχεδιασμού και ανάπτυξης διαλειτουργικότητας. Λόγω αυτού, η Δ/νση Στρατηγικού Σχεδιασμού του Υπουργείου που έχει αναλάβει την υλοποίηση του προγράμματος «Τουρισμός για Όλους» έτους 2020, προέβη σε άμεση ενημέρωση του Υπουργείου Ψηφιακής Διακυβέρνησης και της εποπτευόμενης από αυτό ΓΓΠΣΔΔ. Αναλυτικότερα, το ως άνω ηλεκτρονικό μήνυμα του Α (ημερομηνίας … και ώρας …) προς την ηλεκτρονική διεύθυνση tourism4all@mintour.gr προωθήθηκε αμέσως (στις …), με την επισήμανση του υπερεπείγοντος και με υψηλή σπουδαιότητα, στις αρμόδιες εμπλεκόμενες υπηρεσίες, ήτοι στην Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης, στο Υπουργείο Ψηφιακής Διακυβέρνησης, στην ανάδοχο εταιρεία του Υπουργείου Ψηφιακής Διακυβέρνησης, Threenitas Α.Ε. και εσωτερικά στην Γενική Διεύθυνση Τουριστικής Πολιτικής και στο Γραφείο Υπουργού.

Β) Οι εμπλεκόμενες υπηρεσίες προχώρησαν σε άμεσες τεχνικές διερευνητικές ενέργειες προκειμένου να εντοπιστεί το λάθος στη διαδικασία. Εν τω μεταξύ, με παρέμβαση του Γραφείου Υπουργού Τουρισμού και έως ότου δοθούν οι απαραίτητες εξηγήσεις, διεκόπη προληπτικά η λειτουργία της εφαρμογής την … και ώρα … προς αποφυγή παρόμοιων περιστατικών.

Γ) Στη συνέχεια, και καθώς δεν εντοπίστηκε έως και ώρα …, λάθος επί της υλοποίησης, δηλαδή σε επίπεδο εφαρμογής από την ανάδοχο εταιρεία, προτάθηκε η προσθήκη δεύτερου επιπέδου ελέγχου κατά την αυθεντικοποίηση του χρήστη μέσω της Διαλειτουργικότητας της ΓΓΠΣΔΔ (oAuth2 service) και συγκεκριμένα

επιβεβαίωση του IBAN[1] μετά την εισαγωγή κωδικών taxisnet. Η πρόταση της αναδόχου εταιρείας του Υπουργείου Ψηφιακής Διακυβέρνησης έγινε αποδεκτή, με τη σύμφωνη γνώμη της Διεύθυνσης και του Γραφείου Υπουργού και η εφαρμογή επανήλθε σε κανονική λειτουργία την ίδια ημέρα … και ώρα … και το Υπουργείο Ψηφιακής Διακυβέρνησης ανέλαβε την περαιτέρω διερεύνηση του θέματος σε συνεργασία με την ΓΓΠΣΔΔ, καθώς το πρόβλημα φάνηκε ότι προέκυψε στην φάση αυθεντικοποίησης των χρηστών. Τα ηλεκτρονικά μηνύματα που ανταλλάχθηκαν επισυνάπτονται στην απάντηση του Υπουργείου προς την Αρχή.

Περαιτέρω, το Υπουργείο Τουρισμού αναφέρει στην ως άνω απάντησή του ότι η ηλεκτρονική εφαρμογή www.tourism4all.gov.gr, σύμφωνα με την με αρ. 9126/17.06.2020 Δημόσια Πρόσκληση (ΨΡ73465ΧΘΟ-51Θ), άνοιξε για υποβολή αιτήσεων δικαιούχων στις … και το εν λόγω περιστατικό συνέβη την δεύτερη ημέρα λειτουργίας της και μάλιστα εντός του πρώτου 24ώρου λειτουργίας της (…). Για πρώτη φορά το Κέντρο Διαλειτουργικότητας της ΓΓΠΣΔΔ δέχτηκε τεράστιο όγκο αιτημάτων, καθώς οι εν δυνάμει δικαιούχοι του Προγράμματος, σύμφωνα με στοιχεία της ΑΑΔΕ, ήταν περίπου 5 εκ. πολίτες. Καθ’ όλο το διάστημα λειτουργίας της ηλεκτρονικής εφαρμογής η υπηρεσία του Υπουργείου Τουρισμού ήταν σε διαρκή επικοινωνία με τις εμπλεκόμενες υπηρεσίες, προκειμένου να αντιμετωπιστούν τα προβλήματα που προέκυπταν κατά την διαδικασία, όπως επιτυχώς έγινε – όπως αναφέρει το Υπουργείο - και στη συγκεκριμένη περίπτωση. Ως προς αυτό, το Υπουργείο αναφέρει επίσης ότι με το με αρ. … έγγραφό του διαβιβάστηκε το ως άνω αρχικό έγγραφο της Αρχής στο Υπουργείο Ψηφιακής Διακυβέρνησης για τη συνδρομή του κατά λόγο αρμοδιότητας. Καθώς η απάντηση των αρμοδίων εμπλεκομένων υπηρεσιών (Υπ. Ψηφιακής Διακυβέρνησης και ΓΓΠΣΔΔ) εκκρεμούσε, στις 27 Οκτωβρίου 2020 εστάλη ηλεκτρονικό μήνυμα υπενθύμισης προς το Υπ. Ψηφιακής Διακυβέρνησης. Η σχετική αλληλογραφία, συμπεριλαμβανομένου του δεύτερου υπομνηστικού εγγράφου της Αρχής, προωθήθηκε εκ νέου στις … στο Υπουργείο Ψηφιακής Διακυβέρνησης μέσω ηλεκτρονικού μηνύματος και κατόπιν σχετικής

[1] Σημείωση: όπως ειπώθηκε και σε μεταγενέστερα έγγραφα, αλλά και κατά την ακρόαση του Υπουργείου Τουρισμού ενώπιον της Αρχής, δεν πρόκειται για το IBAN αλλά για τον Αριθμό Φορολογικού Μητρώου (ΑΦΜ).

τηλεφωνικής επικοινωνίας, καθώς και το με αρ. … έγγραφο του Υπουργείου Τουρισμού προς το Υπουργείο Ψηφιακής Διακυβέρνησης για παροχή πληροφόρησης.

Τέλος, αναφορικά με το θέμα ορισμού Υπευθύνου Προστασίας Δεδομένων και λειτουργικότητας της ηλεκτρονικής διεύθυνσης επικοινωνίας και άσκησης δικαιωμάτων, το οποίο εκφεύγει – όπως αναφέρεται στην ως άνω επιστολή του Υπουργείου προς την Αρχή - των αρμοδιοτήτων της Γενικής Διεύθυνσης Τουριστικής Πολιτικής, αναφέρεται ότι το σχέδιο πρόσκλησης υποβολής προσφορών για την ανάθεση υπηρεσιών με αντικείμενο τον σχεδιασμό και την ανάπτυξη Συστήματος Συμμόρφωσης με τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ) και την παροχή υπηρεσιών Υπευθύνου Προστασίας Προσωπικών Δεδομένων βρίσκεται υπό επεξεργασία και μέχρι την ολοκλήρωση της διαδικασίας η διεύθυνση επικοινωνίας έχει αντικατασταθεί στους «Όρους Χρήσης & Πολιτική Προστασίας Δεδομένων» της ηλεκτρονικής εφαρμογής με την ηλεκτρονική διεύθυνση tourism4all@mintour.gr.

Στη συνέχεια, η Αρχή κάλεσε σε ακρόαση, μέσω τηλεδιάσκεψης, το Υπουργείο Τουρισμού στη συνεδρίαση της Ολομέλειας της 23-06-2021 (βλ. κλήση με αριθ. πρωτ. Γ/ΕΞΕ/1344/31-05-2021). Μία ημέρα πριν την ημερομηνία της συνεδρίασης, το Υπουργείο Τουρισμού υπέβαλε μέσω ηλεκτρονικού ταχυδρομείου (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/4112/22-06-2021) τα υπ' αριθμ. πρωτ. … και … έγγραφά του, με το πρώτο από τα οποία παραθέτει αναλυτικότερες πληροφορίες που αφορούν τα ζητήματα που θα συζητούνταν ενώπιον της Αρχής, ενώ με το δεύτερο ζήτησε αναβολή της επικείμενης συζήτησης. Ειδικότερα, στο πρώτο έγγραφο το Υπουργείου Τουρισμού αναφέρονται τα εξής:

Α) Με την υπ' αρ. 9022/16.06.2020 Κοινή Υπουργική Απόφαση των Υπουργών Οικονομικών, Ανάπτυξης και Επενδύσεων, Τουρισμού και Επικρατείας εγκρίθηκε η κατάρτιση προγράμματος με σκοπό την ενίσχυση της ζήτησης του εγχώριου τουρισμού "Τουρισμός για όλους" έτους 2020 μέσω της επιδότησης διακοπών (Β' 2393). Σύμφωνα με την παράγραφο 1 του άρθρου 7 της ως άνω κοινής υπουργικής απόφασης για την ένταξη στο πρόγραμμα απαιτείται αίτηση, η οποία υποβάλλεται από τους δικαιούχους στην ηλεκτρονική εφαρμογή του Υπουργείου Τουρισμού www.tourism4all.gov.gr μέσω της Ενιαίας Ψηφιακής Πύλης της Δημόσιας Διοίκησης.

Για την υποβολή της αίτησης απαιτείται η προηγούμενη αυθεντικοποίηση των δικαιούχων με τη χρήση των κωδικών - διαπιστευτηρίων της Γενικής Γραμματείας Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης του Υπουργείου Ψηφιακής Διακυβέρνησης (taxisnet). Σύμφωνα με την παράγραφο 3 του ίδιου άρθρου, κατά την ηλεκτρονική υποβολή της αίτησης, διατίθενται μέσω του Κέντρου Διαλειτουργικότητας της Γενικής Γραμματείας Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης του Υπουργείου Ψηφιακής Διακυβέρνησης διαδικτυακές υπηρεσίες, προκειμένου για την άντληση, από τα πληροφοριακά συστήματα της Α.Α.Δ.Ε., της Η.ΔΙ.Κ.Α. Α.Ε. και του Μητρώου Πολιτών του Υπουργείου Εσωτερικών, και χορήγηση στο Υπουργείο Τουρισμού, των εξής δεδομένων προσωπικού χαρακτήρα του αιτούντος:

α) από τα πληροφοριακά συστήματα της Α.Α.Δ.Ε.:

i. Ένδειξη εκκαθαρισμένης φορολογικής δήλωσης για το ελεγχόμενο ως προς το εισοδηματικό κριτήριο φορολογικό έτος (0 ή 1),

ii. Ένδειξη εκκαθαρισμένης φορολογικής δήλωσης για το φορολογικό έτος που προηγείται του φορολογικού έτους της ανωτέρω περίπτωσης i (0 ή 1),

iii. Εισόδημα σύμφωνα με τις προβλέψεις της ως άνω Κ.Υ.Α. για τον ΑΦΜ του αιτούντος και των τυχόν υπολοίπων μελών της οικογενείας του και

β) από τα πληροφοριακά συστήματα «ΑΜΚΑ-ΕΜΑΕΣ» της Η.Δ.Ι.Κ.Α. Α.Ε. και του Μητρώου Πολιτών του Υπουργείου Εσωτερικών:

i. Τρέχουσα οικογενειακή κατάσταση με βάση τα στοιχεία του αιτούντος και της συζύγου ή ετέρου μέρους συμφώνου συμβίωσης, εφόσον υπάρχει

ii. Επιβεβαίωση λίστας ανήλικων εξαρτώμενων τέκνων του αιτούντος.

Τέλος, στο άρθρο 14 της ως άνω Κ.Υ.Α. αναφέρεται ότι η παραγωγική λειτουργία των ως άνω διαδικτυακών υπηρεσιών εκκινεί κατόπιν έγκρισης του Γενικού Γραμματέα Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης του Υπουργείου Ψηφιακής Διακυβέρνησης, σύμφωνα με το άρθρο 47 του ν. 4623/2019 (Α΄ 134), ενώ η διάθεση διενεργείται μέσω του Κέντρου Διαλειτουργικότητας (εφεξής ΚΕΔ) της Γενικής Γραμματείας Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης και σύμφωνα με το ισχύον Πλαίσιο Ασφάλειας Πληροφοριακών Συστημάτων της Γενικής Γραμματείας Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης του Υπουργείου Ψηφιακής

Διακυβέρνησης και με τις διατάξεις περί προστασίας των δεδομένων προσωπικού χαρακτήρα.

Β) Η υποβολή των αιτήσεων ξεκίνησε στις 21:30 της …, και προγραμματίστηκε σύμφωνα με τον τελευταίο αριθμό του ΑΦΜ των αιτούντων. Το ηλεκτρονικό μήνυμα του Α (… - … από την ηλεκτρονική διεύθυνση: ...) με θέμα: "Διαρροή στοιχείων στην πλατφόρμα tourism4all.gov.gr" κοινοποιήθηκε στην ηλεκτρονική διεύθυνση tourism4all@mintour.gr που δημιουργήθηκε αποκλειστικά για την άμεση διαχείριση κάθε είδους επικοινωνίας αναφορικά με το πρόγραμμα ΤΟΥΡΙΣΜΟΣ ΓΙΑ ΟΛΟΥΣ ΕΤΟΥΣ 2020. Το μήνυμα είχε ως παραλήπτη την ηλεκτρονική διεύθυνση: complaints@dpa.gr και έτερη κοινοποίηση προς άλλη ηλεκτρονική διεύθυνση (σσ. η οποία φέρεται να είναι αυτή του θιγόμενου προσώπου). Παρόλο που, όπως ισχυρίζεται το Υπουργείο, η αυθεντικότητα του μηνύματος δεν ήταν δυνατόν να πιστοποιηθεί, εν τούτοις διερευνήθηκε ως πραγματικό περιστατικό, ενώ το Υπουργείο σημειώνει ότι ο Α δεν απέκτησε πρόσβαση στα φορολογικά στοιχεία του έτερου προσώπου αλλά σε στοιχεία αίτησής του στο εν λόγω πρόγραμμα. Δεδομένου ότι η υλοποίηση της ψηφιακής εφαρμογής για το πρόγραμμα «Τουρισμός για Όλους» αναπτύχθηκε σε συνεργασία με το Υπουργείο Ψηφιακής Διακυβέρνησης, το οποίο καθοδήγησε το Υπουργείο Τουρισμού για τον σχεδιασμό και την ανάπτυξη διαλειτουργικότητας των υπηρεσιών μέσω του Κέντρου Διαλειτουργικότητας της ΓΓΠΣΔΔ, το Υπουργείο Ψηφιακής Διακυβέρνησης παρέπεμψε στη συνεργαζόμενη με αυτό ανάδοχη εταιρεία THREENITAS Α.Ε. Συνεπώς, η Δ/νση Στρατηγικού Σχεδιασμού προέβη σε άμεση ενημέρωση του Υπουργείου Ψηφιακής Διακυβέρνησης και της εποπτευόμενης από αυτό ΓΓΠΣΔΔ για το εν λόγω περιστατικό, σε σχέση με το οποίο η αλληλουχία ενεργειών περιγράφεται στο ως άνω έγγραφο του Υπουργείου. Ειδικότερα, οι ενέργειες που έλαβαν χώρα είναι συνοπτικά οι εξής:

- …, … μ.μ. - Εισερχόμενο μήνυμα αναφοράς από ... (Α) προς tourism4all@mintour.gr
- …, … μ.μ. - Εξερχόμενο μήνυμα αναφοράς του περιστατικού προς ΓΓΠΣ, Υπουργείο Ψηφιακής Διακυβέρνησης, Ανάδοχο, Διεύθυνση, Γενική Διεύθυνση Τουριστικής Πολιτικής Υπουργείου Τουρισμού, Γραφείο Υπουργού Τουρισμού

- …, … μ.μ. - Ερώτημα από τον ανάδοχο προς την ΓΓΠΣ για την ακριβή ώρα που έγιναν authentication requests στο oAuth2 service των δύο ΑΦΜ που από την καταγραφή στην εφαρμογή φαίνεται ότι δημιούργησαν αιτήσεις με διαφορά 10 λεπτών
- …, … μ.μ. - Δόθηκε εντολή για διακοπή λειτουργίας εφαρμογής από το Γραφείο Υπουργού μέχρι την επίλυση
- …, … μ.μ. - Κλείδωμα εφαρμογής από την ανάδοχο εταιρεία μέχρι να ολοκληρωθεί η σχετική επικοινωνία.
- …, … μ.μ. - Απάντηση της ΓΓΠΣ αναφορικά με τις ώρες που έγιναν τα authentication requests στο oAuth2 service των δύο ΑΦΜ
- …, … μ.μ. - Αίτημα της Υπηρεσίας για εντοπισμό των IP διευθύνσεων
- …, …μ.μ. - Απάντηση του αναδόχου ότι δεν έχει γίνει εντοπισμός λάθους στην υλοποίηση και συνεχίζονται οι προσπάθειες εντοπισμού του λάθους με όλους τους εμπλεκόμενους. Πρόταση υιοθέτησης διπλού ελέγχου ΑΦΜ κατά την είσοδο στην εφαρμογή.
- …, … μ.μ. - Απάντηση ΓΓΠΣ αναφορικά με τις IP διευθύνσεις (αναλυτικές πληροφορίες δίνονται εντός του εγγράφου του Υπουργείου).
- …, … μ.μ. - Αίτημα ανοίγματος της εφαρμογής από την υπηρεσία με εντολή Γραφείου Υπουργού Τουρισμού σύμφωνα με την πρόταση διπλού ελέγχου ΑΦΜ που έγινε από τον ανάδοχο.

Περαιτέρω, σύμφωνα με την από 18.06.2021 (Α.Π. 10906/22.06.2021) σχετική αναφορά του κ. Β, Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ) της αναδόχου εταιρείας THREENITAS Α.Ε.[2] (η οποία συνυποβλήθηκε στην Αρχή μαζί με το εν λόγω έγγραφο του Υπουργείου Τουρισμού), η πρώτη φάση της αντιμετώπισης είχε ως στόχο την αξιολόγηση της έκτασης και της σοβαρότητας του περιστατικού. "*Ως προς την έκταση: Διαπιστώθηκε ότι το περιστατικό δεν μπορούσε να αναπαραχθεί στην κανονική ροή χρήσης της εφαρμογής. Σε ανάλυση των logs δεν εντοπίστηκε καμία άλλη περίπτωση, πέρα από αυτή που οδήγησε στην σχετική αναφορά*." Αναλυτικά, ο ΥΠΔ της αναδόχου εταιρείας καταγράφει τα εξής: "*Παρελήφθησαν στοιχεία που*

[2] Επισημαίνεται ότι η εταιρεία δεν έχει ανακοινώσει στην Αρχή στοιχεία Υπευθύνου Προστασίας Δεδομένων με βάση το άρθρο 37 παρ. 7 του ΓΚΠΔ.

είχαν ζητηθεί από το ΚΕΔ αναφορικά με την χρήση της υπηρεσίας TaxisNet Login, και ανακτήθηκαν δεδομένα από το σύστημα logging της πλατφόρμας. Εκτελέστηκε σειρά από εκτενείς ελέγχους στον κώδικα της εφαρμογής, και επιβεβαιώθηκε η ορθή αντιμετώπιση όλων των υποστηριζόμενων σεναρίων. Δεν εντοπίστηκε κάποιο πρόβλημα στην υλοποίηση και δεν ήταν εφικτή η αναπαραγωγή του συμβάντος. Συνεπώς, αποκλείστηκε κάθε ενδεχόμενο το συμβάν να οφείλεται σε λάθος υλοποίησης που αφορούσε την ψηφιακή πλατφόρμα. Κατόπιν εξετάστηκαν στοιχεία που αφορούσαν την υλοποίηση του OAuth2.0, στο οποίο βασίζεται υπηρεσία TaxisNet Login της ΓΓΠΣ, καθώς και την υποδομή εξυπηρέτησης της εφαρμογής. Ωστόσο, η υλοποίηση του OAuth2.0 χρησιμοποιήθηκε ως έχει από σχετικό software library, στο οποίο έχουν βασιστεί και άλλες υλοποιήσεις υπηρεσιών της ΗΔΙΚΑ, η δε υποδομή εξυπηρέτησης παρέχεται από την υπηρεσία Amazon Web Services, και κάνει χρήση στοιχείων που επιτρέπουν την υποστήριξη μεγάλου όγκου εισερχόμενων αιτημάτων, όπως load balancer και πολλαπλών server instances. Σε κάθε περίπτωση, και τα δύο ενδεχόμενα αφορούν λειτουργίες και συστήματα που τελούν εκτός του ελέγχου της εταιρείας και του Υπουργείου Τουρισμού, και δεν μπορούσαν να αναλυθούν περαιτέρω. Τα παραπάνω ευρήματα αναφέρθηκαν και στο ΚΕΔ προκειμένου να γίνει παράλληλος έλεγχος στην υποδομή που υποστηρίζει το μηχανισμό αυθεντικοποίησης, χωρίς όμως να αναφερθεί κάποιο τεχνικό πρόβλημα. Σημειώνεται ότι μόνο κατά τη διάρκεια της … η ψηφιακή πλατφόρμα tourism4all δέχτηκε επίσκεψη από περίπου 80.000 χρήστες, οι οποίοι εκτέλεσαν 1.200.000 προβολές περιεχομένου. Ωστόσο, πέρα από την αναφορά συμβάντος που έγινε από τον εν λόγω χρήστη, δεν κατέστη δυνατό να εντοπιστεί κανένα άλλο αντίστοιχο περιστατικό στις άλλες 1.200.000 προβολές περιεχομένου».

Περαιτέρω, όπως ήδη αναφέρθηκε ανωτέρω, υλοποιήθηκε βελτιωτική πρόταση της αναδόχου εταιρείας, ήτοι η προσθήκη δεύτερου επιπέδου ελέγχου κατά την αυθεντικοποίηση του χρήστη μέσω της Διαλειτουργικότητας της ΓΓΠΣΔΔ (oAuth2 service) και συγκεκριμένα επιβεβαίωση του ΑΦΜ μετά την εισαγωγή των κωδικών taxisnet. Ο πολίτης, δηλαδή, καλείται να εισαγάγει τον ΑΦΜ του καθώς το στοιχείο αυτό αποτελεί μέρος και της πληροφορίας που ανακτάται κατά την αυθεντικοποίηση. Σύμφωνα με την επέκταση που προτάθηκε, ο ΑΦΜ που εισάγει ο χρήστης συγκρίνεται με τον ΑΦΜ που επιστρέφεται κατά το TaxisNet Login. Σε

περίπτωση που τα δύο διαφέρουν, ο χρήστης αποσυνδέεται, προκειμένου να δοκιμάσει να συνδεθεί εκ νέου. Η πρόταση της αναδόχου εταιρείας του Υπουργείου Ψηφιακής Διακυβέρνησης έγινε αποδεκτή, με τη σύμφωνη γνώμη της Διεύθυνσης Στρατηγικού Σχεδιασμού και του Γραφείου Υπουργού Τουρισμού και η εφαρμογή επανήλθε σε κανονική λειτουργία την ίδια ημέρα … και ώρα … ενώ το Υπουργείο Ψηφιακής Διακυβέρνησης ανέλαβε την περαιτέρω διερεύνηση του θέματος σε συνεργασία με την ΓΓΠΣΔΔ, καθώς το πρόβλημα φάνηκε ότι προέκυψε στη φάση αυθεντικοποίησης των χρηστών και σε κάθε περίπτωση δεν άπτετο των αρμοδιοτήτων του Υπουργείου Τουρισμού λόγω της τεχνικής φύσης του.

Όπως επίσης αναφέρει το Υπουργείου Τουρισμού στο έγγραφό του, σύμφωνα με στοιχεία της ΑΑΔΕ, οι εν δυνάμει δικαιούχοι του Προγράμματος ήταν περίπου 5 εκατομμύρια πολίτες, στοιχείο για το οποίο είχε ενημερωθεί τόσο ο ανάδοχος όσο και η ΓΓΠΣΔΔ από το Υπουργείο Τουρισμού (ηλεκτρονικό μήνυμα …) προκειμένου να ληφθούν όλα τα απαραίτητα μέτρα σε τεχνικό επίπεδο λόγω αρμοδιότητας. Πράγματι, το Κέντρο Διαλειτουργικότητας της ΓΓΠΣΔΔ δέχτηκε τεράστιο όγκο κλήσεων και καθ’ όλο το διάστημα λειτουργίας της ηλεκτρονικής εφαρμογής η Υπηρεσία ήταν σε διαρκή επικοινωνία τόσο με το Κ.Ε.Δ. της ΓΓΠΣΔΔ όσο και την ανάδοχο εταιρεία, προκειμένου να αντιμετωπιστούν τα προβλήματα που προέκυπταν κατά τη διαδικασία και να εξασφαλιστεί η απρόσκοπτη λειτουργία της εφαρμογής κατά την υποβολή των αιτήσεων.

Γ) Το συμβατικό πλαίσιο για τη συνεργασία του Υπουργείου Τουρισμού με όσους εμπλεκόμενους φορείς αναφέρονται ανωτέρω, ήτοι με το Υπουργείο Ψηφιακής Διακυβέρνησης, με τη Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης, με τον ανάδοχο THREENITAS Α.Ε. και την αναθέτουσα αρχή ΕΔΥΤΕ Α.Ε., εποπτευόμενο φορέα του Υπουργείου Ψηφιακής Διακυβέρνησης, διαμορφώθηκε ως εξής:

1) Με το από 01.09.2020 Μνημόνιο Συνεργασίας του Υπουργείου Ψηφιακής Διακυβέρνησης με το Υπουργείο Τουρισμού (συνημμένο στο εν λόγω έγγραφο του Υπουργείου Τουρισμού προς την Αρχή), το οποίο διαβιβάστηκε στο Γραφείο Υπουργού Τουρισμού για υπογραφή στις 11.11.2020 (Α.Π. Γρ. Υπουργού …/…) προσδιορίζεται ότι το αντικείμενο της σύμβασης, ήτοι η δημιουργία ηλεκτρονικής εφαρμογής/πλατφόρμας για την παροχή e-voucher στο πλαίσιο του προγράμματος

“Τουρισμός για όλους” έτους 2020, μέσω της Ενιαίας Ψηφιακής Πύλης της Δημόσιας Διοίκησης, γίνεται από το Υπουργείο Ψηφιακής Διακυβέρνησης, το οποίο αναπτύσσει το τεχνικό και ρυθμιστικό πλαίσιο για τη δημιουργία της σύμφωνα με τις κατευθυντήριες γραμμές του Υπουργείου Τουρισμού, το οποίο εκπονεί το πρόγραμμα. Από την ημερομηνία παράδοσης της ανωτέρω εφαρμογής/πλατφόρμας, το Υπουργείο Ψηφιακής Διακυβέρνησης δεν συμμετέχει περαιτέρω στη διαχείριση και τη λειτουργία της ούτε αποτελεί τον υπεύθυνο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, η οποία πραγματοποιείται στο πλαίσιο διαχείρισης της ηλεκτρονικής εφαρμογής/ πλατφόρμας, ενώ το Υπουργείο Τουρισμού αναλαμβάνει τη γενική διαχείρισή της, αποκτά την περιεχόμενη σε αυτήν πληροφορία και είναι υπεύθυνο για τη διαχείριση, συντήρηση και αναβάθμισή της. Περαιτέρω το Υπουργείο Τουρισμού είναι ο υπεύθυνος επεξεργασίας των δεδομένων προσωπικού χαρακτήρα της πλατφόρμας, της οποίας η τεχνική ανάλυση, ο σχεδιασμός και η υλοποίηση θα πραγματοποιηθεί από την ΕΔΥΤΕ Α.Ε., εποπτευόμενο φορέα του Υπουργείο Ψηφιακής Διακυβέρνησης. Με την υπογραφή του Μνημονίου, το Υπουργείο Ψηφιακής Διακυβέρνησης παραδίδει όλα τα δεδομένα και στοιχεία που σχετίζονται με το πρόγραμμα “Τουρισμός για όλους”, τον ιστότοπο «tourism4all.gov.gr» και την ηλεκτρονική πλατφόρμα «tourism4all».

2) Η με αρ. 10183/14.09.2020 Σύμβαση με αντικείμενο τη «Δημιουργία πλατφόρμας για την παροχή e-voucher στο πλαίσιο του προγράμματος “Τουρισμός για Όλους”» μεταξύ της Αναθέτουσας Αρχής ΕΔΥΤΕ Α.Ε. και του αναδόχου ΘΡΙΝΙΤΑΣ ΣΥΣΤΗΜΑΤΑ ΛΟΓΙΣΜΙΚΟΥ Α.Ε. (σσ. THREENITAS) (συνημμένη στο ως άνω έγγραφο του Υπουργείου Τουρισμού προς την Αρχή), έχει ως αντικείμενο την τεχνική ανάλυση, τον σχεδιασμό και την υλοποίηση της πλατφόρμας για την παροχή evoucher στο πλαίσιο του προγράμματος “Τουρισμός για Όλους” για παραγωγική λειτουργία μέσω του gov.gr. Επίσης, αναφέρεται ότι «*Η σύνδεση γίνεται μέσω των κωδικών TAXISnet με την παράλληλη δήλωση του ΑΜΚΑ. Η εφαρμογή διασυνδέεται με WebServices που παρέχονται από το ΚΕΠ της ΓΓΠΣΔΔ για την κάλυψη των αναγκών ανάκτησης ΑΦΜ και στοιχείων χρήστη, επιβεβαίωσης σχέσης γονέα/τέκνου μεταξύ του δικαιούχου και των μελών που δηλώνονται ως τέτοια, επιβεβαίωση σχέσης συντρόφου/συζύγου μεταξύ του δικαιούχου και του μέλους που δηλώνεται ως τέτοιο, ανάκτηση εισοδήματος»* και παρατίθενται τα WebServices τα οποία υποστηρίζουν την εκτέλεση

ελέγχων: *«User Authentication, έλεγχος σχέσης γονέα/τέκνου με χρήση ΑΜΚΑ, έλεγχος σχέσης συζύγου/συντρόφου με χρήση ΑΜΚΑ, Εισόδημα, IBAN/ΑΦΜ».* Αναφορικά με την προστασία προσωπικών δεδομένων, στην εν λόγω σύμβαση αναφέρεται ότι «*η επεξεργασία των δεδομένων προσωπικού χαρακτήρα θα εκτελείται σύμφωνα με τους όρους και συμφωνίες της παρούσας Σύμβασης και τις Οδηγίες της Αναθέτουσας Αρχής. Η Ανάδοχος δεσμεύεται ως προς την εφαρμογή και συμμόρφωση προς την ισχύουσα νομοθεσία για την προστασία δεδομένων προσωπικού χαρακτήρα (…)»* και «*Ο ανάδοχος βεβαιώνει και εγγυάται στην Αναθέτουσα Αρχή ότι θα λαμβάνει όλα τα απαραίτητα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των πληροφοριών που ενδέχεται να περιέχουν και προσωπικά δεδομένα, και γενικότερα όλων των ανάλογων μορφών αρχείων και πληροφορικών της Αναθέτουσας Αρχής, καθώς και για την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση και κάθε άλλη μορφή αθέμιτης επεξεργασίας, στο πλαίσιο των καθηκόντων του που πηγάζουν από την παρούσα»*.

3) Με το από 12.11.2020 Παράρτημα Γ' «Συμφωνητικό για την επεξεργασία δεδομένων προσωπικού χαρακτήρα (Data Processing Agreement-DPA), το οποίο προσαρτήθηκε στη με αρ. 10183/14.09.2020 Σύμβαση (επίσης συνημμένο στο ως άνω έγγραφο της Αρχής), ορίζεται ότι το Υπουργείο Τουρισμού είναι ο υπεύθυνος επεξεργασίας και επεξεργάζεται δεδομένα προσωπικού χαρακτήρα στο πλαίσιο του προγράμματος «Τουρισμός για Όλους», καθώς επίσης και ότι η εκτελούσα-ΕΔΥΤΕ Α.Ε. επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό και σύμφωνα με τις εντολές του υπευθύνου (Υπουργείο Τουρισμού) στο πλαίσιο της πλατφόρμας για παραγωγική λειτουργία μέσω του gov.gr. Η υπεργολάβος (Ανάδοχος- Threenitas) οφείλει: α) να παρέχει τη συνδρομή της προς την ΕΔΥΤΕ ΑΕ και μέσω αυτής προς το Υπουργείο Τουρισμού, αναφορικά με τη διασφάλιση της συμμόρφωσης αυτής με τις υποχρεώσεις της που πηγάζουν από τον ΓΚΠΔ και το Νόμο, αναφορικά με την άσκηση των δικαιωμάτων των υποκείμενων των δεδομένων, β) να ενημερώνει εγγράφως και χωρίς υπαίτια καθυστέρηση την ΕΔΥΤΕ ΑΕ, και αυτή με τη σειρά της το Υπουργείο Τουρισμού, για κάθε ερώτημα, παράπονο, καταγγελία ή αιτήματα που τυχόν λάβει και σχετίζονται με την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων, γ) να υποστηρίζει την ΕΔΥΤΕ ΑΕ, ώστε να παρέχει στον υπεύθυνο τη συνδρομή της

για τη διενέργεια μελέτης εκτίμησης επιπτώσεων/αντικτύπου της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, εάν αυτό καταστεί απαραίτητο με βάση τις διαδικασίες επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και σύμφωνα με τους όρους του ΓΚΠΔ και του Νόμου δ) να παρέχει μέσω της ΕΔΥΤΕ ΑΕ στο Υπουργείο Τουρισμού τη συνδρομή της για τη διαβούλευση με την Αρχή Προστασίας Δεδομένων σχετικά με τα προτεινόμενα και ενδεδειγμένα μέτρα περιορισμού του κινδύνου στις περιπτώσεις, όπου η μελέτη εκτίμησης αντικτύπου υποδεικνύει ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υπερκείμενων των δεδομένων. Τέλος, η υπεργολάβος (Ανάδοχος- Threenitas) υποχρεούται: «*να λαμβάνει όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα (…) προκειμένου να διασφαλίζεται το ανάλογο επίπεδο ασφάλειας έναντι των κινδύνων και συγκεκριμένα να διασφαλίζει το απόρρητο, την ακεραιότητα και τη διαθεσιμότητα της επεξεργασίας και των υπηρεσιών σε συνεχή βάση (…) υποχρεούται γενικά να εφαρμόζει για την παροχή των γενικών υπηρεσιών κατάλληλα μέτρα: κρυπτογράφηση, εξουσιοδοτημένη πρόσβαση, διαβαθμισμένη πρόσβαση, τήρηση logs, τήρηση αντιγράφων ασφαλείας, ισχυρό password για την είσοδο στα συστήματα και τακτική αλλαγή, απενεργοποίηση της λειτουργίας μέσων αποθήκευσης, ενεργοποίηση τείχους προστασίας στον υπολογιστή και ασφαλή απομακρυσμένη σύνδεση μόνο μέσω VPN*».

4) Με τη με αρ. 554/26.01.2021 σύμβαση με αντικείμενο την «Επέκταση της πλατφόρμας για την παροχή e-voucher στο πλαίσιο του προγράμματος "Τουρισμός για Όλους"-Φάση Β» μεταξύ της Αναθέτουσας Αρχής ΕΔΥΤΕ Α.Ε. και του αναδόχου ΘΡΙΝΙΤΑΣ ΣΥΣΤΗΜΑΤΑ ΛΟΓΙΣΜΙΚΟΥ Α.Ε. (συνημμένη στο ως άνω έγγραφο της Αρχής) επεκτείνεται το αντικείμενο της σύμβασης, ενώ το περιεχόμενο των όρων αυτής παρέμεινε ως είχε.

Γ) Αναφορικά με το θέμα ορισμού Υπευθύνου Προστασίας Δεδομένων, το οποίο εκφεύγει των αρμοδιοτήτων της Γενικής Διεύθυνσης Τουριστικής Πολιτικής και της Διεύθυνσης Στρατηγικού Σχεδιασμού που εκπονεί το Πρόγραμμα, το Υπουργείο Τουρισμού αναφέρει ότι μετά από τη δημοσίευση της με αρ. 5979/07.04.2021 πρόσκλησης υποβολής προσφορών για την ανάθεση υπηρεσιών με αντικείμενο τον σχεδιασμό και την ανάπτυξη Συστήματος Συμμόρφωσης με τις Απαιτήσεις του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ) και την παροχή

υπηρεσιών Υπευθύνου Προστασίας Προσωπικών Δεδομένων (ΑΔΑ: 631Τ465ΧΘΟ-Θ93)[3] και τη σχετική διαγωνιστική διαδικασία, εκδόθηκε η με αρ. 10398/14.06.2021 Απόφαση Υπηρεσιακής Γραμματέως Υπουργείου Τουρισμού περί αποδοχής των από 14.5.2021 (Συνεδριάσεις 26.4.2021 και 10.5.2021), 1.6.2021 (Συνεδριάσεις 28.5.2021 και 1.6.2021) και 9.6.2021 (Συνεδρίαση 9.6.2021) πρακτικών της επιτροπής αξιολόγησης των προσφορών της υπ΄ αριθ. 5979/07.04.2021 πρόσκλησης (ΑΔΑ: 93Η9465ΧΘΟ-0ΜΝ). Συνεπώς, επίκειται η υπογραφή σύμβασης με εξωτερικό συνεργάτη-ανάδοχο του Υπουργείου Τουρισμού, ο οποίος θα παράσχει υπηρεσίες Υπευθύνου Προστασίας Προσωπικών Δεδομένων[4]. Επισημαίνεται ότι, σύμφωνα με την ως άνω πρόσκληση, όπως διαπιστώθηκε από την Αρχή κατόπιν εξέτασής της από τη «Διαύγεια» όπου έχει αναρτηθεί, η προϋπολογισθείσα δαπάνη ανέρχεται έως του ποσού των 20.000,00€ χωρίς ΦΠΑ (ΦΠΑ: 4.800,00€, συνολικό ποσό 24.800,00€) και θα βαρύνει τον Προϋπολογισμό εξόδων του Υπουργείου, οικονομικών ετών 2021 και 2022.

Αναφορικά δε με το ζήτημα της λειτουργικότητας της διεύθυνσης ηλεκτρονικής επικοινωνίας και άσκησης δικαιωμάτων η οποία εμφανιζόταν στον ιστότοπο του Προγράμματος, η εν λόγω διεύθυνση έχει αντικατασταθεί, μέχρι την ολοκλήρωση της διαδικασίας ανάθεσης σύμβασης στους «Όρους Χρήσης & Πολιτική Προστασίας Δεδομένων» της ηλεκτρονικής εφαρμογής με την ηλεκτρονική διεύθυνση tourism4all@mintour.gr.

Δ) Συμπερασματικά, το Υπουργείο Τουρισμού αναφέρει ότι θεωρεί κρίσιμη την συνεισφορά των άμεσα εμπλεκόμενων φορέων στην τεχνική ανάπτυξη της εφαρμογής, ήτοι την ΕΔΥΤΕ, την Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης και το Υπουργείο Ψηφιακής Διακυβέρνησης, σημειώνοντας μάλιστα ότι από το Υπουργείο Ψηφιακής Διακυβέρνησης και τη ΓΓΠΣΔΔ δεν έχει λάβει μέχρι τις 22-6-2021 έγγραφη απάντησή τους σχετικά με τη διαχείριση του περιστατικού. Αναφέρει επίσης ότι η εφαρμογή σχεδιάστηκε από το Υπουργείο Ψηφιακής Διακυβέρνησης και έχει παραγωγική λειτουργία μέσω του gov.gr (η

[3] Προϋπολογισμού 24.800 ευρώ

[4] Όπως προκύπτει από το υπ' αριθμ. πρωτ. 10398/14-06-2021 έγγραφο του Υπουργείου (ΑΔΑ: 93Η9465ΧΘΟ-0ΜΝ) για την παροχή της υπηρεσίας επιλέχθηκε η εταιρεία INTERACTIVE Ο.Ε. με ποσό προσφοράς 21.948,00€ (συμπεριλαμβανομένου ΦΠΑ)

τεχνική ανάλυση, ο σχεδιασμός και η υλοποίηση της πλατφόρμας ανατέθηκε στην ΕΔΥΤΕ ΑΕ και από εκείνη σε εξωτερικό συνεργάτη - Ανάδοχο/Threenitas), ενώ οι Υπηρεσίες του Υπουργείου Τουρισμού δεν είχαν πλήρη γνώση των όρων συνεργασίας και όταν αυτή πραγματοποιήθηκε η εφαρμογή ήταν ήδη σε πλήρη λειτουργία. Ανακεφαλαιώνει επίσης αναφέροντας εκ νέου ότι το Υπουργείο Τουρισμού αποτελεί τον υπεύθυνο επεξεργασίας δεδομένων της πλατφόρμας, αλλά η εμπλοκή του δεν είναι δυνατό να έχει χαρακτήρα τεχνικής φύσης, ενώ η διασφάλιση της ορθής λειτουργίας της πλατφόρμας και της λήψης όλων των αναγκαίων μέτρων ασφάλειας προσωπικών δεδομένων αποτελεί υποχρέωση του Αναδόχου. Τέλος, το εν λόγω περιστατικό ήταν μεμονωμένο, αντιμετωπίστηκε άμεσα, ωστόσο τα προσωπικά δεδομένα δεν έγιναν ευρέως γνωστά/δεν εκτέθηκαν, ώστε να αξιολογηθεί ο κίνδυνος ως μεγάλος και σε συνδυασμό με τη μοναδικότητα και απολύτως περιορισμένη έκταση του περιστατικού και την αδυναμία επαλήθευσης και εντοπισμού σφάλματος, αξιολογήθηκε ότι το θιγόμενο πρόσωπο δεν τέθηκε σε κίνδυνο. Συνεπώς, κατά τους ισχυρισμούς του Υπουργείου Τουρισμού, δεν είναι δυνατόν να θεωρηθεί ότι παραβιάστηκαν τα οριζόμενα στα άρθρα 33 και 34 του Γενικού Κανονισμού Προστασίας Δεδομένων αναφορικά με τα περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα.

Κατά τη συνεδρίαση της 23-06-2021 παρέστησαν, μέσω τηλεδιάσκεψης, οι Γ, Νομικός Σύμβουλος, Γραφείο ΝΣΚ, Δ, Πάρεδρος, Γραφείο ΝΣΚ, Ε, Σύμβουλος του Γραφείου Υπουργού, ΣΤ, … Τουριστικής Πολιτικής, Ζ, … Στρατηγικού Σχεδιασμού, Η, … Τμήματος Ειδικών Μορφών Τουρισμού και η Θ, υπάλληλος Τμήματος Ειδικών Μορφών Τουρισμού, ως εκπρόσωποι του υπεύθυνου επεξεργασίας, ο οποίος υπέβαλε και προφορικά το αίτημα αναβολής της συζήτησης, το οποίο και έγινε δεκτό, με καθορισμό νέας ημερομηνίας συζήτησης της υπόθεσης την 19-7-2021. Στη συνεδρίαση της 19-7-2021 παρέστησαν, μέσω τηλεδιάσκεψης, οι Δ, Πάρεδρος, Γραφείο ΝΣΚ, Ε, Σύμβουλος του Γραφείου Υπουργού, ΣΤ, … Τουριστικής Πολιτικής, Ζ, … Στρατηγικού Σχεδιασμού, Θ, υπάλληλος Τμήματος Ειδικών Μορφών Τουρισμού, η Η, … Τμήματος Ειδικών Μορφών Τουρισμού, καθώς επίσης η Ι και Κ εκ μέρους της αναδόχου εταιρείας που έχει αναλάβει την παροχή υπηρεσιών Υπευθύνου Προστασίας Προσωπικών Δεδομένων στο Υπουργείο Τουρισμού, ως εκπρόσωποι του

υπεύθυνου επεξεργασίας. Μετά τη συνεδρίαση ο υπεύθυνος επεξεργασίας έλαβε προθεσμία για υποβολή υπομνήματος, το οποίο και υπέβαλε, εντός της ταχθείσας προθεσμίας, με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/5104/02-08-2021 έγγραφο.

Ήδη, πριν την υποβολή του υπομνήματος του Υπουργείου Τουρισμού, υποβλήθηκε στην Αρχή, από την ΓΓΠΣΔΔ του Υπουργείου Ψηφιακής Διακυβέρνησης, ενημερωτικό σημείωμα (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/4794/20-07-2021), το οποίο, αφού περιγράφει εκ νέου τις σχετικές διατάξεις της υπ' αρ. 9022/16.06.2020 Κ.Υ.Α., αναφέρει τις ενέργειες στις οποίες προέβη η ΓΓΠΣΔΔ για το εν λόγω περιστατικό, αναφέροντας ειδικώς τα εξής:

α) Η ΓΓΠΣΔΔ έλαβε ενημέρωση για το περιστατικό από το Υπουργείο Τουρισμού με ηλεκτρονικό μήνυμα την … και ώρα …. Σε σχέση με το αναφερόμενο συμβάν, ζητήθηκε η συνδρομή της.

β) Η ΓΓΠΣΔΔ προχώρησε σε έλεγχο της διαδικτυακής υπηρεσίας και δεν διαπίστωσε κάποιο πρόβλημα στην λειτουργία της και στην υποδομή αυθεντικοποίησης. Επιπλέον έλεγξε λεπτομερώς τα σχετικά αρχεία καταγραφής.

γ) Η ΓΓΠΣΔΔ απέστειλε με e-mail την ίδια ημέρα και ώρα … τα σχετικά logs που τηρούνται στο Κέντρο Διαλειτουργικότητας και αφορούσαν αναφορές στις κλήσεις στο oAuth 2.0.

δ) Κατά τις πρώτες ημέρες λειτουργίας της πλατφόρμας το ΚΕ.Δ./ΓΓΠΣΔΔ ενημέρωσε το Υπουργείο Τουρισμού με στατιστικά χρήσης των διαδικτυακών υπηρεσιών για την παρακολούθηση της δράσης.

ε) Η υπηρεσία αυθεντικοποίησης oAuth 2.0 του ΚΕΔ είναι ευρέως διαδεδομένη και χρησιμοποιούμενη σε πλήθος ηλεκτρονικών υπηρεσιών των φορέων του Δημοσίου. Οι κλήσεις oAuth 2.0 εντός του 2020 ανήλθαν σε 54.185.731, ενώ στο πρώτο εξάμηνο του 2021 έχουν πραγματοποιηθεί ήδη 86.396.905 κλήσεις, χωρίς να έχει αναφερθεί ή διαπιστωθεί κάποια δυσλειτουργία στον μηχανισμό αυτό.

Περαιτέρω, η ΓΓΠΣΔΔ αναφέρει ότι προκειμένου μία web εφαρμογή να αξιοποιεί πολλαπλά ταυτόχρονους χρήστες, χρειάζεται η εφαρμογή να έχει τον έλεγχο των συνόδων (sessions) που δημιουργούνται, ώστε τελικά κάθε χρήστης να εξυπηρετείται με τη λειτουργικότητα και τα δεδομένα που τον αφορούν. Σημειώνεται ότι οι κλήσεις

του oAuth2.0 και των web services προς το ΚΕ.Δ. καθώς και οι αποκρίσεις αυτών, ελέγχονται από την εκάστοτε εφαρμογή που τα καλεί. Ο διαχωρισμός των πληροφοριών για κάθε διακριτό φυσικό πρόσωπο πρέπει να διενεργείται μέσω της διακριτής διαχείρισης των session ids από την Web Εφαρμογή («Τουρισμός για όλους»). Ως προς την περαιτέρω διερεύνηση του θέματος, πέρα από θέματα αποκλειστικά αρμοδιότητας ΚΕΔ, η ΓΓΠΣΔΔ θεωρείται αναρμόδια.

Στο προαναφερθέν υπόμνημα του Υπουργείου Τουρισμού, το οποίο υποβλήθηκε μετά την ακρόασή του ενώπιον της Αρχής, επαναλαμβάνεται η περιγραφή των διαδικασιών που ακολουθήθηκαν για την αντιμετώπιση του περιστατικού (όπως αυτές ήδη είχαν περιγραφεί σε προηγούμενα έγγραφα του Υπουργείου), επισυνάπτεται το περιεχόμενο του ως άνω ενημερωτικού σημειώματος της ΓΓΠΣΔΔ, ενώ επίσης επαναλαμβάνεται το περιεχόμενο της αναφοράς του ΥΠΔ της Αναδόχου (Threenitas). Περαιτέρω, το Υπουργείο Τουρισμού αναφέρει ότι, μετά την ακρόασή του ενώπιον της Αρχής, ζήτησε περαιτέρω διευκρινίσεις από την ανάδοχο εταιρεία, η οποία με την με αρ. … (Α.Π. Υπουργείου Τουρισμού) επιστολή της (συνημμένη στο εν λόγω υπόμνημα του Υπουργείου προς την Αρχή) διευκρινίζει: «*Η εφαρμογή "Τουρισμός για Όλους" χρησιμοποιεί βιβλιοθήκη βασισμένη στην επίσημη βιβλιοθήκη της Microsoft για τη διασύνδεση με OAuth2 providers, όπως η υπηρεσία Αυθεντικοποίησης του GSIS. Η βιβλιοθήκη χρησιμοποιεί χωρίς τροποποιήσεις τις μεθόδους που παρέχει η Microsoft για τη διαχείριση των πολλαπλών sessions. Στην περίπτωση που εξετάζεται, όπου παρατηρήθηκε η εμφάνιση στοιχείων άλλου χρήστη, το ζήτημα εντοπίστηκε στο γεγονός ότι τα στοιχεία που επεστράφησαν από το GSIS προς την υποδομή μετά το redirection της αυθεντικοποίησης, αφορούσαν άλλον χρήστη από αυτόν για τον οποίο έγινε η διαδικασία της αυθεντικοποίησης. Η διαδικασία της αυθεντικοποίησης και το session management, η διαχείριση δηλαδή των sessions που δημιουργούνται στα πλαίσια των σχετικών αιτημάτων εξυπηρέτησης των χρηστών, εκτελέστηκε αποκλειστικά με χρήση των μεθόδων που παρέχονται από την εν λόγω βιβλιοθήκη. Με δεδομένο ότι: α) ο μηχανισμός για τη διαχείριση των πολλαπλών συνδέσεων γίνεται με χρήση των βιβλιοθηκών της Microsoft που δεν δικαιολογεί την αμφισβήτηση της ορθότητάς τους β) η λειτουργία της επιβεβαιώθηκε με την εκτέλεση δοκιμών, καθώς και σε συνθήκες τεχνητού*

φόρτου, όταν αυτές εφαρμόστηκαν στον εξυπηρετητή που φιλοξενεί την εφαρμογή, γ) λειτούργησε εν γένει χωρίς προβλήματα κατά τις συνθήκες μεγάλου φόρτου που παρατηρήθηκαν σε όλες τις επόμενες φάσεις της λειτουργίας του συστήματος θεωρούμε ως μόνο πιθανό ενδεχόμενο το συγκεκριμένο ζήτημα να δημιουργείται από λάθος διαχείριση σε οποιονδήποτε από τις ενδιάμεσες δικτυακές υποδομές μεταξύ *της εφαρμογής και της ΚΕΔ. Οι υποδομές αυτές δεν τελούν υπό τον έλεγχο της Threenitas και του Υπουργείου Τουρισμού, και χρησιμοποιούνται ως έχουν. Ενδεικτικά αναφέρεται ότι η υποδομή χρησιμοποιούσε τις υπηρεσίες Application Load Balancer και Web Application Firewall, όπως αυτές παρέχονται από το Amazon Cloud, που θα μπορούσαν υπό συνθήκες να οδηγήσουν στη λανθασμένη διαχείριση των πολλαπλών ενεργών συνδέσεων με τις υποδομές της ΚΕΔ. Όπως αναφέρθηκε και στην από 18/06/2021 αναφοράς μας, μετά την επιβεβαίωση της ορθής λειτουργίας της εφαρμογής, και κατόπιν εισαγωγής επιπλέον ελέγχων για την αντιμετώπιση του φαινομένου που παρατηρήθηκε, ώστε να αποτραπεί η πιθανότητα δυσλειτουργίας ακόμη και εξ αιτίας γεγονότων που δεν τελούν υπό τον έλεγχο της εφαρμογής, το πρόβλημα αντιμετωπίστηκε και δεν παρατηρήθηκε εκ νέου».* Περαιτέρω, από την ηλεκτρονική αλληλογραφία που έλαβε χώρα την ημέρα του περιστατικού διαφαίνεται ότι ο Χρήστης με ΑΦΜΧΧΧΧΧ… (Λ) προέβη σε δύο (2) συνδέσεις, συγκεκριμένα την … … ΜΜ (…) και … … ΜΜ από την ίδια IP διεύθυνση …, και ο Χρήστης με ΑΦΜ ΧΧΧΧΧ… (Α) επίσης σε δύο (2) συνδέσεις την … … ΜΜ και την … … ΜΜ, από δύο διαφορετικές IP διευθύνσεις, τις … και … και το Υπουργείο Τουρισμού εικάζει ότι κατά την πρώτη σύνδεση υποβλήθηκε η αίτηση και στη δεύτερη επιχειρήθηκε ανάκτησή της, όποτε και παρατηρήθηκε το περιστατικό ανάκτησης αίτησης του έτερου χρήστη. Ο λόγος που το περιστατικό δεν γνωστοποιήθηκε στην Αρχή, σύμφωνα με το άρθρο 33 του ΓΚΠΔ, είναι ότι: α) Η αναφορά είχε γίνει απ' ευθείας προς την Αρχή Προστασίας Δεδομένων από τον πολίτη (Α) με κοινοποίηση στο θιγόμενο πρόσωπο, το οποίο δεν προέβη σε καμία ενέργεια, β) Ο υπεύθυνος επεξεργασίας προέβη σε ενέργειες και έλαβε κατάλληλα μέτρα με την εισαγωγή ενός επιπλέον επιπέδου ασφάλειας κατά την είσοδο και ταυτοποίηση των χρηστών, που διασφάλισαν τη μη επανεμφάνιση ενός τέτοιου περιστατικού. Το περιστατικό αξιολογήθηκε ήσσονος σημασίας και ο κίνδυνος μηδαμινός έως ανύπαρκτος, ότι

δηλαδή δεν υφίσταται ενδεχόμενο πρόκλησης κινδύνου για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Στο υπόμνημά του το Υπουργείο επίσης αναφέρει ότι δεδομένου ότι α) η υλοποίηση της ψηφιακής εφαρμογής για το πρόγραμμα «Τουρισμός για Όλους» αναπτύχθηκε σε συνεργασία με το Υπουργείο Ψηφιακής Διακυβέρνησης, το οποίο καθοδήγησε το Υπουργείο Τουρισμού για το σχεδιασμό και την ανάπτυξη διαλειτουργικότητας των υπηρεσιών μέσω του Κέντρου Διαλειτουργικότητας της ΓΓΠΣΔΔ και της συνεργαζόμενης με το Υπουργείο Ψηφιακής Διακυβέρνησης ανάδοχης εταιρείας THREENITAS Α.Ε. και β) στις … δεν είχε συμβασιοποιηθεί το έργο, το οποίο προχώρησε με την μορφή του κατεπείγοντος λόγω της πανδημίας με σκοπό την ενίσχυση του εσωτερικού τουρισμού και τη στήριξη της εγχώριας τουριστικής αγοράς με την απ' ευθείας συνεργασία των Γραφείων των δύο Υπουργών (Τουρισμού και Ψηφιακής Διακυβέρνησης), η Δ/νση Στρατηγικού Σχεδιασμού του Υπουργείου Τουρισμού προέβη σε άμεση ενημέρωση του Υπουργείου Ψηφιακής Διακυβέρνησης και της εποπτευόμενης από αυτό ΓΓΠΣΔΔ για το εν λόγω περιστατικό ως αναφέρεται. Το Υπουργείο Τουρισμού δεν γνώριζε τους όρους της σύμβασης με την ανάδοχο εταιρεία. Για τους ως άνω λόγους επίσης θεωρήθηκε – εσφαλμένα - ότι η ηλεκτρονική διεύθυνση dpo@mintour.gov.gr που περιλήφθηκε στους όρους χρήσης της εφαρμογής ήταν ηλεκτρονική διεύθυνση την οποία θα λειτουργούσε το Υπουργείο Ψηφιακής Διακυβέρνησης και η διαχείριση αυτής δεν θα πραγματοποιούνταν από το Υπουργείο Τουρισμού. Άλλωστε, όπως αναφέρεται και στο Μνημόνιο Συνεργασίας, η πλατφόρμα ως προς το περιεχόμενό της σχεδιάστηκε σύμφωνα με οδηγίες του Υπουργείου Τουρισμού, το οποίο όμως δεν είχε δώσει ποτέ αυτή την ηλεκτρονική διεύθυνση για το Πρόγραμμα, αλλά μόνο την δική του ηλεκτρονική διεύθυνση tourism4all@mintour.gr. Εξάλλου όλες οι ηλεκτρονικές διευθύνσεις του Υπουργείου Τουρισμού είναι της μορφής xxxxxxx@mintour.gr χωρίς να συμπεριλαμβάνεται σε αυτές η λέξη gov και από πλευράς του Υπουργείου δημιουργήθηκε στις 16.06.2020 η ηλεκτρονική αυτή διεύθυνση προκειμένου να δέχεται ερωτήσεις/παράπονα/καταγγελίες κ.λ.π. αναφορικά με το Πρόγραμμα. Στην ηλεκτρονική αυτή διεύθυνση εστάλη και η εν λόγω καταγγελία και υπήρξε άμεση αντίδραση, ως περιγράφεται σε όλα τα έγγραφα του Υπουργείου προς την Αρχή.

Τέλος, το Υπουργείου Τουρισμού αναφέρει ότι με τη με αρ. 23/2021 (ΑΔΜΑ:

21SYMV008841946 2021-06-30) σύμβαση ανέθεσε την παροχή υπηρεσιών Υπευθύνου Προστασίας Προσωπικών Δεδομένων στην εταιρεία Interactive ΟΕ και υπέβαλε τη με αρ. … ανακοίνωση προς την Αρχή Προστασίας Δεδομένων (Α.Π. ΑΠΔ) για τον ορισμό του Υπευθύνου Προστασίας Δεδομένων. Επομένως, έχει ήδη πραγματοποιηθεί από πλευράς Υπουργείου Τουρισμού ο ορισμός Υπευθύνου Προστασίας Δεδομένων. Στις 16.07.2021 ενημερώθηκαν οι Όροι Χρήσης και Πολιτική Προστασίας Δεδομένων της εφαρμογής www.tourism4all.gov.gr με την ηλεκτρονική διεύθυνση επικοινωνίας του ΥΠΔ, ήτοι: dpo@mintour.gr.

Η Αρχή, μετά από εξέταση όλων των στοιχείων του φακέλου και αφού άκουσε τον εισηγητή και τους βοηθούς εισηγητές, οι οποίοι (βοηθοί) αποχώρησαν μετά τη συζήτηση της υπόθεσης και πριν από τη διάσκεψη, μετά από διεξοδική συζήτηση

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Σύμφωνα με τις διατάξεις των άρθρων 51 και 55 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679 (εφεξής, ΓΚΠΔ) και του άρθρου 9 του ν. 4624/2019 (ΦΕΚ Α΄ 137), 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 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· 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 στο ίδιο άρθρο στοιχ. 8 ορίζεται ως εκτελών την επεξεργασία «*το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας*».

3. 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*».
4. 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, στις οποίες περιλαμβάνεται 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 5 παρ. 1 στοιχ. στ'. 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.
5. 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 (…)*»

6. Στο άρθρο 28 παρ. 2 του ΓΚΠΔ, αναφορικά με τους εκτελούντες την επεξεργασία, προβλέπεται ότι «*ο εκτελών την επεξεργασία δεν προσλαμβάνει άλλον εκτελούντα την επεξεργασία χωρίς προηγούμενη ειδική ή γενική γραπτή άδεια του υπευθύνου επεξεργασίας. Σε περίπτωση γενικής γραπτής άδειας, ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας για τυχόν σκοπούμενες αλλαγές που αφορούν την προσθήκη ή την αντικατάσταση των άλλων εκτελούντων την επεξεργασία, παρέχοντας με τον τρόπο αυτό τη δυνατότητα στον υπεύθυνο επεξεργασίας να αντιταχθεί σε αυτές τις αλλαγές*». Περαιτέρω, στην παρ. 3 του ιδίου άρθρου, προβλέπεται ότι η επεξεργασία από τον εκτελούντα την επεξεργασία διέπεται από σύμβαση ή άλλη νομική πράξη υπαγόμενη στο δίκαιο της Ένωσης ή του κράτους μέλους, που δεσμεύει τον εκτελούντα την επεξεργασία σε σχέση με τον υπεύθυνο επεξεργασίας και καθορίζει το αντικείμενο και τη διάρκεια της επεξεργασίας, τη φύση και τον σκοπό της επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα και τις κατηγορίες των υποκειμένων των δεδομένων και τις υποχρεώσεις και τα δικαιώματα του υπευθύνου επεξεργασίας. Εξάλλου στην παρ. 4 του ιδίου άρθρου ορίζεται: «*Όταν ο εκτελών την επεξεργασία προσλαμβάνει άλλον εκτελούντα για τη διενέργεια συγκεκριμένων δραστηριοτήτων επεξεργασίας για λογαριασμό του υπευθύνου επεξεργασίας, οι ίδιες υποχρεώσεις όσον αφορά την προστασία των δεδομένων που προβλέπονται στη σύμβαση ή στην άλλη νομική πράξη μεταξύ υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία, κατά τα προβλεπόμενα στην παράγραφο 3, επιβάλλονται στον άλλον αυτόν εκτελούντα μέσω σύμβασης ή άλλης νομικής πράξης σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους, ιδίως ώστε να παρέχονται επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, ούτως ώστε η επεξεργασία να πληροί τις απαιτήσεις του παρόντος κανονισμού»*. Στη δε παράγραφο 9 του ιδίου άρθρου διατυπώνεται σαφώς ότι «η σύμβαση ή η άλλη νομική πράξη που αναφέρεται στις παραγράφους 3 και 4 υφίσταται γραπτώς, μεταξύ άλλων σε ηλεκτρονική μορφή».

7. Σύμφωνα με το άρθρο 24 παρ. 1 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας, λαμβάνοντας υπόψη 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, εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με το ΓΚΠΔ, τα εν λόγω δε μέτρα πρέπει να επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο. Περαιτέρω, 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, προβλέπεται 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*».
8. Αναφορικά με τα περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα, ο ΓΚΠΔ επιβάλλει 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 εποπτική αρχή[5], εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν

[5] 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

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 η πληροφορία που πρέπει κατ' ελάχιστο να περιέχεται σε μία τέτοια γνωστοποίηση, στην οποία συμπεριλαμβάνονται - μεταξύ άλλων – «β) … το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες, γ) … οι ενδεχόμενες συνέπειες της παραβίασης των δεδομένων προσωπικού χαρακτήρα, δ) …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 αδικαιολόγητη καθυστέρηση.

Περαιτέρω, σύμφωνα με το άρθρο 34 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. 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). Η ανακοίνωση στο υποκείμενο των δεδομένων δεν απαιτείται, εάν πληρείται μία από τις προϋποθέσεις που περιγράφονται στην παράγραφο αυτή.

9. 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 και τα ανακοινώνουν στην εποπτική αρχή.

Εξάλλου, όπως προαναφέρθηκε, στοιχεία επικοινωνίας 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* (…)».

10. Στη συγκεκριμένη περίπτωση, το Υπουργείο Τουρισμού είναι υπεύθυνος επεξεργασίας, κατά την έννοια του άρθρου 4 στοιχ. 7 του ΓΚΠΔ, για την επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία πραγματοποιείται στο πλαίσιο της πλατφόρμας «tourism4all», σύμφωνα με όσα αναφέρονται στα ως άνω έγγραφα του Υπουργείου και με βάση την σχετική πληροφόρηση που παρείχε η πλατφόρμα. Τούτο δε απορρέει από την Κοινή Υπουργική Απόφαση Αριθμ. 9022/2020 «Πρόγραμμα "Τουρισμός για όλους" έτους 2020» (ΦΕΚ Β΄ 2393). Ειδικότερα, στο άρθρο 1 παρ. 2 της Κ.Υ.Α. υπ' αρ. 9022/16.06.2020 όπως τροποποιήθηκε με την υπ' αρ. 12181/31-07-2020 Κ.Υ.Α. (ΦΕΚ Β' 3155), προβλέπεται ότι «*Για την ένταξη στο πρόγραμμα απαιτείται αίτηση, η οποία υποβάλλεται από τους δικαιούχους στην ηλεκτρονική εφαρμογή του Υπουργείου Τουρισμού www. tourism4all.gov.gr μέσω της Ενιαίας Ψηφιακής Πύλης της Δημόσιας Διοίκησης*» ενώ στο άρθρο 7 παρ. 4 της ίδιας ΚΥΑ προβλέπεται ότι «*Με την υποβολή της αίτησης συμμετοχής παρέχεται η συγκατάθεση προς το Υπουργείο Τουρισμού για την επεξεργασία των ανωτέρω προσωπικών δεδομένων του αιτούντος και των ωφελουμένων μελών του, αποκλειστικά για τους σκοπούς ένταξης στο Πρόγραμμα της παρούσας. Τα ανωτέρω δεδομένα διατηρούνται από το Υπουργείο Τουρισμού για δύο (2) έτη από την έκδοση του Οριστικού Μητρώου Δικαιούχων Ωφελουμένων και του Οριστικού Πίνακα Αποκλειομένων και σε κάθε περίπτωση μέχρι την ολοκλήρωση του προγράμματος*». Συνεπώς, παρά τη μη ορθή αναφορά σε συγκατάθεση (η οποία δεν μπορεί να χρησιμοποιηθεί ως νομική βάση για επεξεργασία προσωπικών δεδομένων για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας) καθίσταται σαφές ότι πρόθεση του νομοθέτη είναι να καταστεί υπεύθυνος επεξεργασίας το Υπουργείο Τουρισμού.

11. Το Υπουργείο Ψηφιακής Διακυβέρνησης, διά της ΓΓΠΣΔΔ, είναι εκτελών την επεξεργασία για την υλοποίηση και λειτουργία της πλατφόρμας, αφού στο άρθρο 7 της ως άνω Κ.Υ.Α. ορίζεται ότι , «*για την ένταξη στο Πρόγραμμα απαιτείται αίτηση, η οποία υποβάλλεται από τους δικαιούχους στην ηλεκτρονική εφαρμογή του Υπουργείου Τουρισμού www.tourism4all.gov.gr μέσω της Ενιαίας Ψηφιακής Πύλης της Δημόσιας Διοίκησης. Για την υποβολή της αίτησης απαιτείται η προηγούμενη αυθεντικοποίηση (επαλήθευση της ταυτότητας) των δικαιούχων με τη χρήση των κωδικών διαπιστευτηρίων της Γενικής Γραμματείας Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης του Υπουργείου Ψηφιακής Διακυβέρνησης (taxisnet)*» και ότι «*Κατά την ηλεκτρονική υποβολή της αίτησης, διατίθενται μέσω του Κέντρου Διαλειτουργικότητας της Γενικής Γραμματείας Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης του Υπουργείου Ψηφιακής Διακυβέρνησης διαδικτυακές υπηρεσίες, προκειμένου για την άντληση και χορήγηση στο Υπουργείο Τουρισμού, από τα πληροφοριακά συστήματα της Α.Α.Δ.Ε., της Η.ΔΙ.Κ.Α. Α.Ε. και του Μητρώου Πολιτών του Υπουργείου Εσωτερικών, (…) δεδομένων προσωπικού χαρακτήρα του αιτούντος (…)*». Η δε εταιρεία THREENITAS Α.Ε, ανάδοχος εταιρεία, συνεργαζόμενη με το Υπουργείο Ψηφιακής Διακυβέρνησης για την εν λόγω επεξεργασία, αποτελεί επίσης εκτελούσα την επεξεργασία (και εφόσον έχει συμβληθεί με εκτελούντα την επεξεργασία, πρόκειται ουσιαστικά για υπο-εκτελούσα, όπως περιγράφεται στο άρθρο 28 παρ. 2 του ΓΚΠΔ). Περαιτέρω, το συμπέρασμα αυτό προκύπτει και από τα πραγματικά γεγονότα, καθώς όπως προκύπτει από το φάκελο της υπόθεσης, ακόμα και στο αρχικό διάστημα κατά το οποίο δεν υπήρξε σύμβαση και έγγραφη ανάθεση της επεξεργασίας η εφαρμογή υλοποιήθηκε με τον τρόπο που περιγράφεται παραπάνω. Περαιτέρω, όπως προκύπτει από τα έγγραφα που υπέβαλε ο υπεύθυνος επεξεργασίας στην Αρχή, η ΕΔΥΤΕ Α.Ε., εποπτευόμενος φορέα του Υπουργείου Ψηφιακής Διακυβέρνησης, αποτελεί επίσης εκτελούσα την επεξεργασία.
12. Αναφορικά με το υπό εξέταση περιστατικό παραβίασης δεδομένων, προκύπτει ότι υπήρξαν αμέσως ενέργειες από τον υπεύθυνο επεξεργασίας για τη διερεύνηση και την αντιμετώπισή του. Σημειώνεται ότι για τεχνικά θέματα ασφάλειας της επεξεργασίας προκύπτει ότι τη σχετική αρμοδιότητα την έχουν οι εκτελούντες την επεξεργασία, ήτοι το Υπουργείο Ψηφιακής Διακυβέρνησης ως προς το σκέλος ιδίως

της αυθεντικοποίησης των χρηστών και η THREENITAS Α.Ε. ως προς την υλοποίηση της πλατφόρμας για την παροχή evoucher στο πλαίσιο του προγράμματος – ως εκ τούτου, η ενέργεια του υπευθύνου επεξεργασίας να αποταθεί αμέσως στο Υπουργείο Ψηφιακής Διακυβέρνησης, αλλά και να διακόψει προσωρινά τη λειτουργία της πλατφόρμας, κρίνεται ως ορθή. Επίσης, το πρόσθετο μέτρο ασφάλειας που υλοποιήθηκε για την αντιμετώπισή του, όπως προτάθηκε από τη THREENITAS Α.Ε. (ήτοι η χρήση δεύτερου παράγοντα αυθεντικοποίησης) είναι στη σωστή κατεύθυνση, αν και δεν σχετίζεται με τη γενεσιουργό αιτία του περιστατικού – η οποία μάλιστα δεν κατέστη εφικτό να προσδιοριστεί.

Τα ζητήματα που εγείρονται ως προς το εν λόγω περιστατικό παραβίασης είναι τα εξής:

Α) Για την εν λόγω επεξεργασία δεν υπήρχε σύμβαση ή άλλη νομική πράξη κατά την περίοδο που έλαβε χώρα το εν λόγω περιστατικό. Συγκεκριμένα, δεν υπήρχε σύμβαση του Υπουργείου Ψηφιακής Διακυβέρνησης (εκτελών την επεξεργασία) με τη THREENITAS Α.Ε. (υπο-εκτελούσα την επεξεργασία), αφού αυτή υπογράφηκε το Σεπτέμβριο του 2020, ενώ δεν προκύπτει ότι ζητήθηκε η (έστω και γενικού τύπου) άδεια του Υπουργείου Τουρισμού, ως υπευθύνου επεξεργασίας, για την εν λόγω ανάθεση (αν και προκύπτει ότι ο υπεύθυνος επεξεργασίας γνώριζε την εν λόγω ανάθεση). Περαιτέρω, το μνημόνιο συνεργασίας μεταξύ του Υπουργείου Τουρισμού, υπευθύνου επεξεργασίας, και του Υπουργείου Ψηφιακής Διακυβέρνησης, εκτελούντα την επεξεργασία, στο οποίο προσδιορίζεται και ο ρόλος της ΕΔΥΤΕ Α.Ε., καταρτίστηκε επίσης το Σεπτέμβριο του 2020, ήτοι αφού είχε ξεκινήσει η εν λόγω επεξεργασία και μετά το υπό εξέταση περιστατικό παραβίασης. Όπως αναφέρει ο υπεύθυνος επεξεργασίας, η εν λόγω καθυστέρηση οφείλεται στο ότι ήταν κατεπείγον να αρχίσει η εν λόγω επεξεργασία, λόγω της πανδημίας και με σκοπό την ενίσχυση του εσωτερικού τουρισμού και τη στήριξη της εγχώριας τουριστικής αγοράς (σκοπός που σαφώς υπάγεται στο δημόσιο συμφέρον). Ωστόσο, η μη έγγραφη σύμβαση ή άλλη νομική πράξη, πέραν του ότι αποτελεί παράβαση του άρθρου 28 παρ. 9 του ΓΚΠΔ[6], δεν επιτρέπει και τον καθορισμό μίας

[6] Βλ. επίσης και τις Κατευθυντήριες Γραμμές 7/2020 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων για τις έννοιες του υπευθύνου επεξεργασίας και εκτελούντα την επεξεργασία, στις οποίες σαφώς αναφέρεται: *«(…) non-written agreements (regardless of how thorough or effective they*

σαφούς διαδικασίας για την αντιμετώπιση περιστατικών παραβίασης, με σαφή διάκριση και προσδιορισμό του ρόλου και της ευθύνης του κάθε φορέα (τόσο του υπευθύνου επεξεργασίας, όσο και των εκτελούντων). Φαίνεται λοιπόν ότι ακολουθήθηκε μία «ad hoc» διαδικασία αντιμετώπισης του περιστατικού, από την οποία τελικά ο υπεύθυνος επεξεργασίας δεν κατέστη εφικτό να ανακαλύψει, διά των εκτελούντων την επεξεργασία, την πηγή του εν λόγω περιστατικού: όπως προκύπτει από τα στοιχεία του φακέλου της υπόθεσης, ο υπεύθυνος επεξεργασίας, πέραν των ηλεκτρονικών μηνυμάτων τα οποία αντηλλάγησαν κατά το πρώτο 24ωρο από τη στιγμή που έγινε γνωστό το περιστατικό, ζήτησε – μετά τα έγγραφα της Αρχής με τα οποία ζητούνταν οι απόψεις του - περαιτέρω απόψεις από το Υπουργείο Ψηφιακής Διακυβέρνησης, χωρίς να λάβει απάντηση. Περίπου ένα έτος μετά το περιστατικό (ήτοι τον Ιούνιο του 2021), ζήτησε και έλαβε απάντηση από τον ΥΠΔ της αναδόχου Threenitas, σύμφωνα με την οποία δεν υπήρχε έκταση στο περιστατικό ενώ το συγκεκριμένο σφάλμα δεν κατέστη εφικτό να αναπαραχθεί, τελικώς δε, απόψεις της ΓΓΠΣΔΔ του Υπουργείου Ψηφιακής Διακυβέρνησης εστάλησαν μετά και την ακρόαση του υπευθύνου επεξεργασίας ενώπιον της Αρχής, ενώ επίσης μετά την ακρόαση ζητήθηκαν εκ νέου και ελήφθησαν οι απόψεις της THREENITAS. Σε κάθε περίπτωση, διατυπώνονται μόνο εικασίες ως προς τη γενεσιουργό αιτία του περιστατικού, οι οποίες σχετίζονται ιδίως με το ενδεχόμενο σφάλματος έτοιμων βιβλιοθηκών λογισμικού που χρησιμοποιήθηκαν, χωρίς να εντοπίζεται σαφώς η αιτία του. Τα ανωτέρω συνιστούν παράβαση των θεμελιωδών προϋποθέσεων περί λήψης κατάλληλων οργανωτικών και τεχνικών μέτρων για την ασφάλεια της επεξεργασίας, σύμφωνα με το άρθρο 32 του ΓΚΠΔ, σε συνάρτηση με το άρθρο 24, καθώς ο υπεύθυνος επεξεργασίας δεν έλαβε υπόψη τους κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων για τον καθορισμό των μέτρων ασφάλειας. Επισημαίνεται επίσης ότι η απουσία καθορισμού των εκτελούντων την επεξεργασία οδηγεί σε αυξημένους κινδύνους, όπως με τη χρήση υπό-εκτελούντων την επεξεργασία οι οποίοι ενδέχεται να μην καλύπτουν τις απαιτήσεις του ΓΚΠΔ, ή να μην έχουν ληφθεί τα κατάλληλα μέτρα για τη χρήση

are) cannot be considered sufficient to meet the requirements laid down by Article 28 GDPR" (διαθέσιμες στο διαδικτυακό σύνδεσμο https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf)

αυτών. Ειδικά επισημαίνεται η αναφορά σε χρήση των υπηρεσιών «υπολογιστικού νέφους» (cloud) της εταιρείας Amazon, γεγονός το οποίο ενδέχεται να σημαίνει ότι υπήρξε διαβίβαση δεδομένων προσωπικού χαρακτήρα εκτός ΕΕ. Σε κάθε περίπτωση η χρήση του εν λόγω υπολογιστικού νέφους προσθέτει έναν ακόμα εκτελούντα την επεξεργασία στην υπό κρίση δραστηριότητα για την οποία, με δεδομένο ότι η εταιρεία Amazon φαίνεται να ανήκει σε όμιλο επιχειρήσεων που υπόκειται στο δίκαιο των Η.Π.Α., θα έπρεπε να έχει διενεργηθεί ανάλυση σε σχέση με τη νομιμότητά της και με βάση όσα διαλαμβάνονται στις συστάσεις 01/2020 του ΕΣΠΔ[7], ενώ το Υπουργείο Τουρισμού, ως υπεύθυνος επεξεργασίας, δεν κατέδειξε ότι ήταν ενήμερο για αυτό κατά τη χρονική περίοδο που έλαβε χώρα το περιστατικό αφού, πέραν της απουσίας συμβάσεων, δεν κάνει οποιαδήποτε σχετική αναφορά.

Β) Δεν υπήρξε γνωστοποίηση του εν λόγω περιστατικού στην Αρχή όπως επιτάσσει το άρθρο 33 του ΓΚΠΔ. Σημειώνεται ότι, σύμφωνα με το άρθρο αυτό, η γνωστοποίηση γίνεται αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Με βάση τα στοιχεία του φακέλου της υπόθεσης, ο υπεύθυνος επεξεργασίας, με τη γνώση των στοιχείων που διέθετε εντός των πρώτων 72 ωρών από τη στιγμή που έλαβε γνώση αυτού, δεν μπορούσε να θεωρεί ότι δεν ενδέχεται να προκληθεί κίνδυνος για θιγόμενα πρόσωπα, αφού δεν διέθετε σαφή εικόνα της πηγής του περιστατικού, ενώ το ίδιο το περιστατικό, με βάση τη γνώση που είχε ο υπεύθυνος επεξεργασίας, ήδη ενείχε κοινοποίηση δεδομένων, συμπεριλαμβανομένων δεδομένων υγείας, σε τρίτους. Συνεπώς, θα έπρεπε να υποβληθεί η γνωστοποίηση στην Αρχή, λαμβάνοντας εξάλλου υπόψη ότι, σύμφωνα με την παράγραφο 4 του ιδίου άρθρου, «*σε περίπτωση που και εφόσον δεν είναι δυνατόν να παρασχεθούν οι πληροφορίες ταυτόχρονα, μπορούν να παρέχονται σταδιακά χωρίς αδικαιολόγητη καθυστέρηση*». Οι ισχυρισμοί του υπευθύνου επεξεργασίας ως προς το ότι δεν προέβη σε γνωστοποίηση στην Αρχή διότι αφενός ο πολίτης είχε ήδη ενημερώσει σχετικώς την Αρχή αλλά και το

[7] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data - https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

θιγόμενο πρόσωπο χωρίς το τελευταίο να προβεί σε κάποια ενέργεια και αφετέρου ο υπεύθυνος επεξεργασίας προέβη αμέσως σε ενέργειες αντιμετώπισής του δεν στοιχειοθετούν λόγο να απαλλαγεί ο υπεύθυνος επεξεργασίας από την υποχρέωση γνωστοποίησης κατά το άρθρο 33.

13. Ο υπεύθυνος επεξεργασίας δεν είχε ορίσει Υπεύθυνο Προστασίας Δεδομένων κατά τη χρονική περίοδο που αφορά η υπόθεση, κατά παράβαση του άρθρου 37 παρ. 1 του ΓΚΠΔ, καθώς ο ορισμός αυτού έγινε τον Ιούλιο του 2021 – ήτοι μετά την πάροδο τριών (3) ετών από τη θέση σε εφαρμογή του ΓΚΠΔ, ενώ η διαδικασία προκήρυξης ξεκίνησε τον Απρίλιο του 2021. Περαιτέρω, παρά την έλλειψη ορισμού ΥΠΔ, υπήρχε ανακριβής πληροφόρηση στην ιστοσελίδα της εν λόγω πλατφόρμας περί ύπαρξης ΥΠΔ με στοιχεία επικοινωνίας αυτού, τα οποία – όπως διαπίστωσε και η Αρχή - δεν ήταν έγκυρα. Ο υπεύθυνος επεξεργασίας αναφέρει ότι τα εν λόγω στοιχεία επικοινωνίας τέθηκαν από τον εκτελούντα την επεξεργασία και θεώρησε ότι πρόκειται για ηλεκτρονική διεύθυνση που αντιστοιχεί στον εκτελούντα. Ο ισχυρισμός όμως αυτός είναι αλυσιτελής σε σχέση με το ζήτημα αν συντρέχει παράβαση της ανωτέρω διάταξης αφού, ως υπεύθυνος επεξεργασίας, έχει στο ακέραιο την υποχρέωση πλήρους και σωστής ενημέρωσης προς τα υποκείμενα των δεδομένων, όπως επίσης και την υποχρέωση διευκόλυνσης ως προς την άσκηση των δικαιωμάτων τους (σκοπός για τον οποίο μπορούσε να χρησιμοποιηθεί η εν λόγω διεύθυνση, σύμφωνα με το άρθρο 38 παρ. 4 του ΓΚΠΔ). Σε κάθε δε περίπτωση, δεν προκύπτει ότι ο υπεύθυνος επεξεργασίας είχε κάνει μία τέτοια ανάθεση στον εκτελούντα την επεξεργασία (βλ. και ανωτέρω σχετικά με την έλλειψη έγγραφης σύμβασης ή άλλης νομικής πράξης). Ως εκ τούτου, υπήρξε και παραβίαση των υποχρεώσεων του άρθρου 13 του ΓΚΠΔ αναφορικά με την ενημέρωση που παρέχεται στα υποκείμενα των δεδομένων.
14. Με βάση τα ανωτέρω, η Αρχή κρίνει ότι συντρέχει περίπτωση να ασκήσει τις κατά το άρθρο 58 παρ. 2 του ΓΚΠΔ διορθωτικές εξουσίες της σε σχέση με τις διαπιστωθείσες παραβάσεις.
15. Η Αρχή κρίνει περαιτέρω ότι πρέπει, με βάση τις περιστάσεις που διαπιστώθηκαν, να επιβληθεί, κατ' εφαρμογή της διάταξης του άρθρου 58 παρ. 2 εδ. θ' του ΓΚΠΔ, αποτελεσματικό, αναλογικό και αποτρεπτικό διοικητικό χρηματικό πρόστιμο κατ'

άρθρο 83 του ΓΚΠΔ τόσο προς αποκατάσταση της συμμόρφωσης, όσο και για την τιμωρία της παράνομης συμπεριφοράς.

16. Περαιτέρω η Αρχή, έλαβε υπόψη τα κριτήρια επιμέτρησης του προστίμου που ορίζονται στο άρθρο 83 παρ. 2 του ΓΚΠΔ, τις παραγράφους 4 και 5 του ίδιου άρθρου που έχουν εφαρμογή στην παρούσα υπόθεση, το άρθρο 39 παρ. 1 και 2 του ν. 4624/2019 που αφορά την επιβολή διοικητικών κυρώσεων στους φορείς του δημόσιου τομέα, και τις Κατευθυντήριες γραμμές για την εφαρμογή και τον καθορισμό διοικητικών προστίμων για τους σκοπούς του Κανονισμού 2016/679 που εκδόθηκαν στις 03-10-2017 από την Ομάδα Εργασίας του άρθρου 29 (WP 253)[8], καθώς και τα πραγματικά δεδομένα της εξεταζόμενης υπόθεσης και ιδίως:

    i) το γεγονός ότι από το περιστατικό παραβίασης προέκυψε και διαρροή ευαίσθητων δεδομένων υγείας του θιγόμενου προσώπου σε τρίτο πρόσωπο,

    ii) το γεγονός ότι ο υπεύθυνος επεξεργασίας καθυστέρησε να ανταποκριθεί στα έγγραφα της Αρχής,

    iii) το γεγονός ότι ο υπεύθυνος επεξεργασίας δεν έχει ακόμα σαφή εικόνα, ούτε διά των εκτελούντων την επεξεργασία, ως προς την πηγή του περιστατικού παραβίασης,

    iv) το γεγονός ότι τα υποκείμενα των δεδομένων δεν διευκολύνθηκαν στην άσκηση των δικαιωμάτων τους, λόγω μη ορθής αναγραφής της ηλεκτρονικής διεύθυνσης του ΥΠΔ,

    v) το γεγονός ότι ο ορισμός του ΥΠΔ από τον υπεύθυνο επεξεργασίας έγινε με καθυστέρηση πέραν των τριών ετών, ενώ οι σχετικές διαδικασίες, οι οποίες οδήγησαν σε ορισμό ως ΥΠΔ εξωτερικής εταιρείας, δεν κινήθηκαν ούτε μετά το αρχικό έγγραφο της Αρχής το οποίο επισήμανε το εν λόγω ζήτημα παρά μόνο μετά την πάροδο δύο μηνών από το υπομνηστικό έγγραφο της Αρχής την 01-02-2021, με αποτέλεσμα, εκτός των άλλων, ο υπεύθυνος επεξεργασίας να έχει σημαντικό οικονομικό όφελος από την παραβίαση της σχετικής υποχρέωσής του, αν ληφθεί υπόψη το ύψος δαπάνης, την οποία θα

[8] Βλ. https://ec.europa.eu/newsroom/article29/items/611237 (τελευταία πρόσβαση: 10/9/2021)

επέσυρε ο έγκαιρος κατά το νόμο ορισμός ΥΠΔ, όπως προκύπτει από τα αναφερόμενα ανωτέρω στο ιστορικό της υπόθεσης σχετικά με την προϋπολογισθείσα δαπάνη για την ανάθεση υπηρεσιών ΥΠΔ,

vi) το γεγονός ότι ο υπεύθυνος επεξεργασίας πραγματοποίησε αμέσως ενέργειες για την αντιμετώπιση του περιστατικού,

vii) το γεγονός ότι δεν έχει διαπιστωθεί προηγούμενη αντίστοιχη παράβαση από τον υπεύθυνο επεξεργασίας,

viii) το γεγονός ότι από τα στοιχεία που τέθηκαν υπ' όψιν της Αρχής και με βάση τα οποία διαπίστωσε τις ανωτέρω παραβιάσεις του ΓΚΠΔ, δεν προκύπτει ότι ο υπεύθυνος επεξεργασίας προκάλεσε, εκ του περιστατικού παραβίασης δεδομένων που έλαβε χώρα, υλική ζημία στο θιγόμενο πρόσωπο,

ix) Το γεγονός ότι η παράβαση των διατάξεων σχετικά με τα δικαιώματα των υποκειμένων υπάγεται, σύμφωνα με τις διατάξεις του άρθρου 83 παρ. 5 εδ. β' ΓΚΠΔ, στην ανώτερη προβλεπόμενη κατηγορία του συστήματος διαβάθμισης διοικητικών προστίμων.

17. Βάσει των ανωτέρω, η Αρχή αποφασίζει ομόφωνα ότι πρέπει να επιβληθούν στον καταγγελλόμενο υπεύθυνο επεξεργασίας οι αναφερόμενες στο διατακτικό διοικητικές κυρώσεις, οι οποίες κρίνονται ανάλογες με τη βαρύτητα των παραβάσεων.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή,

Επιβάλλει στο Υπουργείο Τουρισμού, ως υπεύθυνο επεξεργασίας, το αποτελεσματικό, αναλογικό και αποτρεπτικό διοικητικό χρηματικό πρόστιμο που αρμόζει στη συγκεκριμένη περίπτωση σύμφωνα με τις ειδικότερες περιστάσεις αυτής, ύψους εβδομήντα πέντε χιλιάδων ευρώ (75.000,00) ευρώ, για τις ως άνω διαπιστωθείσες παραβιάσεις των άρθρων 13, 32, 33, και 37 του Κανονισμού (ΕΕ) 2016/679, σύμφωνα με το άρθρο 58 παρ. 2 θ΄ του ΓΚΠΔ σε συνδυασμό με το άρθρο 83 παρ. 4 και 5 του ΓΚΠΔ και τα άρθρο 39 παρ. 1 του ν. 4624/2019.

Ο Πρόεδρος	Η Γραμματέας
Κωνσταντίνος Μενουδάκος	**Ειρήνη Παπαγεωργοπούλου**