TEL: +30 (211) 120 8000
WEB: www.mphotels.com

Greek / Ελληνικά – (English version follows below)

Ανακοίνωση για το πρόσφατο περιστατικό κυβερνοεπίθεσης και παραβίασης προσωπικών δεδομένων.

Αγαπητοί νυν και πρώην εργαζόμενοι,

Ο Όμιλος FTI, και η γερμανική μητρική εταιρεία «FTI Touristik GmbH», υπήρξε πρόσφατα θύμα κυβερνοεπίθεσης, η οποία είχε ως αποτέλεσμα την κρυπτογράφηση ορισμένων διακομιστών (server) και την αθέμιτη εξαγωγή ορισμένων αρχείων από το δίσκο V-drive του δικτύου του Ομίλου.

Η Εταιρεία μας, «MEETING POINT HOTEL MANAGEMENT HELLAS ΤΟΥΡΙΣΤΙΚΗ ΚΑΙ ΞΕΝΟΔΟΧΕΙΑΚΗ ΑΝΩΝΥΜΗ ΕΤΑΙΡΙΑ» με διακριτικό τίτλο «MEETING POINT HOTEL MANAGEMENT HELLAS A.E.» (με έδρα στην Λεωφ. Κηφισιάς 115, Αθήνα, 115 24, Ελλάδα), η οποία διαχειρίζεται τα ξενοδοχεία και τουριστικά θέρετρα: LABRANDA Blue Bay Resort (Ρόδος), LABRANDA Kiotari Miraluna Resort (Ρόδος), LABRANDA Marine Aquapark Resort (Κως), LABRANDA Sandy Beach Resort (Κέρκυρα), KAIRABA Sandy Villas (Κέρκυρα) and KAIRABA Mythos Palace (Κέρκυρα), ήταν μία από τις εταιρείες που επηρεάστηκε από αυτό το περιστατικό.

Ορισμένα από τα αρχεία που επλήγησαν από αυτή την κυβερνοεπίθεση περιέχουν, μεταξύ άλλων, προσωπικά δεδομένα νυν και πρώην εργαζομένων της Εταιρείας μας.

Κατ' αρχάς, θα θέλαμε να σας διαβεβαιώσουμε ότι η Εταιρεία μας και ο Όμιλος FTI κάνουμε ό,τι είναι δυνατό προκειμένου να περιορίσουμε στο ελάχιστο δυνατό τις πιθανές συνέπειες για όσους επλήγησαν.

Παρόλα αυτά, σας ενημερώνουμε ότι κάποια από τα αρχεία, τα οποία περιέχουν προσωπικά δεδομένα, όχι μόνο κρυπτογραφήθηκαν προσωρινά, αλλά επίσης εκλάπησαν από τους δράστες της κυβερνοεπίθεσης. Επιπλέον, οι δράστες της επίθεσης απείλησαν να δημοσιοποιήσουν αρχεία που ισχυρίζονται ότι έχουν στην κατοχή τους. Σε κάποιες περιπτώσεις, οι δράστες έχουν ήδη δημοσιεύσει στο διαδίκτυο δεδομένα από κάποιες από τις οντότητες του Ομίλου FTI, συμπεριλαμβανομένων και δεδομένων από την Εταιρεία μας.

Για αυτούς τους λόγους, αισθανόμαστε ότι είναι απαραίτητο να προχωρήσουμε στην παρούσα ανακοίνωση.

Είτε επηρεαστήκατε από μία πιθανή αθέμιτη εξαγωγή προσωπικών δεδομένων είτε από μία πιθανή δημοσίευση τέτοιων δεδομένων, θα θέλαμε να σας δώσουμε κάποιες πληροφορίες σχετικά με το περιστατικό, προκειμένου να μπορέσετε να καταλάβετε τι συνέβη, σε τι βαθμό ενδέχεται να επηρεαστήκατε, με ποιον τρόπο έχουμε αντιδράσει και ποιες επιπλέον ενέργειες μπορούν να γίνουν για να προστατευθούν τα δεδομένα σας.

Τι συνέβη;

Στις 31 Οκτωβρίου 2021, ειδοποιηθήκαμε από τους συναδέλφους στη γερμανική μητρική εταιρεία «FTI Touristik GmbH» για ένα περιστατικό που αντιλήφθηκαν στις 28 Οκτωβρίου 2021, το οποίο πιθανόν να

επηρέαζε και κάποια από τα δεδομένα της Εταιρείας μας (μεταξύ άλλων Εταιρειών του Ομίλου FTI), που βρίσκονται αποθηκευμένα στα εσωτερικά πληροφοριακά συστήματα του Ομίλου FTI.

Η FTI έθεσε αμέσως σε εφαρμογή πρωτόκολλα αντιμετώπισης, και ξεκίνησε έρευνα με την βοήθεια εξωτερικών εμπειρογνωμόνων και ειδικών στην κυβερνοασφάλεια, και εφάρμοσε σχέδια για την μη διακοπή της επιχειρησιακής λειτουργίας, ώστε να ελαχιστοποιηθούν οι επιπτώσεις για εμάς, τους εργαζομένους, τους πελάτες και τους συνεργάτες μας και να διασφαλιστεί η συνεχής ασφάλεια των συστημάτων μας. Η FTI συνεργάστηκε με ειδικούς προκειμένου να περιοριστεί και να διορθωθεί το περιστατικό, καθώς και για να παράσχουν προτάσεις ώστε να ενισχύσουμε την ασφάλειά μας απέναντι σε πιθανές μελλοντικές απειλές. Η συγκεκριμένη εργασία είναι συνεχής και γίνεται με πλήρη ρυθμό, ήδη από τη στιγμή που συνέβη το περιστατικό. Στο πλαίσιο αυτών των προσπαθειών, αποκαταστάθηκε η πρόσβαση στα αρχεία της Εταιρείας μας τα οποία είχαν κρυπτογραφηθεί κατά την επίθεση.

Εν τω μεταξύ, η συνεχιζόμενη έρευνα του Ομίλου FTI οδήγησε στο συμπέρασμα ότι όχι μόνο κρυπτογραφήθηκε από τους δράστες ο διακομιστής (server) στον οποίο αποθηκεύονταν τα δεδομένα μας, αλλά και ότι επίσης έχουν υποκλαπεί δεδομένα από μεμονωμένους φακέλους.

Αμέσως μόλις τα αρχεία που είχαν επηρεαστεί αποκαταστάθηκαν στο σύστημα μας, ξεκινήσαμε έρευνα σχετικά με το τι είδους δεδομένα περιέχονταν στους φακέλους που επηρεάστηκαν και καταλήξαμε στο συμπέρασμα ότι κάποιοι από τους φακέλους που επηρεάστηκαν περιείχαν, μεταξύ άλλων πραγμάτων, αρχεία με διάφορων ειδών προσωπικά δεδομένα που σχετίζονται με νυν και πρώην εργαζομένους.

Τι δεδομένα επηρεάστηκαν;

Θα θέλαμε να τονίσουμε ότι δεν έχουμε καμία απόδειξη ότι όλα τα προσωπικά δεδομένα που έχουμε αποθηκευμένα έχουν υποστεί ή υπόκεινται παράνομη επεξεργασία. Υπάρχουν από την άλλη ισχυρές ενδείξεις ότι μόνο κάποια από τα δεδομένα που έχουμε αποθηκευμένα εκλάπησαν.

Τα προσωπικά δεδομένα που επηρεάστηκαν από το περιστατικό ενδέχεται να είναι και όλα τα προσωπικά δεδομένα που παρασχέθηκαν σε εμάς ή που δημιουργήθηκαν από εμάς κατά την διάρκεια της εργασιακής σχέσης, π.χ. για τον εργασιακό σας φάκελο.

Αυτά μπορεί να περιλαμβάνουν το ονοματεπώνυμό σας, πατρώνυμο, αριθμό τηλεφώνου, διεύθυνση e-mail, διεύθυνση κατοικίας, ημερομηνία γέννησης, φύλο, εθνικότητα, οικογενειακή κατάσταση, τραπεζικά στοιχεία για μισθολογικούς σκοπούς (π.χ. αριθμό IBAN), πληροφορίες σχετικά με το εργασιακό σας ιστορικό, μισθολογικά στοιχεία, αριθμό δελτίου ταυτότητας ή διαβατηρίου, αριθμό φορολογικού μητρώου, αριθμό μητρώου κοινωνικής ασφάλισης ή ονόματα χρήστη/κωδικοί πρόσβασης (usernames/passwords) που μπορεί να ήταν αποθηκευμένα στα αρχεία μας. Δεν αφορούν όλες οι παραπάνω κατηγορίες κάθε έναν νυν ή πρώην εργαζόμενο.

Αν μας έχετε επίσης χορηγήσει αντίγραφα επίσημων εγγράφων σας, π.χ. δελτίων ταυτότητας και διαβατηρίων, ή μας έχετε χορηγήσει αυτά τα έγγραφα προκειμένου να σαρωθούν (σκαναριστούν) από την Εταιρεία, αυτά τα επίσημα έγγραφα ενδέχεται επίσης να έχουν επηρεαστεί.

Πως αντιμετωπίσαμε το περιστατικό;

Προκειμένου να προστατεύσουμε καλύτερα τα δεδομένα σας και να περιορίσουμε τον κίνδυνο παρόμοιων περιστατικών στο μέλλον, ολόκληρος ο Όμιλος FTI έθεσε σε εφαρμογή εκτενή μέτρα περιορισμού του κινδύνου αμέσως μόλις έγινε αντιληπτό το περιστατικό, συμπεριλαμβανομένων της απομόνωσης του δικτύου μας, της βελτίωσης των δυνατοτήτων να αντιληφθούμε μια εισβολή, και της ενίσχυσης των μηχανισμών αντιμετώπισης.

Επιπλέον, αμέσως μόλις επετεύχθη η αποκατάσταση της πρόσβασης στα αρχεία, η Εταιρεία διεξήγαγε εκτενή έρευνα προκειμένου να ταυτοποιηθούν τα αρχεία που επηρεάστηκαν, τα υποκείμενα των δεδομένων που επηρεάστηκαν και το είδος των δεδομένων που περιλαμβάνονταν στα επηρεαζόμενα αρχεία.

Επίσης από την στιγμή που έλαβε χώρα το περιστατικό, έχουν σταλεί αρκετές επικοινωνίες σε νυν εργαζομένους, με πληροφορίες σχετικά με την κυβερνοεπίθεση.

Επιπροσθέτως, είμαστε σε στενή επικοινωνία με τις αρχές προστασίας δεδομένων και τις ερευνητικές αρχές, ώστε να συντονίσουμε μαζί τους την διαχείριση του περιστατικού και να τους προσφέρουμε την πλήρη συνεργασία μας. Αμέσως μόλις η Εταιρεία μας ειδοποιήθηκε για το περιστατικό, ενημερώσαμε την ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα σχετικά με την κατάσταση. Η μητρική μας εταιρεία «FTI Touristik GmbH», η οποία διαχειρίζεται τους διακομιστές (server) όπου αποθηκεύονται τα δεδομένα της Εταιρείας μας, επίσης ενημέρωσε αμέσως τις αρμόδιες Αρχές Προστασίας Δεδομένων της Γερμανίας και κατήγγειλε την κυβερνοεπίθεση στις Γερμανικές αστυνομικές αρχές.

Τι θα μπορούσε να συμβεί με τα δεδομένα σας/ποιοι είναι οι κίνδυνοι για εσάς συγκεκριμένα;

- Οι δράστες ή τρίτοι που έχουν αποκτήσει τα δεδομένα σας θα μπορούσαν να σας στείλουν e-mail με συνημμένο κακόβουλο λογισμικό. Εάν ανοίξετε τα συνημμένα ενός τέτοιου e-mail, η συσκευή σας θα μπορούσε να μολυνθεί με κακόβουλο λογισμικό,
- Οι δράστες ή τρίτοι θα μπορούσαν να επικοινωνήσουν μαζί σας για να σας εκβιάσουν με τα υποκλαπέντα ή δημοσιευμένα δεδομένα,
- Εάν οι δράστες έχουν υποκλέψει αντίγραφα του δελτίου ταυτότητας ή του διαβατηρίου σας, είναι πιθανό να δημιουργηθούν παρανόμως πλαστογραφημένα δελτία ταυτότητας χρησιμοποιώντας αυτά ως πρότυπο,
- Χρησιμοποιώντας το όνομα, τα στοιχεία του τραπεζικού λογαριασμού και την διεύθυνση e-mail, τον αριθμό κοινωνικής ασφάλισης, τον αριθμό δελτίου ταυτότητας ή διαβατηρίου ή τα επίσημα έγγραφα ταυτοποίησής σας ή πιθανά ονόματα χρήστη/ κωδικούς πρόσβασης (usernames/ passwords) που μπορεί να ήταν αποθηκευμένα στα αρχεία μας, οι δράστες ενδέχεται να διαπράξουν κλοπή ταυτότητας. Θα μπορούσαν να παραγγελθούν αλλού αγαθά με δικά σας έξοδα και κίνδυνο με πίστωση τυχόν αποθηκευμένων μέσων πληρωμής. Αυτό είναι ιδιαίτερα πιθανό, εάν χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης για διαφορετικά συστήματα καταστημάτων.

Τι μπορείτε να κάνετε;

TEL: +30 (211) 120 8000
WEB: www.mphotels.com

Γενικώς, και ως βέλτιστη πρακτική, σας καλούμε να παραμείνετε σε επαγρύπνηση για απόπειρες ηλεκτρονικής εξαπάτησης/υποκλοπής (phishing), συμπεριλαμβανομένου τυχόν κινδύνου κλοπής ταυτότητας και απάτης. Υπάρχουν διάφορα μέτρα που μπορείτε να λάβετε για να βοηθήσετε στην προστασία των προσωπικών σας δεδομένων, συμπεριλαμβανομένων των εξής:

- προστατέψτε τα προσωπικά σας στοιχεία και αναφέρετε οποιαδήποτε ασυνήθιστη δραστηριότητα στις αρμόδιες αρχές (ή/και στην Εταιρεία μας),
- υποβάλετε μήνυση κατά των αγνώστων δραστών σε περίπτωση που αντιληφθείτε παράνομη πράξη σε βάρος σας,
- κάντε αίτηση για την έκδοση νέου διαβατηρίου/δελτίου ταυτότητας (μόνο στην περίπτωση που μας είχατε παράσχει αντίγραφα τέτοιων ταυτοποιητικών εγγράφων),
- χρησιμοποιείτε σύνθετους κωδικούς πρόσβασης, να τους αλλάζετε συχνά και να τους τηρείτε σε ασφαλές μέρος,
- χρησιμοποιείτε διαφορετικούς κωδικούς πρόσβασης για διαφορετικούς ιστοτόπους/ υπηρεσίες,
- αποφύγετε να ανοίγετε συνημμένα σε e-mail ή να κάνετε κλικ σε συνδέσμους που περιέχονται σε e-mail ή σε μηνύματα SMS που φαίνονται ύποπτα με οποιονδήποτε τρόπο,
- παρακολουθείτε τον τραπεζικό σας λογαριασμό για τυχόν ασυνήθιστες πληρωμές που δεν αναγνωρίζετε και αναφέρετε αμέσως οποιαδήποτε ασυνήθιστη δραστηριότητα στην τράπεζά σας.

Η ασφάλεια των δεδομένων σας αποτελεί κορυφαία προτεραιότητα για εμάς. Σας διαβεβαιώνουμε ότι έχουμε κάνει, και θα συνεχίσουμε να κάνουμε, ό,τι μπορούμε για να διασφαλίσουμε τη συνεχή ανθεκτικότητα των συστημάτων μας και για να αποτρέψουμε το ενδεχόμενο να επαναληφθεί ένα τέτοιου τύπου περιστατικό.

Καταλαβαίνουμε ότι η παρούσα ανακοίνωση μπορεί να εγείρει ανησυχίες και περαιτέρω ερωτήσεις από εσάς. Σε περίπτωση που έχετε επιπλέον απορίες σχετικά με αυτήν την ανακοίνωση, μη διστάσετε να επικοινωνήσετε μαζί μας. Μπορείτε για το σκοπό αυτό να επικοινωνήσετε απευθείας με την κο Χάρη Κολιαστάση στο dpo_hellas@mphotels.com .

Σας ευχαριστούμε για την συνεργασία και την υποστήριξή σας.

Η Διοίκηση της Εταιρείας

Εμμανουήλ Ντουλγκέρης
CEO/ Πρόεδρος

Παναγιώτης Στάμου-Δαγκλής
CFO/ Μέλος Δ.Σ.

TEL: +30 (211) 120 8000
WEB: www.mphotels.com

01/03/2022

English /Αγγλικά

Notification regarding the recent incident of cyberattack and personal data breach.

Dear current and former employees,

The FTI Group, and the German parent-company "FTI Touristik GmbH", was recently the victim of a cyberattack which resulted in the encryption of certain servers and the exfiltration of certain files on the V-drive of the Group's network.

Our Company, "MEETING POINT HOTEL MANAGEMENT HELLAS SA" (headquarters: 115 Kifisias Avenue, Athens, 115 24, Greece), which manages the hotels and resorts: LABRANDA Blue Bay Resort (Rhodes), LABRANDA Kiotari Miraluna Resort (Rhodes), LABRANDA Marine Aquapark Resort (Kos), LABRANDA Sandy Beach Resort (Corfu), KAIRABA Sandy Villas (Corfu) and KAIRABA Mythos Palace (Corfu), was one of the companies affected by this incident.

Some of the files that were affected by this cyberattack contain, among others, personal data of current and former employees of our Company.

First and foremost, we would like to assure you that our Company and FTI Group are doing everything in our power to keep the potential consequences for those affected as low as possible.

Nevertheless, we inform you that some of the files, which contain personal data, were not only temporarily encrypted, but also stolen by the perpetrators of the cyberattack. Also, the perpetrators of the attack threatened to publish files that they claim to be in possession of. In some cases, the perpetrators have already published online data of some entities of the FTI Group, including data from our Company.

For those reasons, we feel it is necessary to make this communication.

Whether you were affected by a possible exfiltration of personal data or also by a possible publication of such data, we would like to provide you with some information about the incident so that you can understand what happened, to what extent you may have been affected, how we reacted and what additional steps can be taken to protect your data.

What happened?

On 31 October 2021 we were alerted by our colleagues from our German parent-company "FTI Touristik GmbH" regarding an incident that they detected on 28 October 2021, which was probably affecting some data of our Company (among other Companies of FTI Group), stored in the internal IT systems of FTI Group.

FTI promptly initiated response protocols, launched an investigation with the assistance of third-party cybersecurity and forensic experts, and implemented business continuity plans to minimize disruption to us, to

our employees and to our customers and partners, and to ensure the ongoing security of our systems. FTI worked with experts to fully contain and remediate the incident, as well as provide recommendations to strengthen our security posture against potential future threats. Work on this has been ongoing at full speed since the incident happened. As part of these efforts, the files of our Company that were encrypted during the attack have been restored.

The ongoing investigation by FTI Group meanwhile led to the conclusion that the server that stored our information was not only encrypted by the perpetrators but also that data has been stolen out of single folders.

As soon as the files affected were restored in our system, we immediately initiated an investigation regarding what kind of data were contained in the affected folders and came to the conclusion that some of the affected files contained, among other things, various categories of personal data regarding current and former employees.

What information was involved?

We would like to emphasize that we have no evidence that all personal data stored with us has been or is being misused. Rather there are strong indications that only some of the data stored by us was stolen.

Personal data affected by the incident could be all personal data that was provided to us or generated by us in the course of your employment relationship, e.g. for your personnel file.

This could include your full name, father's name, telephone number, email, home address, date of birth, sex, nationality, marital status, bank details for payroll purposes (e.g. IBAN number), information related to your employment history, salary information, ID or passport number, tax identification number, social security number or usernames/passwords that may have been stored in our files. Not all of the above categories concern each and every current or former employee.

If you have also provided us with copies of your identity documents such as ID cards and passports, or have provided those documents in order to be scanned by the Company, these official documents may also be affected.

How did we respond to the incident?

To best protect your data and limit the risk of similar incidents in the future, the whole FTI Group has initiated extensive mitigation measures immediately after learning of the incident, including isolating our network, improving our intrusion detection capabilities and strengthening our response mechanisms.

In addition, as soon as the restoration of the files was achieved, the Company did intensive research in order to identify which files were affected, which data subjects were affected and what kind of data were included in the affected files.

Also, from the time that this incident took place, several communications have been sent-out to current employees, with information about the cyberattack.

Moreover, we are in close communication with the data protection and investigative authorities to coordinate with them the handling of the incident and offer them our full cooperation. Immediately after our Company was alerted of the incident, we notified the Greek Data Protection Authority regarding the situation. Our parent-company, "FTI Touristik GmbH", which manages the servers where our Company's data is stored, also immediately notified the competent Data Protection Authorities in Germany and reported the cyberattack to the German police authorities.

What could happen with your data/what are the risks for you in particular?

- the perpetrators or third parties who have obtained your data could send you e-mails with malware attached. If you open the attachments of such an e-mail, your end device could be contaminated with malware,
- the perpetrators or third parties could contact you in order to blackmail you with the stolen or published data,
- if the perpetrators have obtained copies of your ID card or passport, it is possible that illegally forged ID card copies could be created using these as a template,
- using the name, bank account details and email address information, your social security number, ID or passport number, or your identity documents, or possibly usernames/passwords that may have been stored in our files, the perpetrators may commit identity theft. Goods could be ordered elsewhere at your expense and risk to the detriment of the payment sources stored there. This is especially true if you use the same password for different shop systems.

What can you do?

As a general matter and for best practice, we encourage you to remain vigilant to phishing attempts including any risk of identity theft and fraud. There are various steps you can take to help protect your personal information, including those set out below:

- protect your personal information and report any unusual activity to the competent authorities (and/or to our Company),
- file a criminal complaint against the unknown perpetrators in case you become aware of an illegal act against you,
- apply for a new passport/ID card (only in case you provided us with copies of such identity documents),
- use complex passwords, change them often, and keep them in a safe place,
- use different passwords for different websites/services,

- avoid opening e-mail attachments or clicking on links in emails or in SMS messages that look suspicious in any way,
- monitor your bank account for any unusual payments that you do not recognize and report immediately any unusual activity to your bank.

The security of your data is a top priority for us. We assure you that we have been doing, and will continue to do, everything we can to ensure the ongoing resilience of our systems and to prevent this type of incident from occurring again.

We understand that this communication may raise some concerns and further questions from you. Therefore, if you have any additional questions about this notice, please feel free to contact us. You may reach directly for this purpose Mr. Haris Koliastasis at dpo_hellas@mphotels.com .

We thank you for your collaboration and support.

The Company's Management

Emmanouil Doulgkeris
CEO/ Chairman

Panagiotis Stamou-Dagklis
CFO/BoD member