IMPORTANT - Recent Cyber Incident

The FTI Group was recently the victim of a cyberattack which resulted in the encryption of certain servers and files on the Group's network. Meeting Point Hotel Management Malta Limited, the company that manages the LABRANDA Riviera Hotel & Spa in Mellieha, Malta was one of a number of entities around the world that was affected by this attack.

The perpetrators of the attack had threatened to publish data that they claimed to be in possession of. At that stage it was impossible to determine if this was true or not. It now results that these perpetrators have indeed started publishing, online, the data of some entities within the FTI Group, including LABRANDA Riviera Hotel & Spa's. It is for this reason that we felt it prudent to make this public communication – despite the fact that a group-wide investigation is still underway.

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

Whether you were affected by a possible publication or only by encryption, 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 28th October, 2021, we were alerted by our colleagues abroad to an incident affecting the internal IT systems of FTI Group on which we also store data. 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 and our customers 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 28th October 2021.

The FTI group immediately made a press release alerting the general public to the fact that we had been attacked (as a group).

Group-wide communications were also sent to employees around the world on 28th October 2021, and from 1st November 2021 onwards at regular intervals.

Without waiting for the results of the investigation to conclude, and as a precaution, we, immediately notified the Maltese Information and Data Protection Commissioner (IDPC) about the situation with the information we had available at that time. The notification was acknowledged on 31st October 2021.

Since then, the ongoing investigation has started to reveal what data from LABRANDA Riviera Hotel & Spa has been exfiltrated by the perpetrators.

What information was involved?

We would like to emphasise 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.

The main categories of data subjects who were affected are our employees – both present as well as past. Some of our customers and third parties (mainly suppliers and partners) were also affected but this, to a much lesser extent. From what we have seen so far, details of suppliers and partners are limited to signatory details when acting in representation of a company.

Personal data of our employees that were affected by the incident could be all data that was provided to us and or generated by us in the course of the employment relationship, e.g. the employee's personnel file. If you were or are employed by us, this could include your full name, telephone number, email and home address, date of birth, bank details for payroll purposes, national security/ID number and CVs (if these were still on file). If you have also provided us with copies of your identity documents, these may also be affected. In some very limited instances, there may also be photos as included in your personnel file and of office-related events.

Although we take various precautions to minimize the personal data that we process, for example by redacting sick leave records of employees to avoid revealing medical information and by processing guest complaints/queries by room number rather than by using the name and surname of the guest(s), there are inevitably occasions when specific individuals are identifiable. In this regard, although very few instances were found, some medical data (eg. generic chronic conditions such as back pain and asthma) may have been exfiltrated by the perpetrators.

We would like to reassure our customers that our booking system is on a separate network and that therefore, the amount of stolen data relating to customers is limited in nature.

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. We are also in close communication with the relevant data protection and investigative authorities to coordinate with them the handling of the incident and offer them our full cooperation.

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

- the attackers 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 attackers or third parties could contact you in order to blackmail you with the stolen or published data (especially if you are an affected employee of ours, past or present).

- if the attackers have obtained copies of your ID cards, it is possible that illegally forged ID card copies could be created using these as a template. We are aware of only few copies of ID cards and passports that have been exfiltrated by the perpetrators and so far, no such documents of customers seem to have been affected.
- using the name, account details and email address information, as well as information you have shared with us (for example, your hobbies and interests), the attackers 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 appropriate authorities (and/or us if you are an employee)
- use complex passwords and change them often
- keep your passwords in a safe place
- avoid opening e-mail attachments that look suspicious
- monitor your bank account and report any unusual activity to your bank

The security of your data is a top priority for us. We can 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 sincerely regret that not only we, on whom the attack was perpetrated, but also our employees and customers have been put in this extremely unpleasant position. We understand that this communication may raise some concerns and further questions. Therefore, if you have any additional questions about this notice, please feel free to contact us **guestrelations.rivierahotel@labranda.com**

We thank you for your collaboration and support,

The Management