КОМИСИЯ ЗА ЗАЩИТА
НА ЛИЧНИТЕ ДАННИ

София 1592,
бул. „Проф. Цветан Лазаров" 2
тел.: 02/915 35 15
факс: 02/915 35 25
e-mail: kzld@cpdp.bg
www.cpdp.bg

DECISION

OF

THE COMMISSION FOR PERSONAL DATA PROTECTION

REG. No. ПАИКД-13-28/2023

SOFIA,……

The Commission for Personal Data Protection (CPDP, the Commission), composed of Chairman [redacted] and members [redacted], [redacted] and [redacted], at a meeting held on 7 February 2024, examined and discussed a notification with ref. No. ПАИКД-13-28/20.07.2023 of a personal data breach under Article 33 of Regulation (EU) 2016/679. BOROVETE I AD, (the company, the controller), submitted the notification. In connection with a "medium level of risk" found, according to the "Methodology for risk assessment of personal data breach", adopted by the Decision of the CPDP of Protocol No. 35/29.09.2022, a documentary check was carried out on the controller. A Finding Report was issued with reference No. ПАИКД-13-28#26(23)/05.02.2024, containing detailed findings regarding the inspection.

I. Factual background

By letter with ref. No. ПАИКД-13-28/20.07.2023 notification of a personal data breach under Article 33 of Regulation (EU) 2016/679 was received from the Controller BOROVETE I AD, Company No. (UIC): 204605689, having its headquarters and registered office in Varna, Primorski District, Postal Code 9006, Sts. Constantine and Helena Resort, administrative building, whose scope of business is: hotel and restaurant management, tour operator and travel agency services, domestic and foreign excursion arrangement, leisure events. In addition, a letter with ref. No. ПАИКД-13-28#5/14.08.2023 was submitted to clarify the facts of the case.

II. Initial analysis of the breach notification and actions taken

1. Nature of the breach

The notification under Article 33 of Regulation (EU) 2016/679 states that on 18 July 2023 the Controller identified a data breach when a responsible employee of the hotel's Reservations Department (Aquahouse Hotel & SPA) found out that a large number of messages have been received to the Company's account on Booking.com. Those messages were received in response to 'phishing' communications to customers concerning reservations made. At the same time,

София 1592,
бул. „Проф. Цветан Лазаров" 2
тел.: 02/915 35 15
факс: 02/915 35 25
e-mail: kzld@cpdp.bg
www.cpdp.bg

telephone calls have also been received concerning the nature of this message and inquiries whether payments were due in respect of current and/or pending reservations. As a result of the breach, phishing messages were sent to hotel customers. The message sent to the individuals (translated into several languages depending on the nationality of the message addressee) contains a fraudulent warning of current or future customer reservations if they fail to confirm their payment card details on a redirecting malicious link sent for this purpose.

According to information provided to the Controller by the IT Security Department of Booking.com the unauthorised access was made through the account of the Company's Executive Director with the username [redacted]

A person who had made a reservation to stay in the hotel contacted a staff member of the Reservations Department asking for assistance in the transfer from the airport to the hotel. In the course of the correspondence, this person sent a file containing information that the employee should have used for the transfer. The employee started a file entitled 'Additional information about the reservation.exe', which contained a malicious code.

The password of the Company's Executive Director for Booking.com was revealed through the infected file, and such password was probably used to access her account and have illegal correspondence with Company's customers.

Citizens of the following countries are affected by the breach: Bulgaria – 4, Romania – 47, Poland – 1, Canada – 1, Russia – 1, Ukraine – 3, Sweden – 1, Switzerland – 1, Türkiye – 1, UAE – 1, Israel – 1, Italy – 6, Germany – 1, UK – 8.

People who replied to the phishing message are from Bulgaria – 1, Poland – 1, Israel – 1, Italy – 1, Russia – 1, Ukraine – 1, Germany – 2, Romania – 12.

The categories of personal data affected by the breach are: names, nationality, e-mail address, telephone number, and with respect to people who replied to the phishing message information about their bank payment card, bank and/or payment account were also affected.

2. Actions taken by the Controller to limit and prevent further breach

- Following the identification of the unauthorised access to the Company's business account on Booking.com, measures have been taken to change passwords and means of authentication to Aquahouse Hotel & SPA account;
- The devices used by the Company for access were scanned for malware;
- Email passwords were changed;
- An additional specialised antivirus program was installed;

София 1592,
бул. „Проф. Цветан Лазаров" 2
тел.: 02/915 35 15
факс: 02/915 35 25
e-mail: kzld@cpdp.bg
www.cpdp.bg

- A standard of operation and automation of a dynamic change of passwords (30 days of activity) was introduced;
- Additional initial staff training at the start of employment was foreseen;
- EDR system (Endpoint Threat Detection and Response System) was integrated; the IT Unit will monitor the system on a 24/7 basis and will response to breakthrough alerts;
- The persons affected by the breach were notified.

The initial analysis of the information in the notification is contained in Report No. ПАИКД-13-28#6/11.09.2023. The level of risk to the rights and freedoms of data subjects was determined in accordance with the 'Methodology for assessing the risk of a personal data breach' adopted by CPDP Decision in Protocol No. 35/29.09.2022. There is a 'medium risk' to the rights and freedoms of the affected individuals. At a meeting, CPDP adopted the following decisions:

1. Carry out a documentary check of the Data Controller.
2. To constitute CPDP as the lead supervisory authority, as the Controller's main or single establishment is located in the territory of the Republic of Bulgaria (Article 56 (1) of the Regulation);
3. To register the case in the Internal Market Information System (IMI), specifying that CPDP is the lead supervisory authority and to provide brief information on the breach and the nationalities of the affected EU citizens. The procedure is initiated by the CPDP on 26 September 2023 and is registered in the Internal Market Information System (IMI) under number IMI 560753. The supervisory authorities of Rhineland-Palatinate, Italy, Romania, Berlin, Bavaria and the Netherlands have identified themselves as concerned supervisory authorities. On 17 April 2024, the Commission for Personal Data Protection published in IMI a draft decision in relation to Notification No. ПАИКД-13-28/20.07.2023 submitted by the controller BOROVETE I AD. No reasoned and relevant objections were raised by the deadline for the submission of objections (expired on 15 May 2024) by the concerned supervisory authorities.

III. Analysis of the documents and opinions submitted in connection with the inspection

In order to fully clarify all the relevant circumstances of the case, additional information was requested from BOROVETE I AD by letter with ref. No. ПАИКД-13-28#10/02.10.2023.

София 1592,
бул. „Проф. Цветан Лазаров" 2
тел.: 02/915 35 15
факс: 02/915 35 25
e-mail: kzld@cpdp.bg
www.cpdp.bg

By letter with ref. No. ПАИКД-13-28#14/23.10.2023, the Controller provided the requested information.

In connection with the breach, additional information was also requested from Booking.com by letter ref. No. ПАИКД-13-28#19/15.12.2023. Booking.com provided the requested information via IMI through the Dutch supervisory authority, by a letter with ref. No. ПАИКД-13-28#24/19.01.2024.

The Controller specifies that the personal data protection is ensured in accordance with the requirements of Regulation (EU) 2016/679. The guidelines, opinions and recommendations of the European Data Protection Board and the implementing decisions of the European Commission are observed.

In accordance with the requirements of Article 24(2) of Regulation (EU) 2016/679, the Controller has adopted an Instruction (internal rules) on measures and means to protect personal data collected, processed, stored and provided by Borovete I AD. Privacy Policy and Information Security Policy have also been approved.

The Information Security Policy is part of the internal corporate documentation approved for the purposes of ensuring the compliance of the Company's activities with the requirements arising from European and national regulations in the field of personal data protection, as well as the best practices in the field of cybersecurity. The staff has been familiarized with the Information Security Policy and with other internal corporate documents. A copy of such documents has been sent to the heads of all Company's departments and thus all employees have been informed of the objectives and texts of the internal documents adopted. The heads of departments are, in their turn, engaged to bringing the corporate documents adopted, including the Information Security Policy, to the attention of the staff. The Controller has provided evidence that the employees are familiar with internal corporate documents.

The Controller has developed an instruction to regulate the creation of accounts on online tour operator platforms, and such instruction shows which employees may have accounts on online platforms used by the Controller.

The organisation in the company is set up so that employees of the Reservations Department have their own profiles on the online platforms they use.

The heads of departments carry out the overall monitoring of compliance with the obligations arising from all internal orders and instructions.

The control of compliance with the internal rules and procedures for dealing with accounts and passwords is also carried out directly by all the staff in the IT Department, who have software generating log files allowing real-time tracking of all processes carried out by the Company's

София 1592,
бул. „Проф. Цветан Лазаров" 2
тел.: 02/915 35 15
факс: 02/915 35 25
e-mail: kzld@cpdp.bg
www.cpdp.bg

computers. In this regard, all employees of the Company's IT Department report to the head of department any irregularities detected in the use of data, including unauthorised access from a personal computer to accounts of other employees with other computers, including through access to third-party service providers platforms.

The Controller reports that access to information assets is provided on a need-to-know basis, and that access control is carried out directly by the heads of departments. The overall business of the Company complies with this principle.

All databases containing personal data are accessed only by employees expressly authorised by the Executive Director of the Company and solely for the performance of their duties.

The Company's employees work through individual accounts with individual passwords for the computer and system devices, with no access to the data files of any other employee, department, or access to PCs or internal accounts of other employees in the same or other department. The creation of these accounts ensures the proper functioning of the Company's business operations involving tourist accommodation and the provision of hotel services to customers.

All employees of the Company are informed of compliance with this principle as soon as they start working in the relevant department or in the event of changes in the Company's policies.

It is clear from the information provided by Booking.com that when partners register on the platform, they are given access to the Extranet on Booking.com, where they can manage all matters concerning their facility, such as room prices, room availability, discount offers, reservations made, the partner's contact details, adding or deleting 'trusted devices' allowed to enter the Extranet, etc. The Extranet allows a partner to communicate directly with the guests via a partner-guest communication tool and to see selected personal details of guests who made a reservation with that partner. A partner does not have access to the guest's email address via Extranet, but only to the alias of the guest's email address. Access to the Extranet is provided to partners on a need-to-know basis and partners are informed and contractually bound to keep their login credentials secret. Access to Extranet is protected by technical and organisational security measures such as mandatory two-factor authentication, which cannot be disabled. It is possible to create accounts with different access rights so that to ensure that certain actions can only be performed by Extranet users having root privileges. These are the so-called 'child accounts' (subaccounts). Child accounts are accounts linked to the partner's main Extranet account, but have their own username and password. Passwords are required to include a minimum of 10 characters, including upper and lower case letters and digits.

София 1592,
бул. „Проф. Цветан Лазаров" 2
тел.: 02/915 35 15
факс: 02/915 35 25
e-mail: kzld@cpdp.bg
www.cpdp.bg

When a new session is started, Booking.com requests the Extranet user to authenticate itself by two-factor authentication at least once every 15 days. In addition, Extranet sessions have a life of 7 days in an active session or 2 hours when they are inactive; this means that every 7 days or 2 hours, depending on the activity of the session, the partner may be required to log in again.

As a result of the internal investigation, Booking.com identified ten 'child accounts' in the Extranet account of the partner Aquahouse Hotel & SPA, all such accounts having root privileges. It can therefore be inferred that the Controller has not taken action to limit the powers of its staff to the Extranet account.

In this case, it can be concluded, and this was confirmed by Booking.com, that following the start of the malicious executable file, the person acting maliciously obtained access to information in the partner's web browser during a session where the partner had already entered its account by means of two-factor authentication. Subsequently, the person acting maliciously used the compromised account and sent messages on behalf of the Controller requesting payment card data to be provided to a relevant redirecting malicious link.

The Controller reports that data to which the Company and its authorised employees have access on Booking.com are the client's name and reservation details (stay, type of room, number of guests). The storage, including retention periods for personal data of Company's customers on Booking.com, is determined by the rules of the platform, and Company's employees have only single access to the data accessible on the platform after the performance of their hotel accommodation duties. In this context, the Company stores no data of its customers on Booking.com after their reservation is made.

Booking.com states that customers' personal data are stored in partners' accounts as follows:

- For the time prior to the date of accommodation of the person who made the reservation and during the stay of this person in the partner's accommodation facility;
- The alias of the email address of the person who made the reservation is subject to deactivation two months after the departure date. Partners may send communications only from the moment of booking to seven days after the departure date or seven days after cancellation;
- Customer's personal data are not displayed on the partner's Extranet after 30 days from the departure date.

София 1592,
бул. „Проф. Цветан Лазаров" 2
тел.: 02/915 35 15
факс: 02/915 35 25
e-mail: kzld@cpdp.bg
www.cpdp.bg

Booking.com also states that following the investigation it was established that the person who acted maliciously had not accessed credit card data from the Controller's Extranet account.

The Company's internal inspection did not identify any damage or abuse of the personal data of the customers who communicated with the unauthorised person.

All affected hotel guests were duly accommodated. No person has made any claim, in law or in fact, against the hotel. All guests were addressed with compliments by the team of Aquahouse Hotel & SPA, their reservations were prepaid via the Booking.com platform, and the latter has not reported any information about clients' claims or claimed damages.

The Controller reports that the Company's organisation with regard to the collection, storage and processing of personal data is as follows:

Physical protection:

- Only authorised staff of the department to which the computers have been made available have physical access to the individual computers. This means that the computers in the Reception Department are only accessible by staff of this department by means of an individual password of each employee;
- Aquahouse Hotel & SPA has a security alarm system, a video surveillance system, a back-up power supply, a fire alarm and fire protection system, air conditioning of the premises where hardware devices are located;
- The Company has a personal data breach response team;
- Access to all hotel rooms, staff entrances, administrative offices, parking areas and the premises in which the hotel server is located is controlled;
- The hotel managed by the Company has 24/7 physical security and an electromechanical hotel patrol system.

Personal protection:

- The Company's employees have appropriate personal data protection training;
- When dealing with external providers, verification of the identity of the person who will provide the service in question;
- Personal protection measures include access to personal data only by persons whose duties or specifically assigned tasks require such access, subject to the "need-to-know" principle;
- Arrangements and measures are in place to prevent disclosure of information to third parties;

София 1592,
бул. „Проф. Цветан Лазаров" 2
тел.: 02/915 35 15
факс: 02/915 35 25
e-mail: kzld@cpdp.bg
www.cpdp.bg

- The levels of access to the different categories of personal data are regulated and differentiated by the approved Instruction;
- The staff members sign a declaration of non-disclosure of personal data to third parties.

Documentary protection:

- Access to personal data records is governed and regulated by an instruction;
- For each of the personal data registers a retention period is set which complies with the relevant regulatory requirements;
- A procedure is in place for the destruction of personal data in paper and electronic form.

Protection of automated information systems and/or networks:

- The Company's network is not specifically certified in terms of information security. However, under the approved rules, the Company uses technical devices and software which is in line with international standards;
- Access to the Company's IT systems is regulated through usernames and passwords, and the different accounts have different levels of access;
- The software products used by the Company allow logging of access and actions carried out, and any act of entering, modifying, deleting data from hotel customer registers can be traced;
- Archives are produced at operating system and file level;
- Measures have been taken to ensure the reliability and integrity of the systems: back-up power supply of servers, isolation of the server from the internet database, separation of the physical integrity of servers in separate, dedicated double-locked premises, separation of network into segments;
- Rules are in place for regular technical maintenance of computer equipment and systems;
- The Company uses TLS cryptographic protocols for its email customer, thus ensuring the confidentiality, integrity and authenticity of the data;
- The Company has also configured the maintenance of TLS cryptographic protocol for its web server;
- All platforms and software used by Company's employees apply control by time-limiting user sessions;

София 1592,
бул. „Проф. Цветан Лазаров" 2
тел.: 02/915 35 15
факс: 02/915 35 25
e-mail: kzld@cpdp.bg
www.cpdp.bg

- Some of the Company's employees use external connectivity to databases through VPN;
- The process of creating copies and back-ups (autosave) is automated at server and storage level (storage sites);
- Destruction, deletion and erasure of data carriers by designated staff members is controlled by the implementation of a specific Procedure for destruction of personal data in paper and electronic form.

The Controller states that it has notified all persons affected by the breach.

It is found that within 72 hours of becoming aware of the breach, the Controller notified the supervisory authority, the CPDP, in accordance with Article 33 of Regulation (EU) 2016/679.

All the documents provided by BOROVETE I AD for the purposes of the inspection were enclosed in case file with ref. No. ПАИКД-13-28/20.07.2023.

IV. Legal analysis:

Regulation (EU) 2016/679, which applies as of 25 May 2018, is the legal act laying down rules on protection of personal data of natural persons with regard to their processing. The Regulation builds on the former data protection regime introduced by Directive 95/46/EC, transposed into the Bulgarian Personal Data Protection Act of 2002, while taking into account the dynamics of the development of new technologies and of personal data processing activities.

According to the legal definition set out in Article 4(12) of the Regulation, a '*personal data breach*' is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The specific breach consists of starting a malicious executable file by a Controller's employee, resulting in a third party having accessed the Executive Director's account on Booking.com. This shows the employee's insufficient awareness and caution, despite the training on data protection. In addition, the Controller has not taken sufficient technical and organisational measures to limit the access rights of its employees on Booking.com, although this platform provides such limitation as an option, and thus the third party has easily accessed the account of the Controller's Executive Director. Personal data of 80 (eighty) persons were affected by the breach: names, nationality, email address, telephone number, including financial data of 20 (twenty) natural persons who replied to the phishing message such as details of a bank payment card or bank account or account with a payment service provider. In this case, Article 5(1)(f) of Regulation (EU) 2016/679 has been infringed, namely the data were processed in a manner that

София 1592,
бул. „Проф. Цветан Лазаров" 2
тел.: 02/915 35 15
факс: 02/915 35 25
e-mail: kzld@cpdp.bg
www.cpdp.bg

fails to ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, subject to the principle of 'confidentiality'.

On the other hand, as mitigating circumstances, it should be taken into account that the Controller notified the CPDP without undue delay, within 72 hours of becoming aware of the breach. Data subjects are informed by email. Additional actions have been taken to prevent such incidents by installing an additional specialised antivirus program, actions to ensure additional initial training for new hires, and EDR system (Endpoint Threat Detection and Response System) has been integrated.

It is the responsibility of the Controller to take the appropriate technical and organisational measures to protect data and to apply mechanisms to monitor the implementation of such measures, and thus the Controller could demonstrate compliance with the rules of the Regulation.

CPDP has a margin of discretion, in accordance with the powers entrusted to it, to determine which corrective powers referred to in Article 58(2) of Regulation (EU) 2016/679 to exercise. The assessment is based on considerations of appropriateness and effectiveness, taking into account the specificities of each individual case and the extent to which the interests of the specific data subjects are affected, as well as the public interest. The powers referred to in Article 58(2), other than that under subparagraph (i), have the nature of coercive administrative measures designed to prevent or put an end to a breach, thereby achieving proper conduct in the area of personal data protection.

When applying the appropriate corrective measure under Article 58(2) of the Regulation, account shall be taken of the nature, gravity and consequences of the breach, as well as any mitigating and aggravating circumstances. The assessment of what measures are effective, proportionate and dissuasive in each individual case also reflects the objective pursued by the chosen corrective measure of preventing or putting an end to the breach or penalising the unlawful conduct, or both, as provided for in Article 58(2)(i) of Regulation (EU) 2016/679.

Having regard to the facts of this case and the results of the documentary check which unequivocally confirmed the facts and circumstances of the case, taking into account the nature, gravity and consequences that could arise from the data breach, and after reviewing and analysing all the documents gathered in the administrative case file, and in order to prevent further such breaches, the Commission for Personal Data Protection adopted the following

София 1592,
бул. „Проф. Цветан Лазаров" 2
тел.: 02/915 35 15
факс: 02/915 35 25
e-mail: kzld@cpdp.bg
www.cpdp.bg

D E C I S I O N :

1. Pursuant to Article 58(2)(b) of Regulation (EU) 2016/679, for breach of Article 5(1)(f) in conjunction with Article 32(1)(b) and (d), issues a ***reprimand*** to BOROVETE I AD in connection with notification of a personal data breach under Article 33 of Regulation (EU) 2016/679 with ref. No. ПАИКД-13-28/20.07.2023.
2. Pursuant to Article 58(2)(d) of Regulation (EU) 2016/679, for breach of Article 5(1)(f) in conjunction with Article 32(1)(b) and (d) of Regulation (EU) 2016/679, ***orders*** the Data Controller BOROVETE I AD to:

   2.1 Take actions to restrict the rights of its employees on Booking.com, in order to comply with the 'need-to-know' principle; and

   2.2 To draw up a plan for periodic training of employees in the area of personal data protection, including points concerning phishing messages. Periodic phishing drills should be conducted to increase employees' vigilance.

The order under paragraph 2.1 shall be complied with **within 1 (one) month from the entry into force of the decision,** after which, within 14 (fourteen) days, the Controller shall notify the Commission for Personal Data Protection of its implementation by submitting the relevant evidence.

The order under point 2.2 shall be complied with **within 3 (three) months from the entry into force of the decision**, after which, within 14 (fourteen) days, the Controller shall notify the Commission for Personal Data Protection of its implementation by providing relevant evidence, including the training materials to be used for the training.

This Decision of the Commission for Personal Data Protection and may be appealed against before Varna Administrative Court within 14 (fourteen) days of its receipt.

CHAIRPERSON: [redacted]

MEMBERS: [redacted]

[redacted]

[redacted]