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

COMMISSION FOR PERSONAL DATA PROTECTION

FINAL DECISION
Ref. № ПАИКД-13-28/2022
IMI A56 424363

The Commission for Personal Data Protection (CPDP, the Bulgarian SA) has initiated a procedure under Article 56 (1) of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) in its capacity as supervisory authority competent to act as the lead supervisory authority for cross-border processing carried out by a controller established in the Republic of Bulgaria. The procedure was initiated by the CPDP on 2 September 2022 in the Internal Market Information System with number IMI A56 424363.

In connection with the above, at a plenary meeting held on 26 October 2022, the Commission, composed of: [redacted] (Chairperson) and [redacted] and [redacted] (Members), considered a Statement of Findings, drafted by the Legal Analysis, Information and Control Directorate.

I. The Facts

The data controller LockTrip Ltd., with a National Identification Number: 204752244 (the company, the controller), submitted a personal data breach notification with the CPDP (№ ПАИКД-13-28/09.06.2022 г. pursuant Article 33 GDPR. The controller's single place of establishment is at 78 Alexander Malinov Blvd., Mladost 4 Residential Area, 1799, Sofia, Bulgaria. The controller is a company that provides services, related to software development and consultancy in the field of information technology. According to the information received, the personal computer of an employee of the controller (a call centre operator) was compromised by logging in to a public Wi-

Fi network. As a result of the breach, passwords for access to shared private spaces and platforms of partners of LockTrip Ltd. were leaked.

II. Actions taken by the CPDP after receiving the notification:

Pursuant to Article 62 of the Rules on the Activity of the Commission for Personal Data Protection and Its Administration (RACPDPA), the data breach notification was registered in the relevant internal register. Since the initial information in the notification form did not contain the minimum information required under Article 33 (3) GDPR, it was subsequently requested in the course of the administrative proceedings by letter (№. ПАИКД-13-28#1/16.06.2022 г.). The controller provided additional information by letters. №. ПАИКД-13-28#2/20.06.2022 г.#2 and №. ПАИКД-13-28#3/30.06.2022 г. Pursuant Article 63 of the RACPDPA, the notification was analysed on the basis of the Methodology for Risk Assessment upon a Personal Data Breach, adopted with a Decision of the Bulgarian SA of 24 June 2021. Further to the above, following a Decision of the CPDP from 6 July 2022a document inspection was carried out in connection with the breach which had been brought to the attention of the supervisory authority.

The main task of the inspection was to ascertain the facts and circumstances related to the breach, the technical and organisational measures that had been taken before the incident, and to identify the possible omissions that had made possible for the breach to occur. Another task of the inspection was to ascertain the measures taken to mitigate the possible adverse effects and minimise the possibility of such an incident to occur again.

III. Analysis of the information provided in connection with the notification received and the actions taken:

1. Nature of the breach:

According to the information provided on 5 June 2022 the controller's monitoring systems, as well as its employees, detected suspicious and unauthorised activity. An on-duty employee was alerted by email from a partner platform of LockTrip Ltd. of a misapplied operating algorithm for hotel bookings. After the case was scrutinised, it was found that data security had in fact been breached. It was established that the personal computer of an employee of the controller (a call centre operator) was compromised by logging in to a public Wi-Fi network. As a result of the breach, passwords for access to shared private spaces and platforms of partners of LockTrip Ltd. including: Agoda, Booking, Dida Travel, DOTW, Escalabeds, Expedia, GetARoom, Go Global, GRNconnect, Hotelbeds, HotelDo, Hotelston, Hotusa, LotsOfflotels, Miki Travel, RateHawk, RTS, Stuba, SunHotels, TBOHolidavs, TotalStay, WelcomeBeds, were leaked.

There is no information showing and suggesting that the integrity of the data was compromised. The third party who committed the unauthorised access retrieved all data that they have accessed.

The number of personal data records affected by the breach is 2,199 unique records.

The number of data subjects (natural persons) affected by the breach is 2,025 data subjects.

If broken down by type of bookings: successful bookings, cancelled bookings, and attempted bookings.

Bookings where the arrival date is prior to the incident (5 June 2022): 2,046 unique emails from natural persons;

Bookings where the arrival date is after the incident (5 June 2022): 182 unique emails from natural persons.

The controller points out that 19 (nineteen) of the bookings affected indicated that there could be children aged under 14 will check in. Two of all the bookings affected specified the children's names and age.

The following categories of personal data were affected by the breach: names; address; email address; IP address from which the booking was made.

The persons affected by the breach include both EU citizens and third-country nationals.

Number of persons affected broken down by the value of the booking:

Bookings for an arrival date after the 5 June 2022 incident:

- from EUR 0 to EUR 100: 14 bookings;
- from EUR 100 to EUR 500: 70 bookings;
- from EUR 500 to EUR 1,000: 42 bookings;
- over EUR 1,000: 56 bookings.

Bookings for an arrival date before the 5 June 2022 incident (past bookings):

- from EUR 0 to EUR 100: 537 bookings;
- from EUR 100 to EUR 500: 893 bookings;
- from EUR 500 to EUR 1,000: 265 bookings;
- over EUR 1,000: 351 bookings.

In the data breach notification, the controller argues that the presence of personal data, such as names, address, email address and IP address from which the booking was made, could not be used for financial abuse or transactions.

The controller reports that users of the LockTrip Ltd. booking system, depending on the preferred payment method, are redirected to an external encrypted link of one of two payment processors: Stripe or CoinPayments. The employees of LockTrip Ltd. do not have access to sensitive information like bank card number or CVV/CVC code, while the respective booking is in progress.

The notification indicates that the breach has a significant potential impact on the data subjects whose names, addresses and forthcoming booking were leaked because they may be targeted by phishing attacks requiring additional payments for a booking or the submission of copies of an identity document or a payment instrument. It is possible that data subjects provide this information as it is normally associated with visits at hotels. The controller is of an opinion that the data subjects in question may be targeted by other attempts at criminal activity, considering that they are not present at their home. However, that would be s hardly likely because it is quite possible that the potential third party is not present in a country where the data subject's permanent address is or in a country in which the data subject will reside during their booking.

LockTrip Ltd. notes that the breach has a limited potential impact on the data subjects whose names, addresses and past booking were leaked, however they could be targeted by phishing attacks requiring extra payments for a certainstay, but the effect of something like that could be less significant owing to the lower likelihood of the data subject being misled.

2. Designating the CPDP as the Lead Supervisory Authority

In addition, responding to the CPDP's query № ПАИКД-13-28#1/16.06.2022 г., by letter with № ПАИКД-13-28#6/20.07.2022 г. LockTrip Ltd. provided particular information regarding:

The number of persons who indicated their country of origin in their registration (applicable to bookings done before 5 June 2022):

AE (United Arab Emirates) 239; AM (Armenia) 1; AR (Argentina) 13; AT (Austria) 144; AU (Australia) 48; AZ (Azerbaijan) 1; BA (Bosnia and Herzegovina) 32; BD (Bangladesh) 1; BE (Belgium) 70; BG (Bulgaria) 396; BO (Bolivia) 3; BR (Brazil) 20; BS (Bahamas) 3; BY (Belarus) 9; CA (Canada) 96; CH (Switzerland) 57; CL (Chile) 24; CO (Colombia) 13; CR (Costa Rica) 14; CY (Cyprus)27; CZ (The Czech Republic) 15; DE (Germany) 222; DK (Denmark) 22; DO (Dominical Republic) 10; EE (Estonia) 1; EG (Egypt) 16; ES (Spain) 141; FI (Finland) 29; FR (France) 108; GB (United Kingdom) 350; GE (Georgia) 3; GI (Gibraltar) 2; GM (Gambia) 3; GR (Greece) 16; T (Guatemala) 5; HK (Hong Kong) 8; HN (Honduras) 11; HR (Croatia) 422; HU (Hungary) 14; ID (Indonesia) 20; IE (Ireland) 69; IL (Israel) 10; IM (Isle of Man) 5; IN (India) 97; IR (Iran) 7; IS (Iceland) 3; IT (Italy) 90; JE (Jersey) 16; JM (Jamaica) 2; JO (Jordan) 8; JP (Japan) 22; KE (Kenya) 2; KH (Cambodia) 2; KR (South Korea) 4; LB (Lebanon) 1; LI (Liechtenstein) 1; LK (Sri Lanka) 4; LT (Lithuania) 3; LV (Latvia) 3; LY (Libya) 2; MA (Morocco) 6; MC (Monaco) 27; MD (Moldova) 1; ME (Montenegro) 10; MK (North Macedonia) 4; MN (Mongolia) 1; MO (Macao) 5; MT (Malta) 17; MX (Mexico) 30; MY (Malaysia) 17; NG (Nigeria) 5; NL (The Netherlands) 160; NO (Norway) 18; NP (Nepal) 4; NZ (New Zealand) 9; PA (Panama) 6; PE (Peru) 9; PH (Philippines) 3; PK (Pakistan) 3; PL (Poland) 21; PR (Puerto Rico) 4; PT (Portugal) 31; PY (Paraguay) 4; QA (Qatar) 24; RO (Romania) 14; RS (Serbia) 54; RU (Russia) 32; SA (Saudi Arabia)

2; SD (Sudan) 2; SE (Sweden) 82; SG (Singapore) 19; SI (Slovenia) 12; SK (Slovakia) 1; SV (El Salvador) 3; TH (Thailand) 44; TN (Tunisia) 10; TR (Turkey) 33; TW (Taiwan) 1; TZ (Tanzania) 1; UA (Ukraine) 14; US (The United States of America) 630; UY (Uruguay) 1; VE (Venezuela) 3; VN (Vietnam) 14; ZA (South Africa) 18.

and

the number of persons who indicated their country of origin in their registration (applicable to bookings after 5 June 2022):

AE (United Arab Emirates) 4; AT (Austria) 4; AU (Australia) 12; AZ (Azerbaijan) 1; BA (Bosnia and Herzegovina) 4; BE (Belgium) 7; BG (Bulgaria) 24; CH (Switzerland) 1; CO (Colombia) 1; CZ (The Czech Republic) 2; DE (Germany) 15; DK (Denmark) 4; EG (Egypt) 3; ES (Spain) 4; FR (France) 2; GB (United Kingdom) 40; HR (Croatia) 84; IE (Ireland) 4; IN (India) 1; IR JE (Jersey) 1; KR (South Korea) 1; MY (Malaysia) 1; NL (The Netherlands) 8; NO (Norway) 1; NZ (New Zealand) 3; PK (Pakistan) 1; PL (Poland) 1; PT (Portugal) 3; QA (Qatar) 2; RS (Serbia) 9; SE (Sweden) 2; SG (Singapore) 3; SI (Slovenia) 2; SK (Slovakia) 1; TN (Tunisia) 1; US (The United States of America) 11; ZA (South Africa) 18.

The EU citizens affected by the breach are 2,108, including 420 Bulgarian citizens.

The third-country nationals affected by the breach are 2,423.

The information as additionally received was presented at a plenary meeting of the Bulgarian SA on 27 July 2022 (Report № ПАИКД-13-28#7/25.07.2022 г.), pursuant to which the following decisions were adopted as recorded in Minutes of Proceedings before the CPDP № 31 of 27 July 2022:

1. The CPDP will assume the role of the lead supervisory authority as the main establishment or the single establishment of the controller is within the territory of the Republic of Bulgaria (Article 56 (1) GDPR.

2. The case would be registered in the Internal Market Information System (IMI), stating that the CPDP would assume the role of the lead supervisory authority, and brief information will be provided about the breach and the nationalities of the affected EU citizens.

The Commission for Personal Data Protection assumed the role of the lead supervisory authority under procedure IMI A56 424363. At the time of the drafting of the present decision, the supervisory authorities of Rhineland-Palatinate, the Netherlands, Lower Saxony, Italy, France, Brandenburg, Norway, Ireland, Austria, Belgium, Estonia, Romania, Sweden, Slovakia, Denmark, Finland and Spain have identified themselves as concerned supervisory authorities (CSAs).

On 2 December 2022, the Bulgarian SA launched an Article 60 procedure – draft decision IMI A60DD 464486. Within the established deadline only a comment by the Polish SA was received, stating that the authority was satisfied with the draft decision.

3. Actions taken by the data controller to restrict the breach:

- The data subjects were notified (by email) in order to be more vigilant about any messages sent to them in connection with their booking registrations. The affected persons were notified by email of the security breach. Information, regarding the type of data to which the third parties had gained access to, the way in which that data could be used against the data subjects *(phishing attacks, for example)*, as well as how they could protect themselves. Also, on 8 June 2022 the Managing Director of LockTrip Ltd. published an official announcement in the LockTrip Telegram channel at the Telegram messenger platform, whose members are long-term investors, supporters and fans of the project;
- The compromised profile of the employee of the controller, as well as their personal computer were localised;
- The compromised profile of the employee of the controller was temporarily deactivated, and its access to all shared private spaces and partner platforms were blocked;
- The passwords for access to all shared private spaces and partner platforms were changed;
- An additional two-factor security verification for granting access to all shared private spaces and partner platforms was activated;
- Reinstalling and deleting all the information stored on the hard disk of the compromised personal computer; The employee of the controller whose personal computer had been compromised was provided with a new wireless internet router in order to enhance security.

4. Actions taken by the data controller to prevent a recurrence of the breach:

- Establishment of a new internal policy and procedure for security enhancement;
- Implementation of new methods for monitoring access to the shared private spaces and partner platforms;
- Delivery of internal technical training to all employees in order to raise their awareness of cyber security.

The initial analysis of the information provided with the notification was covered in a Report № ПАИКД-13-28#4/05.07.2022 г. The severity of the risk to the rights and freedoms of data subjects was determined according to the Methodology for Risk Assessment upon a Personal Data

Breach, adopted with a Decision of the Bulgarian SA from 24 June 2021. The rights and freedoms of the persons affected were found to be at “medium risk”.

IV. Analysis of the evidence presented in connection with the document inspection carried out:

In order to fully clarify all the circumstances relevant to the case, additional information was requested from LockTrip Ltd. by the CPDP with letters. № ПАИКД-13-28#8/26.07.2022 г. and № ПАИКД-13-28#15/02.09.2022 г.

In connection with the additional information requested, an exchange of correspondence took place between the Bulgarian SA and LockTrip Ltd. The controller requested an extension of the legally defined period of time for the provision of the abovementioned information: letters from LockTrip Ltd. № ПАИКД-13-28#9/27.07.2022 г.; № ПАИКД-13-28#10/02.08.2022 г.; № ПАИКД-13-28#16/12.09.2022 г. and letters, sent by the CPDP. № ПАИКД-13-28#12/03.08.2022 г.; № ПАИКД-13-28#18/26.09.2022 г.;. № ПАИКД-13-28#19/27.09.2022 г.

The information as presented below was provided by the data controller with the following letters № ПАИКД-13-28#14/17.08.2022 г.; № ПАИКД-13-28#17/14.09.2022 г.; № ПАИКД-13-28#20/29.09.2022 г.; № ПАИКД-13-28#21/03.10.2022 г.:

- In its response with letter № ПАИКД-13-28#14/17.08.2022 г., the controller indicated that the cause of the incident had been identified as a result of an internal inspection that has been carried out. An employee of LockTrip Ltd., who was subsequently identified, had logged in to a public Wi-Fi network, and the LockTrip’s systems were therefore made available externally. The inspection has furthermore identified the individual whose personal computer had been compromised after the malicious attack, where shared private spaces were subjected to unauthorised access, and where partner portals of LockTrip Ltd. had been subjected to unauthorised access. Written evidence ascertaining the conduct of the internal inspection (reports, conclusions, etc.) was not presented together with the official statement of the controller.
- With regard to whether the controller delivers training in personal data protection to its employees and, hence, to present evidence, the controller stated that before taking the respective position, the persons who are responsible for safeguarding and processing personal data have the obligation not to disclose the personal data to which they have access to and not to share critical information with each other and with third parties. Follow-up training sessions of the staff are held periodically so as to ensure familiarity with the regulatory framework, the potential risks to data security, as well as the measures for their reduction. Evidence was not presented.
- The controller notes that by the date of the breach they did not consider that requirements under Regulation (EU) 2016/679 were available for analysing the risk to the rights and

freedoms of natural persons with regard to the processing of their data. Therefore, no such analysis was carried out before the data breach. A Data Protection Impact Assessment for the Personal Data Processed by the Controller LockTrip Ltd. was presented with letter № ПАИКД-13-28#14/17.08.2022 г.

- With regard to the conduct of a prior audit of the information systems, the controller states that a DEV team checks the information systems on a weekly basis, monitoring a series of records, indicators and values. They are intended to establish whether the overall system functions as intended, whether any of its components exhibits a deviation or technical failure and, last but not least, whether there is a breach of security, the operating algorithm and the authorised access. The controller did not specify whether the checks involve an analysis and audit of the technical and organisational measures taken for the protection of personal data when using remote access, because the present case concerns a security breach that occurred precisely for this reason.

- Regarding the matter of enclosing the evidence collected and analysed of each fact established, namely paper and/or electronic documents (including rules, procedures, instructions, official statements, print screens, etc.), LockTrip Ltd. pointed out in their official statement: "As the CPDP has not thus far requested the so-called "server logs", nor a request for their retention has been sent, their 40-day retention period had expired by 26 July 2022. Accordingly, no collected and analysed evidence whatsoever can possibly be provided as of today's date. All data, concerning the breach were perused and analysed in real time on our server. The reason why nothing is retained is that the 'server logs' in question contain sensitive information which is archived over a definite time interval in order to safeguard its security."

Considering the fact that the additional information sent to the Bulgarian SA (letter № ПАИКД-13-28#14/17.08.2022 г.) does not make it possible to clarify all facts and circumstances relevant to the present case, the controller was requested again to present written statements (letter with № ПАИКД-13-28#15/02.09.2022 г.), enclosing the relevant documents and evidence ascertaining the actions taken with regard to:

- LockTrip Ltd.'s Rules on employees' access to the company's platforms;

- What alert systems have been implemented by the company for attempts of unauthorised access at infrastructure level and at employee level;

- Training materials on personal data protection, compiled and intended for the company's employees, both with regard to their initial training and to the follow-up periodical trainings;

- Written evidence of training in personal data protection delivered to the employee whose personal computer was subjected to a malicious attack (for example, a certificate, an attendance form, a test form, etc.), as well as a declaration by the said employee to the effect that

they have been trained and made familiar with the company's rules concerning personal data protection;

- Considering the information that the personal data are processed in electronic form on computers located at the employees' homes, a specification of the location where the personal data of the data subjects affected by the breach are stored and processed should be provided;

- In connection with the information submitted by LockTrip Ltd. that the 'server logs' had not been requested by the CPDP thus far nor a request had been made for their retention and that they had been destroyed due to the expiration of the period of 40 days , the controller's attention was drawn to the fact that, pursuant to Article 5(1)(f) in conjunction with Article 5(2) of Regulation (EU) 2016/679, the controller is responsible for and is expected to be able to demonstrate (principle of "accountability") that they process the data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (principle of "integrity and confidentiality"). Considering the above, the Bulgarian SA explained that LockTrip Ltd. had to demonstrate compliance with the principles of 'accountability, integrity and confidentiality' with regard to the particular incident that had occurred. Since the CPDP did not have specific information on the internal documents by which the controller was able to demonstrate compliance with the principles at its disposal, it could only point out that LockTrip Ltd. was supposed to present the evidence they had collected and analysed (after the conduct of the appropriate internal inspection) of each fact established in connection with the incident: paper and/or electronic documents (including rules, procedures, instructions, official statements, print screens, etc.. The controller was reminded that the abovementioned, as described had already been requested by letter № ПАИКД-13-28#15/26.07.2022 г. and by that point the controller is invited again to present the appropriate relevant evidence.

- Furthermore, the controller's attention was drawn to the fact that, according to Article 24 (1) and (2) of Regulation (EU) 2016/679, it is expected to take into account the nature, scope, context and purposes of the specific personal data that they process. In this regard, the controller must consider the risks of varying likelihood and severity for the rights and freedoms of natural persons, responding to such risks by implementing appropriate technical and organisational measures, and has also be able to demonstrate their implementation. Considering the above, the Bulgarian SA needs to be informed of the technical and organisational measures for data protection (referred to in the relevant internal documents) that had been taken before the incident occurred.

In response to the CPDP's letter, the controller provided additional information and documents (by letter № ПАИКД-13-28#17/14.09.2022 г.):

- The controller presented *Rules on LockTrip Ltd. Employees' Access to Internal Information Systems and Partner Portals of the Organisation*, endorsed by the Managing Director

of the Company (Ref. No. 20210108 of 1 August 2021). No evidence has been provided as to how employees were made aware of the Rules in question.

- A document entitled *Monitoring of and Access to Internal Information Systems and Shared Partner Platforms* was presented, as endorsed by the Managing Director of the company (Ref. No. 20210108-3 of 1 August 2021). The document, which every employee, including the members of the operational department of LockTrip *(call centre operator and contact centre manager team)* are obliged to observe and comply with, lays down the methods for monitoring, and the access at architecture and agent level to the internal information systems and shared partner platforms. No evidence has been provided as to how employees were made aware of the document in question.

- With regard to the training materials requested by the CPDP that had been used to familiarise employees with the rules on personal data processing, the controller presented a document entitled *European Policies and Personal Data Protection Regulation*, which describes the general provisions introduced with Regulation (EU) 2016/679. The document ends with open-ended questions for self-study:

  - ✓ When does the *GDPR* enter into force?
  - ✓ What does the Personal Data Protection Act regulate in the Republic of Bulgaria?
  - ✓ Define *personal data*.
  - ✓ Which are the areas of data processing specified in the *GDPR*?
  - ✓ What is the other name of the right to erasure?
  - ✓ Which is the most important principle of the *GDPR*?

A further examination and analysis of the content of the document establishes that it does not contain rules, which employees are supposed to follow when processing personal data in connection with the specific activity of LockTrip Ltd. No evidence was presented in order to ascertain that the employees had been made familiar with the document or that they had provided an answer to the open-ended questions for self-study.

- The controller presented *Internal Work Rules of LockTrip Ltd.*, intended to regulate matters related to work discipline, an appropriate organisation of work, and the full and effective utilisation of working hours. In terms of content, the provisions of the document presented as evidence are irrelevant to the present case concerning the matters of personal data processing. As the document itself states, the Rules were drawn up pursuant of Article 181 of the Labour Code.

- The controller presented Order No. 0000005 of 6 December 2021, issued pursuant to Ordinance No. 15 of 31 May 1999 on the Terms, Procedure and Requirements for the Development and Introduction of Physiological Patterns of Work and Rest during Work and Article 151 of the Labour Code. This order, is irrelevant as evidence, as well.

- The controller presented a *Declaration on Compliance with the Requirements for*

Health and Safety at Work. It was pointed out that the declaration was signed on 14 January 2022 by the employee, whose personal computer was compromised as a result of logging in to a public Wi-Fi network.

The declaration reads that the employee: *Has been familiarised with the company's health and safety rules, as well as with established physiological work and rest regime for the activity they perform. They The employee will comply with all the requirements, procedures, technical rules, obligations of confidentiality and health and safety rules related to the performance of work and approved by the company, as well as the health and safety rules prescribed to them in connection with remote working; They will organise their workplace so as to satisfy the minimum health and safety requirements laid down in the Health and Safety at Work Act and in the legal instruments for its application , as well as according to the company's rules on work with displays , will comply with the requirements for working hours and the physiological patterns for work and rest for the type of activity which the employee carries out.*

The declaration presented is irrelevant as evidence to the present case.

- The controller presented WORK CERTIFICATE No. 004 of 4 January 2022, showing that the employee received an initial training on 4 January 2022, however it does not specify its type. The reference is presumably to the *Declaration on Compliance with Requirements for Health and Safety at Work* as described above.

Additionally, LockTrip Ltd. sent the following by letters with № ПАИКД-13-28#20/29.09.2022 г. and № ПАИКД-13-28#21/03.010.2022 г.:

- Partner agreements with Agoda Company PTE LTD and Booking.com BV;
- An internal procedure concerning the cancellation and refund process;
- An internal procedure concerning issues related to the payment process on the customer side;
- An internal procedure concerning the process of hotel booking confirmation;
- An internal procedure concerning issues related to hotel mapping;
- An internal procedure concerning issues related to hotel room mapping;
- Internal procedure concerning manual reservation "rescue";
- An internal procedure concerning a booking flow and email notifications;
- Established rules on the access of the employees of LockTrip Ltd. to the internal information systems and partner portals of the organisation.

The controller presented an annex to the partner agreement with Agoda Company PTE LTD regulating the relationships between the partners with regard to the personal data processing for the purposes of the agreement. Point 11 of the agreement with Booking "CONFIDENTIALITY AND SECURITY" includes clauses regulating the lawful processing of personal data for the purposes of

the agreement between the partners.

Regarding the additionally presented Internal Procedures as described above, they cannot be considered evidence relevant to the present case.

V. Conclusions of the CPDP after conducting the document inspection:

1. Based on the findings of the document inspection, it was established that LockTrip Ltd., in its capacity as "personal data controller" within the meaning of Article 4(7) of Regulation (EU) 2016/679, allowed a security breach while carrying out its activity, namely: On 5 June 2022 the controller's monitoring systems and its employees detected suspicious and unauthorised activity. An on-duty employee was alerted by email from a partner platform of LockTrip Ltd. of a misapplied operating algorithm for hotel bookings. After the case was scrutinised, the controller found that data security had been breached. Even though the controller stated in the information provided, regarding the case file (without presenting evidence, such as audit reports, findings of the auditing team, etc.) that before the security breach the information systems had been audited on a weekly basis by a DEV team in order to monitor whether the overall system functioned as intended, and whether any of its components exhibited a deviation or technical failure and, last but not least, whether there was a breach of security, the operating algorithm and the authorised access, the security breach as described in personal data breach notification № ПАИКД-13-28/09.06.2022 г. demonstrates that the technical and organisational measures taken by the controller were inappropriate. When determining which measures are appropriate, the controller should take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. After making such an assessment and analysis, the controller should apply appropriate technical and organisational measures to ensure a level of security appropriate to the particular risks. In practice, the controller failed to ensure the security of the personal data being processed. The data controller found out about the breach after an email notification was received from a partner platform of LockTrip Ltd., which alerted them of a misapplied algorithm for hotel bookings, resulting in an unauthorised access and unauthorised disclosure of personal data: (names; address; email address; IP address from which the booking was made) of 2,108 EU citizens, including 420 Bulgarian citizens, and 2,423 third-country nationals.

Initially, the controller reported that by the time of the breach they did not consider that conditions under Regulation (EU) 2016/679 were available for analysing the risk to the rights and freedoms of natural persons with regard to the processing of their data. Therefore, no such analysis was carried out before the security breach. A Data Protection Impact Assessment for the Personal Data Processed by the Controller LockTrip Ltd. was presented additionally by letter № ПАИКД-

13-28#14/17.08.2022 г. The document as presented, points out that, in the opinion of the company, the processing of personal data on their part does not pose a high risk to the rights and freedoms of data subjects but, considering a security breach detected in June 2022, a decision was made to prepare an Impact Assessment concerning clients' personal data that have been processed by the company. By way of addressing the risks, the company took the following measures:

1.1 Two-factor authentication (2FA) as a key protection and security measure. It requires from an employee to provide two different pieces of information in order to prove who they are before access is granted. This is a security protocol which essentially provides an extra layer of security in addition to the user's password, in cases where the password is compromised. When a user tries to access an account, they will be asked to enter their user name and password plus 2FA codes. Then the user will receive a text message with a six-digit passcode that they must enter in order to complete the entry process. The user sends the code from their phone, and so the person who has accessed the account never possesses the code.

1.2 Any outside access to the system on the part of employees has been restricted. In extreme necessity, such access is granted after the submission of a notifying request which indicates:

- specific reasons for the need to grant an outside access to the system;

- IP address from which the system will be accessed;

- period of time *(days, weeks, etc.)* for which the need to grant outside access to the system applies.

After considering the abovementioned, the Managing Director of LockTrip Ltd. makes a reasoned decision to allow or reject the submitted request.

1.3 A LastPass Premium service has been implemented, which makes it possible:

- to create a LockTrip master account controlling the access to all passwords *(including shared private spaces and partner portals)*;

- to add or to cancel agent access to shared private spaces and partner portals at any time;

- to "destroy" all web sessions of an agent at any time: by this step the agent will be automatically logged out from all active sessions, regardless of the number and types of devices using LastPass;

1.4 Email notification of an unauthorised access attempt, and push notification to the mobile device linked to the relevant user profile.

2. It is important to note that, according to Article 33(5) of Regulation (EU) 2016/679, the controller should document all facts relating to the personal data breach, its effects and the remedial action taken. That documentation enables the supervisory authority to verify the compliance of the controller with the cited provision of the Regulation. In this particular case, the controller failed to provide documents and evidence that are important for the proceedings, even though the CPDP

repeatedly requested these documents and evidence in the correspondence exchanged in connection with the examination of the personal data breach notification.

- In the personal data breach notification, the controller states that, for the purpose of preventing the breach to occur again, by 10 June 2022 they will adopt a new internal policy and procedure for security enhancement; will implement new methods for monitoring access to shared private spaces and partner platforms; will deliver internal technical training to all employees in order to raise their awareness of cyber security. While an examination of the breach was in progress and in the correspondence exchanged in this regard, no evidence of honouring the commitment assumed by the controller was presented to the CPDP. The internal rules relevant to personal data protection that were presented date from 2021;
- No factual evidence whatsoever was presented to ascertain that the controller's employees have been familiarised with the internal documents introducing rules on the lawful processing of personal data or that they have gone through initial training, as well as periodical training sessions concerning personal data protection (e.g. attendance forms, examination tests, declarations by the persons to the effect that they are familiar with the rules of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, etc.);
- No factual evidence whatsoever was presented to ascertain that the employee, holding the position of call centre operator, whose personal computer had been compromised as a result of logging in to a public Wi-Fi network, has received training, related to personal data protection. This resulted in the leak of passwords for access to shared private spaces and platforms of partners of LockTrip Ltd., including: Agoda, Booking, Dida Travel, DOTW, Escalabeds, Expedia, GetARoom, Go Global, GRNconnect, Hotelbeds, HotelDo, Hotelston, Hotusa, LotsOfflotels, Miki Travel, RateHawk, RTS, Stuba, SunHotels, TBOHolidavs, TotalStay, WelcomeBeds.

In relation with what is pointed in Section 2, it can be concluded that the controller failed to demonstrate compliance with Article 5 (1) of Regulation (EU) 2016/679, thus violating the "principle of accountability" under Article 5(2) in conjunction with Article 33(5) of Regulation (EU) 2016/679.

3. As mitigating circumstances, account should be taken of the fact that the controller notified the Bulgarian SA without undue delay, within 72 hours after having become aware of the breach; The data subjects, were notified via email sent to their email addresses, as well; This is a first personal data breach notification by that controller, regarding the personal data processed; The controller took action to limit the damage by temporarily deactivating the compromised profile of the employee and blocking their access to all shared private spaces and partner platforms; The passwords for access to all shared private spaces and partner platforms were changed; An additional

two-factor security verification was activated for access to all shared private spaces and partner platforms; The entire information stored on the hard disk of the compromised personal computer was reinstalled and deleted; The employee whose personal computer had been compromised was provided with a new wireless internet router in order to enhance security.

VI. Legal analysis

Regulation (EU) 2016/679, which was applicable since 25 May 2018, is the legal instrument laying down the rules related to the protection of natural persons with regard to the processing of personal data. The GDPR builds on the previous data protection legal framework introduced with Directive 95/46/EC, which was transposed into the Bulgarian Personal Data Protection Act of 2002 while, at the same time, takes account of the vigorous development of new technologies and of personal data processing activities.

According to the legal definition pursuant to Article 4(12) of the GDPR, *"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. In this particular case, unauthorised access was gained through the personal computer of an employee of the controller which had been compromised because of logging in to a public Wi-Fi network. As a result, passwords for access to shared private spaces and platforms of partners of LockTrip Ltd. were leaked.

The controller is obliged to take the appropriate technical and organisational measures for protection of the data, as well as to establish mechanisms for control of their implementation, and thus demonstrate compliance with the provisions of the GDPR.

The CPDP has a broad discretion and, in accordance with the functions conferred thereon, assesses which of the corrective powers under Article 58(2) of Regulation (EU) 2016/679 to exercise. The assessment is based on considerations of appropriateness and effectiveness, taking account of the specificities of each particular case and the extent to which the interests of the data subjects concerned are affected, as well as the public interest. The powers under Article 58(2), excluding those pursuant to letter (i) GDPR, are of the nature of coercive administrative measures intended to prevent or to cease the conduct of an infringement, thereby achieving due diligence in the field of personal data protection.

In applying the appropriate corrective measure under Article 58(2) of the GDPR, account is taken of the nature, gravity and consequences of the breach, as well as all mitigating and aggravating factors. The assessment of what measures are effective, proportionate and dissuasive in each individual case also reflects the objective pursued by the corrective measure selected: a prevention

or termination of the breach, sanctioning the unlawful conduct or both, which is a possibility provided for in letter (i) of Article 58 (2) of Regulation (EU) 2016/679.

Considering the present case, the CPDP takes account of the facts and, more specifically, the insufficient technical and organisational measures that allowed vulnerability, namely a breach of security through the personal computer of an employee of the controller due to its connection to a public Wi-Fi network, as well as the results of the document inspection conducted, which certified that additional action had been taken for the prevention of such incidents, taking account of the nature, gravity and possible consequences of the personal data breach.

Considering the above, after a review and analysis of all the evidence collected in the administrative case file, for the purpose of preventing such breaches in the future, the Commission for Personal Data Protection has adopted the following

FINAL DECISION

1.) Pursuant to letter (b) of Article 58(2) of Regulation (EU) 2016/679, for an infringement of letter (f) of Article 5(1) in conjunction with letter (b) and letter (d) of Article 32(1), the Commission hereby ***issues a reprimand to LockTrip Ltd.*** for allowing infringements of the provisions of the Regulation under Personal Data Breach Notification. № ПАИКД-13-28/09.06.2022 г;

2.) Pursuant to letter (d) of Article 58(2) of Regulation (EU) 2016/679, for a breach of the "principle of accountability" pursuant Article 5(2) in conjunction with Article 33(5) of Regulation (EU) 2016/679, the Commission hereby ***orders LockTrip Ltd.*** to bring its processing operations in compliance with the provisions of the Regulation by means of applying appropriate technical and organisational measures of data protection against unauthorised access such as:

- To analyse and audit the technical and organisational measures taken for the protection of personal data when using remote access;
- To draft rules/a policy regulating the use of remote log-in to the company's information systems, envisaging an automatic denial of access when logging in to a public Wi-Fi network;
- To draft internal rules/procedures/instructions regulating the delivery of training in data protection (initial and periodic) and envisaging mechanisms for control of compliance. As part of the rules, a requirement should be included that when training to employees is delivered, the "principle of accountability" is to be respected and the controller must have evidence at their disposal (when inspected

by the CPDP) of the training sessions held, the employees who attended and the training materials;

- In connection with the infringement concerned, to deliver training in personal data protection to all employees and to present evidence of the said delivery, including signed attendance forms and training materials used in the training as delivered.

3.) This order is to be executed within 3 (three) months after the entry into effect of the Decision, and the controller will notify the Commission for Personal Data Protection of the execution within 14 (fourteen) days thereafter, presenting the relevant evidence.

The Decision of the Commission for Personal Data Protection could be appealed before the Sofia City Administrative Court within 14 (fourteen) days after receipt.

CHAIRPERSON: **MEMBERS:**

[redacted]

(Signature)

[redacted]

(Signature)

[redacted]

(Signature)