Ref. no.: **11.17.001.011.004, 12.10.001.011.006.004.066**

Decision

Unauthorised processing of customers' personal data

1. A complaint was lodged with the President of Personal Data Protection Office in Poland (Poland SA) against Briju 1920 Limited (Company). The Company's head office is located in Cyprus and it operates as a plant in Poland. Consequently, on the 28th of December 2022 the complaint was subsequently transmitted to the Office of the Commissioner for Personal Data Protection (Cyprus SA), in line with Article 56 of the General Data Protection Regulation.

2. On the basis of the above, the Commissioner for Personal Data Protection (the Commissioner) is acting as the lead authority in this matter.

Description of the Case

3. According to the Complainant (Data Subject), on the 2nd of December 2022 she made an online purchase from Briju 1920 Limited (Company). On the same day, she received an e-mail from a third party who informed her about unauthorized access to her personal data due to the fact that the Company had never "*withdrawn the relevant data processing authorisations*". In the e-mail was mentioned that, the e-mail's sender had access to 7000 customers' personal data, such as their name, surname, address, telephone number, e-mail address and method/form of payment.

4. On the 5th of December 2022 the Company sent an e-mail with its official position on the above-mentioned incident. In the said e-mail, the Company's director informed its customers that all Company's security systems have been checked and appropriate technical and organizational protection measures have been implemented. The Company moreover confirmed that its databases are fully protected and any attempts of unauthorised access to data are and will continue to be effectively thwarted and provided the contact details of the Company's Data Protection Officer to the customers.

5. Afterwards the Data Subject called the helpline of the Company. As she mentioned, it turned out that she was not the only person to receive the above-mentioned e-mail. Since the provided explanations didn't satisfy her, on the 7th of December 2022, she requested information about the reasons that caused the breach and expressed, in written, her fear and stress for a future cyber-attack. Following her e-mail, the Company assured her once more for its databases' safety, informed her that any unauthorized

15, Kypranoros street, 1061 Nicosia / P.O.Box. 23378, 1682 Nicosia - Cyprus, Tel. +357 22818456, Fax +357 22304565
E-mail: commissioner@dataprotection.gov.cy, Website: http://www.dataprotection.gov.cy

access was effectively thwarted and that the breach was already notified to the Commissioner's Office.

6. In the complaint, the Data Subject asked for an imposition of a fine to the Company and for her personal data erasure from the Company's database. The Data Subject attached to her complaint the e-mails dd 2/12/22, 5/12/22, 7/12/22.

Investigation by Cyprus SA

7. On the 6th of December 2022, the Company submitted the relevant Reporting Form in order to notify Cyprus SA about the above-mentioned incident (Data Breach Notification).

8. Cyprus SA informed the Company for the complaint submission and addressed questions to the Company in order to further investigate the reported incident (e-mails dd 16/1/23, 21/4/23, 13/10/23, 19/1/24).

9. According to the Company's submitted Data Breach Notification (dd 6/12/22):

a) The email's sender sent an email to 100 of the Company's online customers, claiming/informing them that he has unauthorized access to their personal data. As he claimed, he was working for the Company but he retained access to the customers' data even after his leaving from the Company.
b) The Company became aware of the incident on the 2nd of December 2022, when one of the data subjects who received the said email messaged the Company.
c) As the Company explained, it is collecting the customers' personal data for the implementation of their orders. The e-mail addresses of the customers were downloaded from the Company's online store database. E-mail addresses were processed by the Company on the ground of Article 6(1)(b) of the General Regulation of Personal Data Protection (EU) 2016/679 (GDPR).
d) The email's sender (Ex-employee) was processing the customers' data on behalf of the Company for the period he was working at the Company.
e) As the Company clarified, the actual fraud email was sent to 100 customers even if the Ex-employee had claimed that he retained access to 7000 customers' personal data.
f) The Company declared that even if the Ex-employee did retain some access to customers' information post leaving the Company, as he claimed, he should not have disclosed and/or communicated with the data subjects as this breaches any confidentiality clauses and/or NDAs and/or DPAs which formed part of his employment contract with the Company and which remain in force after an employee leaves the Company.
g) The Company has introduced additional organisation and technical measures, to ensure access is granted and/or retained only to those who explicitly work and/or are involved with the Company for the said purposes and to avoid any such future incident from reoccurring in the future. The Company had further ensured that any access the Ex-employee had has been reclaimed.

10. As per the additional information which was provided by the Company (dd 3/2/23, 6/2/23, 16/5/23 and 1/2/23):

a) The Ex-employee was still engaged by the Company on the date of the incident under the contract dated 15/11/2022. Therefore, the Ex-employee had authorized access to the data of the Company's customers at the time the incident occurred. On the 3rd of December 2022 the Company blocked any access the Ex-employee had at its systems (including the Company's platform). His contract with the Company was officially terminated on the 9th of December 2022.

b) There was no reason at the time for the Company to be suspicious about its employees' intentions.

c) Upon becoming aware of this incident, the Company proceeded with the below actions:

   1. On the 3rd of December 2022 the Company blocked any access the Ex-employee had at its systems (including the Company's platform). Therefore, his last logged in to the Company's system was on the 2nd of December 2023. The Ex-employee's access to the Company's platform was blocked by deleting his account (along with his login credentials).
   2. The remaining employees with access to the Company's platform were instructed to immediately change their login credentials.
   3. On the 9th of December 2022, the Company proceeded with an official termination of the Ex-employee's contract.
   4. The Company informed the recipients (customers affected by the incident) about the incident and requested them to permanently delete the correspondence that they fraudulently received.

d) The DS erasure request was satisfied. It was noted that no personal data is kept by the Company, other than the invoices and receipts issued, based on her transactions and/or purchases. As per applicable law, the Company cannot delete those invoices/receipts. The DS has been informed adequately of this (via e-mail dd 3/2/2023). According to the additional information provided by the Company on the 1st of February 2024:

   1. Art. 86(1) of the Tax Ordinance (Act of August 29, 1997, Journal of Laws 2023.2383) obliges taxpayers to keep tax books and related documents until the limitation period for the tax liability expires, unless tax laws otherwise provide. These types of documents include VAT registers, accounting evidence such as sales and purchase invoices, internal documents, correction invoices, correction notes, accounting notes, records of fixed assets, inventory documents (physical inventory), etc.
   Moreover, Art 70(1) of the Tax Ordinance states that the tax liability expires after 5 years, counting from the end of the calendar year in which the tax payment deadline expired.
   2. Art. 47 section 3c of the Act on the Social Insurance System (Act of October 13, 1998 on the Social Insurance System, Journal of Laws No. 2023.1230) states that copies of settlement declarations and personal monthly reports as well as documents correcting these documents, has to be kept for a period of 5 years from the date their transmission. This deadline applies to ZUS declarations submitted from January 1, 2012.

As proofs of the above-mentioned, the Company attached to its responses the below:

- the Contract dated 15/11/2022 between the Company and the Ex-employee and the Statement dated 15/11/2022;
- its Privacy Policy;
- an excel sheet representing the dates of the incidents,
- the e-mail dd 31/1/23 sent by Support Przelewy24.pl confirming that the ex-employee has the status "removed";
- a letter from the Director of PayPro S.A (dated 10/05/2023) and a Letter from the Company's Director (dated 16/5/23) confirming the last date of access of the Ex-employee and the deletion of his account;
- the e-mail dated 5/12/22 which was sent to the Company's customers affected by the incident and the email dd 3/2/23 sent to the Complainant.

Legal framework

11. Based on Article 5 of the GDPR,

"1. *Personal data shall be:*
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
(f) processed 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 ('integrity and confidentiality').
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

12. According to Article 17 of the GDPR,
"*1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:*
(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
(d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
(…)
3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
(a) for exercising the right of freedom of expression and information;
(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
(e) for the establishment, exercise or defence of legal claims."

Cyprus SA assessment

13. According to the provided information and the relevant Contract between the Ex-employee and the Company, the Ex-employee had legitimate access to the customers' email addresses for the time period he was working for the Company. On the basis of the Contract between the Ex-employee and the Company, at the time the incident occurred the Ex-employee was still working for the Company. It was then very difficult for the Company to take prior measures in order to prevent the reported incident and ensure appropriate security of the personal data, including protection against unauthorized processing by its employees.

14. According to the complaint, the Reporting Form and the evidences of the present case, the Ex-employee didn't use any other personal data of the customers besides their e-mail address; even though he claimed that he had access to their name, surname,

address, telephone number, e-mail address and method/form of payment. Therefore, there is no proof that the Ex-employee used in a fraud manner any other data except the customers' e-mails.

15. Concerning the Data Subject's erasure request no personal data is kept by the Company, other than the invoices and receipts issued based on her transactions and/or purchases. As it is explained above the issued receipts and invoices must be kept for compliance with a legal obligation of the Company.

Conclusion

16. Having regard to all the above information, based on the powers vested in me by Articles 58 and 83 of Regulation (EU) 2016/679 and article 24(b) of National Law 125(I)/2018 and taking into consideration that:

a) no special categories of personal data were affected;
b) data subjects were informed about the incident;
c) at the time the incident occurred the Ex-employee was still working for the Company;
d) the Ex-employee's access was immediately blocked;
e) the contract signed by the Ex-employee included clauses which determine that he was authorized to process customers' personal data only to the extend and the purpose which was provided by the Company;

I conclude that no corrective powers shall be implemented to the Company. Taking into account the present case's individual circumstances and features (as mentioned above) I consider that the imposition of a fine is not proportionate since no violation on behalf of the Company was found.

17. In order to prevent such incidents in the future, I suggest to the Company to implement the below:

a) constant control of the actions of employees;
b) withdrawing certain forms of access from employees who have signaled their intention to quit or implementing access logs so that unwanted access can be logged and flagged.

[redacted]

12th of April 2024

Commissioner
For Personal Data Protection
Cyprus