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

REF. NO. ПАИКД-13-40/2022

SOFIA, ...

The Commission for Personal Data Protection (CPDP, the Commission), composed of: Chairman: [redacted] and Members: [redacted] and [redacted], at a meeting held on 13 september 2023, examined and discussed a file with ref. No. ПАИКД -13-40/14.07.2022. In pursuance of a decision of the CPDP from a meeting held on 7 September 2022, an on-site inspection was carried out due to the existence of a "high level of risk" for the rights and freedoms of natural persons. The inspection was related to a received Notification with ref. No. ПАИКД -13-40/14.07.2022 of a personal data breach under Article 33 of Regulation (EU) 2016/679, submitted by SIBERIAN WOLF EOOD (the Controller, the Company). The results of the inspection are objectified in the Report of findings with ref. No. ППН-02-439/06.07.2023.

I. The following factual situation has been established:

The Commission for Personal Data Protection has been approached with a notification of personal data breach under Article 33 of Regulation (EU) 2016/679 ("the GDPR", "the Regulation") with ref. No. ПАИКД-13-40/14.07.2022 from SIBERIAN WOLF EOOD and a supplementary letter with ref. No. ПАИКД -13-40#3/10.08.2022, in which the facts of the breach were presented.

SIBERIAN WOLF EOOD have notified the supervisory authority that in connection with the implementation of its commercial activity related to virtual currencies, the company assigned to [redacted] and [redacted] the development of a website: www.wolfintech.com, through which the company's customers would be able to use the services it offers in relation to virtual currencies and crypto-asset entrustment.

The company has stated that they did not enter into a written contract with the natural persons who developed the website that would regulate their relationship. The work was assigned on the basis of oral agreements between the parties, under the conditions of good faith cooperation and collegiality in relationships.

After the development and launch of the information system and providing the company's customers with access to make registration accounts in order to use 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

services, the controller requested from the persons who developed the website to provide all passwords, codes, keys for access and administration of the website (www.wolfintech.com) and the back-end components. Since the controller did not voluntarily and immediately obtain access and control over the website, due to the disagreement of the persons who developed the website to provide them, the company considers that there is unregulated access by them to all the data of the subjects – customers of the controller.

From the creation of the website in March 2022 until 27 June 2022, SIBERIAN WOLF EOOD, in its capacity as the contracting entity for the elaboration of the website, had no access to the website administration data, passwords, codes, access keys. Despite repeated invitations to [redacted] and [redacted] to hand over all passwords and access data to the website, the information has was not received. The company was not able to use and manage its information system, it had no access to administer, process and store the information data on the website, including contractual information and personal data of the counterparties of SIBERIAN WOLF EOOD, which is contained in the information system www.wolfintech.com.

On 27 June 2022, after repeated requests and efforts by the company and after an official written notification and invitation, [redacted] provided a list of data and passwords for accessing the information system, which was not exhaustive. For full access to the resources of the server where the information system is installed, an additional access verification code is required and this code is sent to a telephone number which is alien to the controller at each attempt to access the website. For this reason, it was impossible to use and administer the information system in full, as they were placed in technical impossibility to do so. [redacted] provided partial assistance for the controller's ability to access the information system and all the data contained in it. He offered to render additional assistance, provided that he was paid an additional fee other than what he was originally paid for the development of the website.

On 4 July 2022, SIBERIAN WOLF EOOD found that the access code to the content management system of the website (WordPress.com) had been changed by a third party without their consent. This confirms the fact that there had been unregulated access by a third party to an information system (website) and the controller had not yet had full access and control over the system and all the data contained in it.

The company allowed the registration of customers for the use the services provided, as it agreed with the persons who developed the website that they would provide professional and technical assistance until all registrations of the company's customers who had previously expressed a desire to use its services were completed. In order to complete the customer registration process, it was necessary to create accounts by requesting registration on the website, to fill in the "Know Your Customer" questionnaires, as well as the declarations within

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 meaning of the Act on the Measures on Anti-Money Laundering (AMAML). Only after performing these actions, technical authorisation of each customer was carried out through the website and the registration on the website was confirmed. Without obtaining this full authorisation, customers would not be able to use the company's services and entrust their intended cryptoassets (bitcoin). For these technical actions on authorisation the company trusted the persons who created the website. This made necessary the registration of customers in the information system before the acquisition of full controller rights by the company.

The company has stated that an internal investigation was carried out in relation to the incident and they did not find any illegal acquisition, storage or distribution of personal data of the customers. **However, in view of the fact that the persons who developed and administered the website had access to all information and data contained and stored on the website and in view of the fact that these persons did not voluntarily provide all passwords and access keys within the specified period, it can be concluded that there is a risk of possible fraudulent use of a large volume of personal data.**

After repeated invitations to the persons who developed the website to hand over to the company all passwords and keys for access and administration of the website and after negotiations with them, as well as with the help of an expert technical (IT) team, the company was able to acquire a full access to the information system and to all stored data of the company's customers, as well as to suspend any possibilities for unlawful interference and access by third parties. The data are currently stored on a secure storage device (in a secure cloud space) and the data transfer is carried out with the help of an expert technical (IT) team.

Number of data subjects affected by the breach – a total of **129 natural persons.**

126 natural persons – citizens of Italy;
1 natural person – citizen of Romania;
1 natural person – citizen of Moldova;
1 natural person – citizen of Bulgaria.

Categories of personal data affected by the breach:

As an obligated person within the meaning of Article 4(38) of the AMAML, SIBERIAN WOLF EOOD collects the data required by law about its counterparties and performs monitoring in compliance with the Internal rules on control and prevention of money laundering and financing of terrorism, adopted by the Company.

The categories of personal data affected by the breach are the following: **names; personal identification number, copy of identity card, place of birth, telephone number; e-mail; origin (racial, ethnic); property status; financial position; origin of assets; a self-**

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

made photo of a person taken by the subject for the purpose of identifying and proving the subject's identity with the person whose passport data have been provided.

The following technical and organizational measures have been taken:

- The controller has informed all customers and data subjects about the circumstances. It is recommended that all customers download their data from the website, store them on their own media, outside the website and, at their discretion, print them out for storage on paper;
- On a secure medium, with the help of specialists (in a secure cloud space), secure copies of all the data of the subjects who provided them during their voluntary registration on the website are stored;
- Through an external company, the overall control of the information system was restored.

II. Actions undertaken by the CPDP:

1. On the occasion of the notification received, by a letter from the CPDP, ref. No. ПАИКД-13-40#1/29.07.2022, information and relevant documents have been requested from SIBERIAN WOLF EOOD.

a. By a letter with ref. No. ПАИКД-13-40#3/10.08.2022 information and additional documents were received by the CPDP.

b. By Report note, ref. No. ПАИКД-13-40#4/02.09.2022, the received notification was reported at a meeting of the CPDP held on 7 September 2022 and a Decision was adopted to carry out an on-site inspection due to the presence of a "high level of risk" for the rights and freedoms of natural persons.

c. With a view to clarifying facts and circumstances relevant to the case, Order No. РД-15-73/03.03.2023 ordered the performance of on-site inspection of the personal data controller SIBERIAN WOLF EOOD.

d. By a letter, ref. No. ПАИКД-13-40#15/17.02.2023, a notification was sent to SIBERIAN WOLF EOOD regarding the upcoming inspection on 7 March 2023.

2. On the basis of Article 56(1) of the GDPR, the CPDP has initiated a procedure as a supervisory authority competent to act as lead supervisory authority for cross-border processing carried out by a controller established in the Republic of Bulgaria. The procedure was initiated by the Commission on 17 December 2022 and is registered

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

in the Internal Market Information System under number A56ID 437940. After the expiry of the statutory period, no objections were raised by the other concerned supervisory authorities, Italy and Romania, and the decision is therefore final.

III. Carrying out an on-site inspection at the controller's registered office

The inspection was opened on 7 March 2023 at the registered office of SIBERIAN WOLF EOOD, located in the city of Sofia, Mladost 3, 51 Aleksandar Malinov Blvd., Metro City Shopping Centre, Office No. G 21. [redacted], a citizen of the Republic of Italy, manager of the company, was served with the inspection order, in the presence of [redacted] – a lawyer from the SBA ([redacted]) and [redacted] - a translator, who provided assistance and ensured access and collection of evidence by the inspection team.

The tasks of the inspection were clarified and the data and circumstances regarding the incident were discussed. The actions taken by SIBERIAN WOLF EOOD in relation to the personal data breach were discussed.

- The company does not have specifically developed rules and criteria to apply when selecting service providers to develop the website. The persons who were selected assured the manager of their professional qualities, technical skills and knowledge for the purposes for which they were engaged. They gave an assurance that they would take care of the creation of the information system, the preparation and publication of a Privacy Policy and Cookie Policy that are suitable for the website, the secure storage of provided data and the successful commissioning and operation of the website.
- During the design and development of the website, as well as after its commissioning until the establishment of the circumstance – subject of the specific personal data breach notification, the company did not have any access to the website administration data, passwords, codes, access keys. During the entire period from the creation of the website until 27 June 2022, only [redacted] and [redacted] had access to the www.wolfintech.com information system.
- The company had a verbal agreement with the persons who developed the website that they would provide professional and technical assistance until all the registrations of the company's customers, who previously expressed a desire to use its services, were completed. Before the incident was established, the company fully entrusted the design and development of the website www.wolfintech.com to the persons [redacted] and [redacted] including the provision of the appropriate technical protection of the website, as well as the preparation and publication of appropriate Privacy Policy and Cookie Policy on the website.

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 company has stated that they repeatedly invited [redacted] and [redacted] to hand over immediately all passwords and access data to the website. In practice, the controller SIBERIAN WOLF EOOD was in no way able to use and manage its own information system www.wolfintech.com. It had no access to administer, process and store information data on the website, including contractual information and personal data of counterparties/customers of SIBERIAN WOLF EOOD. The company was unable to carry out freely and unimpededly its commercial activity, store and lawfully process contractual information and data of its counterparties, which they voluntarily provided in relation to the registration and creation of their accounts on the website www.wolfintech.com for the purpose of using the services provided by the company.

SIBERIAN WOLF EOOD specifies that potential citizens affected by the security breach are: citizens of **Italy – 126 natural persons; citizens of Romania – 1 natural person; citizens of Moldova – 1 natural person and citizens of Bulgaria - 1 natural person.**

The company has appealed for assistance to the hosting platform www.infomaniak.com, being the web hosting of www.wolfintech.com and to the information system www.sectigo.com, which in turn takes care of the cyber security of www.wolfintech.com, but until 14 July 2022 they did not obtain the necessary timely assistance.

SIBERIAN WOLF EOOD has stated that on 27 June 2022, after repeated requests and efforts, [redacted] sent a list of data and passwords for access to the information system www.wolfintech.com, which is not exhaustive. For full access to the resources of the server where the information system is installed, an additional access verification code is required and this code is sent to another's telephone number at each attempt to access the website. Thus, it was impossible for the company to use and administer the information system in full. [redacted] rendered partial assistance in providing full access to the information system and all the data contained in it. He made it a condition that for the provision of full assistance he had to be paid additional remuneration.

On 4 July 2022, it was found that the access code to the content management system WordPress.com had been changed by a third party, without the consent of SIBERIAN WOLF EOOD. For this reason, the company still did not have full access and control over the information system and all the data contained in it. In this regard and in view of the above, the manager of SIBERIAN WOLF EOOD – [redacted] filed a complaint with the Sofia Regional Prosecutor's Office (ref. No. 28966/14.07.2022). Subsequently, they were informed that the file was terminated and a refusal to initiate pre-trial proceedings was ruled.

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

During the entire period from the creation of the website until 14 July 2022, access to the company's information system www.wolfintech.com was available only to [redacted] and [redacted] It was also found by the company that at the end of June 2022, changes were repeatedly made to the website, information data were deleted, new information was added, the access of the company's registered counterparties to the information contained in their existing accounts at www.wolfintech.com was restricted and it has not been established who committed these illegal acts – without the consent of the company and without the consent of the counterparties registered on the website.

In order to carry out its commercial activity and to fulfil its contractual commitments to its counterparties, the company aimed to use entirely the website www.wolfintech.com. **The lack of access to control, storage and management of the information data on the website put the company in a complete inability to fulfil its obligations to its counterparties and completely hindered the lawful processing and storage of the provided personal data.**

[redacted] has stated that according to the information that he was provided with by [redacted] and [redacted] at the stage of design and construction of the information system www.wolfintech.com, the system was protected by an anti-virus program, passwords and access codes, which were available only to the persons entrusted with the creation of the website – [redacted] and [redacted] **The company has no specific documents regarding this circumstance.**

After the occurrence of the incident and in view of protecting the interests of customers and protecting the data provided by them upon registration, SIBERIAN WOLF EOOD commissioned to the specialised company Bcademy Sri. (address Via Piave 26. Pordenone 33170, Italy, VAT number 01838830931) to carry out a complete audit of the information system, to obtain all access codes and to prevent any possibility of a third party's access to the system. The expert technical team of the company Bcademy Sri. performed a comprehensive audit of the information system www.wolfintech.com, for which a Forensic Analysis Report on the website www.wolfintech.com was drawn up on 22 July 2022. After an automatic and manual analysis of the website's code from backup copies made on different dates, it was concluded that www.wolfintech.com did not contain any malicious code in its content.

After an additional inspection and assessment of the condition of the assets of www.wolfintech.com, which was assigned by SIBERIAN WOLF EOOD, a report was drawn up by Dracteam Technology LLC on 7 November 2022 and the following was done:

- Full ongoing scanning for malware detection;
- Scanning files on websites for integrity control;
- Checking the latest PHP version;

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

- Checking the integrity of the SQL DB (the database);
- Checking folder permissions;
- Latest version of the Content Management System (CMS);
- Checking for access and modification of critical data of the original/child website template;
- Checking the latest version of plugin (a software component that adds a specific function to an existing computer program);
- Checking the consistency and compatibility of the plugin;
- Verification of the authentication management process;
- Checking the validity of the SSL (cryptographic protocol for client-server connection) server;
- Third-party software verification www.passbase.com;
- Know Your Customer ("KYC") software;
- Comprehensive website diagnostics and performance.

The report outlined the following results of the inspection of www.wolfintech.com:

- No traces of malicious code were found;
- Some of the original files from the template's child theme were code modified by the previous web administrator to adjust and force the native content CMS workflow;
- The latest process for automatic registration/approval of the user did not comply with the initial request agreed with SIBERIAN WOLF EOOD;
- User login/registration workflow was not designed properly;
- The workflow designed to complete automatically the contract was not fully automatic and was not directly related to KYC.

In relation to the identified problems and after coordination with SIBERIAN WOLF EOOD, the following actions were taken:

- Re-changing any pre-existing access credentials;
- Moving outside of the actual website any link related to the Application Programming Interface ("API") at www.passbase.com;
- Reducing the field of sensitive data in the user registration form as a temporary collection of potential customers (if necessary): "first name, last name, country of origin, e-mail ID (identifier)";
- Creating a brand new Privacy Policy and Cookie Policy with pre-emptive blocking and asynchronous reactivation regarding the new upcoming website project in accordance with digital laws and regulations;

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

- Changing the status of www.wolfintech.com to "Under Maintenance" for security and protection of user data.

During the inspection, gaps were identified that were related to the lack of clear criteria and rules for selection of a contractor for the development of the company's initial information platform www.wolfintech.com. No written contract was concluded to regulate clearly and in detail the relations between the company and the natural persons who developed the website www.wolftntech.com – [redacted] and [redacted] and to regulate how and at what stage the company would have full access to its website, as well as the liability and penalties for non-performance on behalf of the contractor.

The controller has announced that, following the expert forensic analysis of the website, it was found that the persons who created the website had access only to the information which was stored on the website and that the personal data that were contained on the platform were the name and e-mail of the relevant subject – customer of the company. All other data, such as passport data, address, place of birth, telephone number, were stored in the company's account, again in the information platform www.passbase.com, and only the manager – [redacted] – had access to this account. **But the forensic report provided by Dracteam Technology LLC did not conclusively confirm this fact. Therefore, the controller's claims regarding the said circumstance are unproven.**

Following the incident, the website www.wolfintech.com was suspended and the company took steps to develop a completely new information platform in order to continue providing its services to customers.

When planning the inspection, the inspection team was informed that all activities and functionality on the old website www.wolfintech.com are suspended and for the purposes of the services offered by SIBERIAN WOLF EOOD, a new information system www.siberianwolf.biz is being developed. The purpose of using the platform is to inform customers about the services provided by the company. If interested, the customer can fill in a contact form to get more information.

Currently, the company has adopted the following policies, rules and procedures for personal data protection:

- Internal rules for personal data protection;
- Procedure concerning personal data security breach;
- Register of personal data security breaches;
- Risk assessment standard in the processing of personal data;
- Privacy policy of the company's showcase website www.siberianwolf.biz;

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

- Cookie policy of the company's showcase website www.siberianwolf.biz.

During the inspection, [redacted] demonstrated the functionalities of the current website www.siberianwolf.biz. It has been established that personal data are processed on two information platforms whose services are used by SIBERIAN WOLF EOOD and to which the company has commissioned data processing. Any natural person who wishes to familiarise himself/herself with the services provided by the company should visit the showcase website www.siberianwolf.biz and choose whether to continue using the website, having previously familiarised himself/herself with the published Cookie Policy and declaring his/her agreement that he/she is familiar with the relevant Cookie Policy and that he/she wishes to continue using the website. In the event that the natural person wishes to receive more information about the services provided by the company or to declare his/her intention to use the services offered by SIBERIAN WOLF EOOD, the customer has the opportunity by using the contact form to send an inquiry to the company. The website contains a contact form with the company and for this purpose SIBERIAN WOLF EOOD uses the services of a third party – a service provider that allows website owners to add personalised contact forms to their websites. In this case, the natural person should declare that he/she has familiarised himself/herself with and accepts the Privacy Policy published on the website, and that he/she voluntarily provides his/her personal data – name and contact e-mail, and agrees for these data to be processed in accordance with the accepted conditions of the Privacy Policy published at www.siberianwolf.biz.

For the purposes of the company's activity, the services of a third party that is external to the company were used – a service provider – for creation and integration of personalised contact forms to websites. For this purpose, the company, as a website owner, uses an external service at www.iotform.com for the creation and management of contact forms.

The controller uses the services of the international platform Passbase Inc., which is a set of identification tools, including vitality detection, document verification, face recognition, etc. These tools are combined to assess the authenticity of a user's true identity. Passbase Inc. provides the ability to verify securely users from over 190 countries without having to store their data. User submits a video selfie and valid identification resources during verification. Once all the necessary resources are provided, the data points are extracted, digitized and authenticated. These data points then become part of the user's identity. User is required to provide consent to share resources and/or data points of their identity. This information is transmitted and can be used to make decisions about the user (e.g. account activation).

All data of natural persons – customers of the company, are collected, processed and stored by the platform www.iotform.com and by the platform www.passbase.com. The www.passbase.com platform has built its system in compliance with the California Consumer

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

Protection Act (CCPA) to ensure a high level of privacy and in compliance with Regulation (EU) 2016/679.

SIBERIAN WOLF EOOD, as a user of the platform www.passbase.com and the services provided by it, has access to an account with data of the natural persons – customers of the company. Only the company manager has passwords and access codes to the company's account on the www.passbase.com platform. Passwords and access codes are stored on paper, sealed in an envelope and located in the company's safe in a Bulgarian commercial bank. Only [redacted] – manager of SIBERIAN WOLF EOOD has access to the safe. The company's access is limited to the extent that the manager can familiarise himself with the data provided by a natural person – a potential customer of SIBERIAN WOLF EOOD, in order to assess the risk profile of the customer, according to the AMAML, and to assess whether the customer agrees to use company services. The manager of SIBERIAN WOLF EOOD has no ability to copy, download, store, delete or correct customer data.

In relation to the operation of the new website www.siberianwolf.biz., the company assigned the preparation of a Compliance Report made by an expert team of Dracteam Technology LLC, in which no inconsistencies are reported regarding the personal data processed and regarding the security measures taken.

On 1 March 2022, the company adopted the Risk Assessment Standard in the personal data processing of SIBERIAN WOLF EOOD. The need for a data protection impact assessment at the start of each project is identified, assessing the project and the type of personal data associated with it or the processing activity. Proceeding from the initial arrangements with the contractors [redacted] and [redacted] for the creation of an information system www.wolfintech.com and considering the fact that the data should have been collected under the conditions of the availability of control possibilities, guaranteed rights of the subjects, implemented monitoring and reporting mechanisms, data structuring, anonymisation, encryption or pseudonymisation mechanisms at the time of assignment and development of the previous website. **The controller has reports that the risk was determined to be low, without providing evidence of a risk assessment, impact assessment or other analysis, based on which the provision of the company's customer data was allowed through www.wolfintech.com to third parties without written documents and security guarantees.**

Until now, the company has not received any alerts, complaints or other form of information from natural persons regarding illegal processing of their personal data or misuse thereof as a result of the incident.

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

All data subjects were informed of the fact that the persons who developed the previous information platform of the company – www.wolftntech.com, affected by the incident, had access to the data therein. The manager of the company sent a written notification to the persons who developed the website and a warning that they have to provide him with all passwords for access and control over the website, as well as to suspend their access to the website and the data stored in it. The data subjects were notified by electronic correspondence in an official group created by means of the communication and instant messaging application Telegram, this group being created for the purpose of direct and rapid communication with all customers of the company (data subjects) and group participants. The data subjects were also informed through telephone conversations and during a virtual video conference through the Zoom video communication platform, which was transmitted live between all participants.

IV. Conclusions of the inspection:

On the basis of the findings of the inspection, which are recorded in the Report of Findings with ref. No. ППН-02-439/06.07.2023, it is established that SIBERIAN WOLF EOOD, in its capacity of "Data Controller" within the meaning of Article 4(7) of the GDPR, has committed a data security breach when carrying out its activity, namely: it has lost control over the personal data that are collected and processed on its behalf – the persons who developed the website (www.wolfintech.com) had full control over them, including the personal data contained therein, without the controller's consent. **The personal data breach described in notification with ref. No. ПАИКД-13-40/14.07.2022 is evident of the fact that SIBERIAN WOLF EOOD did not take technical and organisational measures to ensure an appropriate level of security of the personal data provided by the controller's customers.** The company should have implemented measures that comply in particular with data protection principles "Privacy by design and by default". When determining which measures are appropriate, the controller should assess the current technical and technological achievements in combination with the costs of implementation, the nature, scope, context and purposes of the processing, as well as the risks of varying probability and severity to the rights and freedoms of natural persons. After carrying out such assessment and analysis, SIBERIAN WOLF EOOD should have implemented appropriate technical and organisational measures to ensure a level of security consistent with the specific risks. This is enshrined in the obligation envisaged in the provision of Article 25 of the GDPR, which refers to "Privacy by design and by default". The fulfilment of this obligation, as well as the obligation to introduce appropriate technical and organisational measures, according to Article 32(1) of the GDPR are conditions that guarantee compliance with the principle of integrity and confidentiality (Article 5(1)(f) of the GDPR).

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 responsibility of SIBERIAN WOLF EOOD is, according to Article 5(2) of the GDPR (principle of accountability), to demonstrate compliance with the data processing principles defined in Article 5(1) of the GDPR. In this regard, the controller should properly document all processes of personal data processing. It is necessary to create a documentary environment regarding the personal data processing – to have written documents that allow traceability of data processing processes. Thus, it can be proved that the data is processed lawfully, in good faith, transparently and in a minimum volume to achieve the clearly defined objectives, and the data is stored accurately and only for the time necessary to achieve these objectives, and the said processing is ensured with an appropriate level of security and data protection. **In the specific case, the controller did not take these actions, therefore it is unable to prove compliance with Article 5(2) of the GDPR ("accountability").**

Also, when a controller uses the services of a personal data processor for the processing of personal data, the provisions of Article 28 of the GDPR should be observed, namely: SIBERIAN WOLF EOOD should use a processor that provides sufficient guarantees for the application of appropriate technical and organisational measures. The relations with the processor should be regulated by a contract or other legal act (made in writing), which is binding and regulates the subject matter and the duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects and the obligations and the rights of the processor and of the controller. It is evident from the performed inspection that SIBERIAN WOLF EOOD, in its capacity as a Data Controller, did not take any actions for the processing to proceed in accordance with the requirements of the GDPR and is not able to prove compliance with the requirements of Article 28 of the GDPR.

The controller allowed the development and implementation of technical security measures to be made by persons with whom it did not have a contract specifying what technical and organisational measures should be taken when developing and implementing the website – www.wolfintech.com. In relation to its activity, the controller should have collected and processed a large volume of personal data of its customers, including those, the access to which may cause serious financial losses for the data subjects. The company has not assessed the risks of varying probability and severity for the rights and freedoms of natural persons. Given the fact that there were no clear rules and criteria regarding the technical and organisational measures upon the development of the website, the controller allowed the persons who developed it to have uncontrolled access to the provided data, being unable in this period to ensure the relevant security and guarantees for the lawful processing of the data provided by the customers. This has also been confirmed by Dracteam Technology LLC, which carried out an inspection and assessment of the assets of www.wolfintech.com.

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

For the purposes of the services offered by SIBERIAN WOLF EOOD, a new information system www.siberianwolf.biz was developed.

V. Legal analysis

General Data Protection Regulation, which applies from 25 May 2018, is the legal act defining the rules related to the protection of the personal data of natural persons during their processing. The GDPR builds on the previous data protection regime introduced by Directive 95/46/EC, transposed into the Bulgarian Personal Data Protection Act of 2002, while at the same time taking into account the dynamics of the development of new technologies and of personal data processing activities.

According to the legal definition referred to in Article 4(12) of the GDPR, "personal data breach" means 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, third parties had access to the data sets of the controller and an opportunity to acquire them without hindrance. Due to the fact that the controller did not take the necessary technical and organisational measures, the third parties had access to data on 129 natural persons – data subjects. The combination of personal data to which the third parties had access allowed easy identification of the affected data subjects, without the need for additional efforts:

- Basic data – names; personal identification number, copy of identity card, place of birth, telephone, e-mail, photo of the person for the purpose of identification and proof of identity with the subject whose passport data are provided;
- Sensitive data – racial, ethnic origin;
- Financial data – property status, financial status, origin of assets.

After the entry into force of the GDPR on 25 May 2018, personal data controllers have an obligation to maintain the security of personal data in a way that prevents processing in breach of the Regulation. It should be noted that Article 24 of the GDPR introduces an **obligation and responsibility** for the Data Controller to implement the appropriate technical and organisational measures, taking into account the factors listed in the same Article. **In this regard, the controller should carry out an assessment of the risks associated with the specific processing and take measures to limit these risks.** The measures must ensure an appropriate level of security, including confidentiality, taking into account the state of technical progress and the costs of implementation in relation to the risks and the nature of the personal data to be protected. The data security risk assessment implies consideration of the specific risks arising from the processing of personal data by the particular controller – such as accidental or unlawful destruction, loss, alteration, unlawful disclosure, or access to

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

transmitted, stored or otherwise processed personal data. It should be assessed whether the risks described in the previous sentence that are related to the processing of personal data may lead to physical, material or non-material damages. This means that the controller must, in addition to processing only the personal data necessary for the performance of its functions, have also implemented strict mechanisms that make it possible for it to exercise increased control over the data and prevent unauthorised access and distribution, as stated in the case. **During the review of the case, it was established that the Data Controller SIBERIAN WOLF EOOD did not perform a risk analysis before the personal data breach.** As a consequence of the stated circumstance, the controller SIBERIAN WOLF EOOD did not comply with the principles of "privacy by design" and of "privacy by default", in accordance with the provisions of Article 25 of the GDPR, accordingly, it did not take appropriate technical and organisational measures and this led to the occurrence of the incident under consideration. In relation to the above, the controller violated **Article 5(1)(f) in conjunction with Article 32(1)(d) of the GDPR – by failing to perform an analysis and assessment of the effectiveness of the technical and organisational measures in order to ensure security of processing.**

One of the primary duties of data controllers is accountability. It is enshrined in the specific principle formulated in Article 5(2) of the GDPR and it assigns to them the responsibility to document their personal data processing actions and achieve compliance with the principles of personal data protection. It is expressed in the controller's obligation to maintain documentation in relation to the personal data it processes, describing on what legal basis it processes the data, for what period of time, as well as to prepare and implement specific privacy policies and other relevant documents. **In this particular case, at the time of the occurrence of the incident, the controller did not have written internal rules for the processing of personal data related to the specific subject matter of activity of SIBERIAN WOLF EOOD. With regard to the above, the controller does not prove any compliance with Article 5(1) of the GDPR and thus a breach of the "principle of accountability" under Article 5(2) of the GDPR has been committed.**

Article 28 of the GDPR imposes an obligation on the respective controller to use only personal data processors which provide sufficient guarantees for the application of appropriate technical and organisational measures in such a way that the processing takes place in accordance with the requirements of the GDPR and ensures sufficient protection of the data subjects' rights, such as reliability and resources, that they will take technical and organisational measures that meet the requirements of the GDPR, including the requirements for security of processing. The performance of processing by a personal data processor should be regulated in writing between the controller and the processor with a contract or other legal act. The document

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

should regulate the subject matter and the duration of the processing, the nature and purposes of the processing, the type of personal data and the categories of data subjects, taking into account the specific tasks and responsibilities of the personal data processor in the context of the processing to be carried out, as well as the risk to the rights and freedoms of the data subject. The written document between the controller and the processor should contain clauses according to which, after the completion of the processing on behalf of the controller, the personal data processor must hand over the relevant documents. **It follows from the above that SIBERIAN WOLF EOOD did not comply with the provisions of Article 28 of the GDPR, having assigned through a verbal agreement and in the absence of clear criteria for selection of a contractor to develop the company's website www.wolfintech.com. No written contract has been concluded that clearly and in detail regulates the relationship between the company and the contractors who developed the website www.wolftntech.com, and regulates how and at what stage the company will have full access to its website. The responsibility and sanctions against the developers of the website www.wolftntech.com in case of non-fulfilment, including with regard to the legality of the actions related to the processed personal data, have not also been agreed upon.**

The CPDP has operational independence and, in accordance with the functions assigned to it, it makes an assessment as to which of its corrective powers under Article 58(2) of the GDPR to exercise. The assessment is based on considerations of expediency and effectiveness of the decision, taking into account the particularities of each specific case and the degree of impact on the interests of the specific natural persons – data subjects, as well as the public interest. The powers under Article 58(2) of the GDPR, without those under (i), have the nature of coercive administrative measures, the purpose of which is to prevent or stop the commission of a violation, thus achieving due behaviour in the field of personal data protection. The administrative fines under Article 58(2)(i) of the GDPR have a punitive nature.

In applying the appropriate corrective measure under Article 58(2) of the GDPR, the nature, gravity and consequences of the infringment, as well as any mitigating and aggravating circumstances, shall be taken into account. The assessment of what measures are effective, proportionate and dissuasive in each individual case also reflects the objective pursued by the selected corrective measure – prevention or termination of the infringement, sanctioning of illegal behaviour or both and such possibility is provided for in Article 58(2)(i) of the GDPR.

According to Article 83(2) of the GDPR, depending on the circumstances in each specific case, the administrative fines are imposed in addition to the measures under Article 58(2) of the GDPR. When imposing an administrative fine under Article 58(2)(i), of the GDPR

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

and determining its amount, an analysis of the elements in Article 83(2)(a) to (k) of the GDPR should be duly made in each specific case.

In this particular case, the analysis is as follows:

a) Affected data regarding: names; personal identification number; a copy of an identity card; place of birth; telephone; e-mail; a photo of the person for the purpose of identification and proof of identity with the subject whose passport data are provided; sensitive data – racial, ethnic origin; financial data – property status, financial status, origin of assets. By means of the listed data, the persons can be unambiguously identified, respectively, the potential impact on the data subjects can lead to a loss of control over their personal data, as well as a loss of privacy of the personal data of the affected subjects;

b) In this particular case, the violation was committed intentionally. The fact that the controller did not take sufficient appropriate technical and organisational measures to preserve the confidentiality of personal data contributed to a large extent to the commission of the violation;

c) The controller SIBERIAN WOLF EOOD sent several invitations to [redacted] and [redacted] to hand over all passwords and access data to the website, but no information was received. The controller was not able to use and manage its information system, it did not have access to administer, process and store the information data on the website, including contractual information and personal data of the customers of SIBERIAN WOLF EOOD, contained in the information system www.wolfintech.com;

d) In this particular case, the Data Controller is fully responsible for the occurrence of the personal data breach, since it did not take appropriate technical and organisational measures to protect the confidentiality of the personal data as early as at the stage of design (it did not carry out a risk assessment in accordance with the main criteria laid down in the GDPR; at the time of the violation, the controller did not have internal rules regulating the lawful processing of personal data; did not select personal data processors that provide sufficient guarantees for the implementation of appropriate technical and organisational measures in such a way that the processing takes place in accordance with the requirements of the GDPR and ensures sufficient protection of the rights of the data subjects; did not enter into a written contract with the processors, having the minimum required content specified in Article 28(3)(a) to (h) of the GDPR);

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

e) In this particular case, with respect to the controller, there are no related previous violations of a similar nature;

f) The personal data controller has cooperated with the CPDP in order to eliminate the violation and mitigate its possible adverse consequences;

g) The violation has affected the following categories of personal data: names; personal identification number; a copy of an identity card; place of birth; telephone; e-mail; a photo of the person for the purpose of identification and proof of identity with the subject whose passport data are provided; sensitive data – racial, ethnic origin; financial data – property status, financial status, origin of assets. Through these data, the affected data subjects can be fully identified;

h) The personal data breach became known to CPDP directly from the Data Controller;

i) No previous corrective measures have been imposed on the controller;

j) In view of the fact that there is not yet an approved code of conduct in the Republic of Bulgaria, according to Article 40 of the GDPR, the controller does not adhere to such a code;

k) The non-application of technical and organisational measures by the controller, which allowed the occurrence of the incident under consideration, should be taken into account as an aggravating factor. The controller's cooperation with the CPDP and the fact that the controller notified the persons affected by the violation should be taken into account as mitigating factors.

In this particular case, only the issuance of an order and the imposition of a corrective measure under Article 58(2)(d) of the GDPR is not enough. According to the reasons described above and taking into consideration the nature and type of the found violation, it is expedient, proportionate and dissuasive to impose a measure under Article 58(2)(i) of the GDPR, namely imposition of a fine on the controller SIBERIAN WOLF EOOD. After the accomplished analysis and evaluation of the evidence gathered in the case and taking into account the extenuating circumstances, the Commission for Personal Data Protection considers that the imposed specific measure will have a warning and deterrent effect and will contribute to the compliance with the established legal order on behalf of the controller.

In view of the above, after review and analysis of all evidence gathered in the administrative file, in order to prevent future similar violations, the Commission for Personal Data Protection has 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

DECISION:

1. Pursuant to Article 58(2)(d) of the GDPR for violation of Article 5(1)(f) in conjunction with Article 32(1)(b) and (d) and Article 5(2) of the GDPR, it **ORDERS** for the Data Controller SIBERIAN WOLF EOOD:

   - To provide for performance of periodic risk analysis in its internal documents (determining a specific period in which it should be performed), and in the case of the introduction of new technology, it should be mandatory;
   - To provide for compliance with the principles of accountability in its internal documents.

The order under item 1. must be executed **within three (3) months of the entry into force of the decision**, and then, within fourteen (14) days, the controller must notify the Commission for Personal Data Protection of its execution, by presenting relevant evidence.

2. Pursuant to Article 58(2)(i) of the GDPR, it imposes on the Data Controller SIBERIAN WOLF EOOD an administrative penalty – **FINE** in the amount of **BGN 10,000 (ten thousand),** according to Article 83(4)(a) of the GDPR for violation of Article 25, Article 28, Article 32(1)(b) and (d) of the GDPR and Article 83(5)(a) of the GDPR for violation of Article 5(2) of the GDPR.

When determining the appropriate amount of the fine, it is important to note that the GDPR specifies only the maximum amount and the criteria for determining the corresponding administrative fines. The specific amounts should be determined by the supervisory authority on a case-by-case basis, taking into account all the circumstances related to the situation under consideration. According to Article 83(4) and (5) of the GDPR, the maximum amount of the fine shall be up to EUR 10,000,000 or, in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83(4), respectively up to EUR 20,000 000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83(5). In this case, given the fact that the controller is a company registered under the Commercial Act, it is obliged on the grounds of Article 38 of the Accountancy Act to announce its Annual Financial Report for the financial year 2022 until 30 September 2023. In this regard, as at the date of the CPDP's meeting – 13 September 2023, at which this decision was taken, the Annual Financial Report of SIBERIAN WOLF EOOD for the financial year 2022 was not yet announced in the Commercial Register. On this occasion, the CPDP has determined a specific amount of the fine, which tends to a minimum amount – BGN 10,000 (ten thousand), which is approximately equal to EUR 5,000 (five thousand), referring to reasons listed in detail and

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

recorded in the legal analysis of the decision. In addition, the CPDP also takes into account the fact that the company was founded in 2021 and falls into the category of "micro enterprises" within the meaning of the Small and Medium Enterprises Act.

After the entry into force of this decision, the amount of the imposed administrative fine should be transferred by bank transfer to the Commission for Personal Data Protection, Sofia, 2 Prof. Tsvetan Lazarov Str.:

Commission for Personal Data Protection, Bulstat 130961721,
Bank account IBAN: BG18BNBG96613000158601 BIC BNBGBGSD
BNB Bank – Central Office.

In the event that the obligation is not paid voluntarily within the statutory period after the entry into force of the decision, actions will be taken for forced collection, according to Bulgarian legislation.

The decision of the Commission for Personal Data Protection may be appealed to the Administrative Court - Sofia City within fourteen (14) days from its receipt.

The decision was taken at a meeting of the Commission for Personal Data Protection, held on 13 September 2023.