Summary Final Decision Art 60

IMI Number 588536 - Notification

EDPBI:BG:OSS:D:2023: 1066

Administrative fine ; Compliance order; Violation identified

Date of summary: 08/07/2024

Background information

Date of complaint:	N/A
Draft decision:	N/A
Revised draft decision:	N/A
Date of final decision:	13 September 2023
Date of broadcast:	12 December 2023
Controller:	Siberian Wolf EOOD
Processor:	N/A
LSA:	BG
CSAs:	IT SA; RO SA
Legal Reference(s):	Article 5 (Principles relating to processing of personal data) , Article 32 (Security of processing), Article 28 (Processor), Article 25 (Data protection by design and by default)
Decision:	Administrative fine, Compliance order, Violation identified
Key words:	Administrative fine, Accountability, Data protection by design and by default, Personal data breach, Responsibility of the controller

Summary of the Decision

Origin of the case

The LSA had been notified of a data breach by the controller whose main activity is acting as an intermediary in the financial sector. The controller had engaged two developers to build a website through which its customers would be able to use the services it offers in relation to virtual currencies. The company had however never entered in a written contract with the developers but rather relied on an oral agreement. After the development and launch of the information system and providing the company's customers with access to make registration accounts, the controller requested the website developers to provide all passwords, codes, keys for access and administration of the website, as well as the back-end components.

Despite repeated invitations, for a number of months, the developers refused to hand over the access codes and passwords to the controller, during which time users could register. Due to these circumstances, the controller considered that there was unregulated access by the developers to all of the controller's customers' personal data for the period between May and June 2022, when the developers partially complied with the controller's request. However, soon after that, the controller found that a third party had changed the codes to access the content management system of the website without the controller's consent. The company allowed the registration of customers to use the services provided, as it agreed with the developers that they would provide professional and technical assistance until all customers registrations who had previously expressed an interest in using its services were completed. Following the incident, the controller commissioned a complete audit of the information system and an internal investigation was carried out. According to the controller, no illicit acquisition, storage or distribution of personal data had taken place and a number of measures were taken in relation to the problems identified, including suspending the website and creating a new information platform.

However, after carrying-out an on-site inspection at the controller's office, the LSA suspected that given the circumstances, there was a risk of possible fraudulent use of a large volume of personal data. A total of 129 data subjects were affected by the breach and the categories of personal data affected were: names, addresses, Personal ID Numbers, copies of ID documents, places of birth, phone numbers, e-mails, origin (racial, ethnic), information related to the individual's property and financial status, origin of assets, photos.

Findings

The LSA considered that the lack of access to control, storage and management of the information data on the website put the controller in a complete inability to fulfil its obligations to its counterparties and completely hindered the lawful processing and storage of the provided personal data. The LSA also found that the controller had not taken appropriate technical and organisational measures to ensure an appropriate level of security of the personal data provided by its customers and hence, did not comply with the principles of data protection by design and by default. In addition, the LSA considered that by not having access to its website, the controller has not complied with the obligation to document the processes of personal data processing and therefore was unable to prove compliance with Article 5(1) and (2) GDPR. Furthermore, the oral agreement does not rise to the rigors of article 28 as firstly, there ought to be a binding contract that governs the controller-processor relation and secondly, aspects such as the purpose and nature of processing, the categories of personal data and the categories of data subjects were never determined.

Decision

The LSA concluded that the controller infringed Article 5(1)(f) in conjunction with Article 32(1)(b) and (d) and Article 5(2) GDPR; ordered the controller to provide, within a period of 3 months, for performance of periodic risk analysis in its internal documents and to ensure compliance with the principles of accountability in its internal documents.

In addition, the LSA imposed on the controller an administrative of 10.000 BGN (approximately 5.000 EUR) for the breach Article 25, Article 28, Article 32(1)(b) and Article 5(2) GDPR.