STATE DATA PROTECTION INSPECTORATE

The Fine for the Breaches of the GDPR Was Imposed on the Company Providing the Payment Initiation Services
(private sector, 61.5 thous. EUR)

Year 2019

The State Data Protection Inspectorate (Inspectorate) has imposed an administrative fine in the amount of EUR 61,500 for the breaches of the General Data Protection Regulation (GDPR). The sanctions were imposed on MisterTango UAB for the breaches of Articles 5, 32 and 33 of the afore-mentioned Regulation, i.e. the personal data breach in the payment initiation service system which, inter alia, has also not been reported to the supervisory authority. In the opinion of the Inspectorate, the start of imposing fines under the General Data Protection Regulation should be a significant signal to other companies which only declaratively comply with the provisions of the above legal acts.

Inspectorate carried out an investigation and imposed a fine taking into account the received information on the personal data of bank customers which was made public and the possibly committed personal data breach at MisterTango UAB. The company operates internationally and provides payment services to the residents and companies of Lithuania and to foreign residents and companies. It has established a branch in Latvia, provided services in other countries. The Lithuanian supervisory authority which has coordinated its decision with the Latvian personal data protection supervisory institution according to the provisions of the GDPR had the opportunity to receive a confirmation of the correctness of the made conclusions from its colleagues. This case also shows that companies should pay more attention to the management of data breaches and cooperation with the supervisory authority in the course of the investigations.

Having carried out the investigation, the Inspectorate has determined that the company breached the requirements of the GDPR as it improperly processed personal data in screenshots (SS), made personal data publicly available and failed to report the personal data breach to the personal data protection supervisory authority.

Regarding improper processing of personal data. In the light of the information collected during the investigation and the provided clarifications, it has been determined that MisterTango UAB processes (accesses, collects) more personal data than it indicates as necessary for effecting of the payment initiated by the payer itself. The Inspectorate considers that, for the purposes of implementation of the data minimisation principle, only such data as the name, surname and, if the payer wishes, his/her identification code, bank account number, currency and balance, purpose of the payment/payment code necessary for effecting the payment should be collected. However, in addition to the afore-mentioned data, the company also collected such data as dates of provision of not reviewed electronic invoices, names of the senders and amounts; dates, topics of submission of not read notifications and a part of the text of the notification; purposes, types, amounts of the loans; names of the pension funds, accumulated units, value thereof, accumulated amounts; types of credits (e.g. mortgage credit), due balances, amounts and dates of other payments, numbers of

the issued payment cards and amounts in such payment cards which should be considered as superfluous data. Furthermore, it has been determined that the company stores such data longer than it has established and indicated as necessary by itself, i.e. the data provided during the investigation suggests that the data was stored for 216 days instead of 10 minutes. According to Article 5 of the GDPR, the company shall be responsible for and be able to demonstrate compliance with the principle of accountability; nevertheless, the company failed to provide sufficient evidence to the supervisory authority during the investigation.

Regarding the publicity of personal data. During the investigation it has been determined than the website with the list of payments processed by MisterTango UAB were visible for more than 2 days (9-10 July 2018). The payments made by the customers of different bank institutions through the payment initiation service system of MisterTango UAB and personal data of such customers were made public. Besides, more than 9,000 SSs with the pages of details of the payment sessions of the customers of 12 different banks in different countries were made publicly available. Furthermore, it has been determined that management, installation and maintenance of the IT infrastructure (hardware and software) of MisterTango UAB were carried out by one employee. One employee fulfilled the contradictory functions. Consequently, proper minimisation of possible unauthorised or unintentional modifications and implementation of proper personal data protection policy were not ensured. Thus, MisterTango UAB has failed to choose the appropriate technical or organisational measures which would help to ensure a level of security appropriate to the risk, including protection against unlawful processing, disclosure, thus, breaching Articles 5 and 32 of the GDPR.

Regarding the failure to give the notification of the personal data breach. According to the GDPR, an incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed shall be a personal data breach. From the point of view of the Inspectorate, the afore-mentioned incident where unauthorised persons were granted access to personal data in the Internet for 2 days should be considered as a data breach which must be reported to the supervisory authority. Therefore, MisterTango UAB was obliged to without undue delay and, where feasible, not later than 72 hours after having become aware of the personal data breach, notify the personal data breach to the Inspectorate. As MisterTango has failed to notify the Inspectorate of the breach, it breached Article 33 of the GDPR.

When deciding on the amount of the administrative fine, the Inspectorate took into account all circumstances relevant to extending liability to MisterTango UAB, for example, that the company processed the personal data in a non-transparent manner, to a greater extent and longer than necessary for achievement of the purpose of the processing; the unlawful processing was done systematically; it failed to ensure security of the personal data at the moment of the personal data breach, failed to report the personal data breach which has occurred and which had an impact on the personal data allowing to directly identify the data subject to the supervisory authority; furthermore, the data constituted the banking secrecy and was processed without encryption and during the period of the personal data breach the data was processed without ensuring control of access to such data. When imposing the administrative fine in the amount of EUR 61,500 on the company, the total annual worldwide turnover of the company was taken into account. The decision of the Inspectorate is not effective and may be appealed against to the court.

According to the data available to the Inspectorate, France, Spain, Germany, Poland, Austria, Bulgaria, Cyprus, Malta have already imposed significant fines under the GDPR