THE OFFICE FOR PERSONAL DATA PROTECTION
Pplk. Sochora 27, 170 00 Prague 7
tel.: 234 665 111, fax: 234 665 444
posta@uoou.cz, www.uoou.cz

[redacted]

Ref. No UOOU-02351/19-19
Prague 26. August 2019

[redacted]

IDDS: xwgci53

Request for compliance and reprimand regarding infringement

Let me inform you that following the investigation regarding the complaint received by the Office for Personal Data Protection (hereinafter 'the Office') from a German supervisory authority on 13 May 2019, and after assessment of the case at hand, the Office concluded that in this case it is not reasonable to initiate an inspection or administrative proceedings (to impose measures to rectify the infringement).

However, it should be reiterated that by disclosing personal data to another customer's you have infringed the obligations referred to in Article 32 of the Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Furthermore, you have breached this regulation also by failing to evaluate this breach of confidentiality of personal data as personal data breach [redacted] the meaning of Article 33 of Regulation (EU) 2016/679, although it is evident that [redacted] mployees were aware of the breach (as is clear from the e-mail communication between customer and [redacted] mployee attached to the complaint).

However, in this case there are mitigating circumstances, especially the fact that disclosure of personal data to an unauthorised person was an isolated incident that was clearly attributable to a misconduct of a particular employee, i.e. there are no grounds for suspecting systematic failure to comply with personal data protection obligations. At the same time, following the request made by the Office, [redacted] took an immediate action to prevent recurrence of similar security breaches.

Similarly, the absence of an assessment of the breach is due to the misconduct of a specific employee, since the persons responsible for the agenda did not have any information about the breach until they were contacted by the Office. In this context, a mitigating circumstance is in particular the fact that the company had adopted an internal procedure for reporting and notifying personal data breaches, comprising of individual steps to be taken, after awareness of such breach is acquired (handling the incident, documentation regarding the incident, corrective measures), and which includes a method of risk assessment and notification of a breach. Employees are obliged to follow this procedure.

In addition to the above, the fact that [redacted] after a request from the Office has willingly cooperated with the Office to resolve the case and has immediately taken steps to resolve the incident, has sent an apology to the complainant and begun realization of measures ensuring such incident does not recur in the future.

In view of the above, and in particular the fact that [redacted] based on the Office´s request has already taken measures to increase the level of personal data protection, the Office in this case does not consider it to be justified to impose measures to rectify the infringement or to conduct further proceeding.

In this context, I reiterate that controllers must take appropriate technical and organisational measures to ensure a level of security appropriate to the risk. When providing access to personal data (for example [redacted] is then necessary to take measures to verify that the recipient is the intended and authorized person. The level of verification depends on the extent of risk potentially caused by disclosure to an unauthorised person.

In the case of a personal data breach, the controller is obligated to respond to this incident immediately after he becomes aware of it. According to the Office the moment of controller´s awareness is inferred from the time when the first person whose conduct is attributable to him became aware of the breach (in this case, it was the customer support officer), irrespective of whether it is such person´s job to handle the breaches. If dealing with breaches is not in the job description of the person who has acquired knowledge about the data breach, the controller has to ensure that this information is immediately shared with the responsible person.

Each data breach must be documented and investigated, it must be assessed whether the obligation to notify it to the supervisory authority (within 72 hours from the awareness of the incident) and to communicate it to affected data subjects arose. Regarding the personal data breaches, I recommend to your attention the Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01, adopted by the European data protection board and available on the website https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

Please note, that the case is recorded by the Office and the information that file might be taken by the Office into account during any future proceedings with [redacted] nd during the preparation of an investigation plan.

This case was subject to the cooperation procedure according to Art. 60 of the regulation (EU) 2016/679, whereas the Office was the leading supervisory authority.

[redacted]
inspector of the Office