



CH-3003 Bern

POST CH AG  
EDÖB; EDÖB-A-1E8D3401/3

MLL Meyerlustenberger Lachenal Froriep AG  
Schiffbaustrasse 2  
Postfach  
8031 Zürich

Your reference:

Our reference:

Case officer: Katja Gysin

Bern, 17 March 2023

**Mitto AG, possible misuse of access to the mobile network,  
conclusion of preliminary investigation**

Dear Sir or Madam

In December 2021, the Federal Data Protection and Information Commissioner (FDPIC) became aware through reports in the media of possible unlawful data processing by an employee of Mitto AG. Allegations were made that an employee of Mitto AG had facilitated the unauthorised surveillance of individuals, possibly by third-party companies, via the company network.

As part of a preliminary investigation, the FDPIC carried out the following investigative procedures:

**Enquiries**

1.

Mitto AG was first requested on 8 December 2021 to comment generally on the matters in question. The response was sent by Mitto AG's legal representative on 7 January 2022 before the extended deadline, stating that Mitto AG had no knowledge of any such irregularity and that Mitto AG had taken organisational and technical data protection measures to prevent unauthorised processing. This statement was accompanied by extensive documentation on the applicable processes and guidelines.

In parallel to requesting Mitto AG's statement, the FDPIC had asked the three Swiss mobile phone operators to answer a list of questions. The focus was on a possible business connection with Mitto AG and the technical assessment of the vulnerability that Mitto AG had allegedly exploited. The mobile phone providers confirmed contractual links with Mitto AG, but referred to technical and organisational measures to ensure data security to rule out any effective irregularities using their respective mobile networks.



2.

In a second exchange of correspondence, the FDPIC requested Mitto AG on 4 April 2022 to provide it with documents showing which specific audits had been carried out by Mitto AG or its agents in order to establish, as it had claimed, that there had been no irregularities.

Mitto AG responded to this request of 1 June 2022 before the extended deadline. Its response referred to Mitto AG's ISO certifications and further claimed that an internal audit of the service platform had not shown that the system was compromised in any way. It maintained that no evidence of irregularities had been found and that the people mentioned in the media reports did not have access to code repositories, and therefore could not have made any unlawful modifications. No modifications or undesirable activities had been detected in the software either. It stated that an external examination in the course of a security audit of Mitto AG's service delivery platform and telecommunication systems had also failed to reveal any anomalies.

3.

In a letter dated 19 August 2022, the FDPIC requested Mitto AG to provide additional information regarding possible unauthorised access to the systems. It raised the question of whether one or more persons had used their right of access to Mitto AG's systems to enable unauthorised third parties to access information or gain direct access to the system itself. The FDPIC expected an evaluation of logging data to prove that all system accesses were justified.

Mitto AG commented in detail on this issue in a letter dated 28 October 2022 and provided an investigation report on the test steps carried out. The report analysed active directory logs, remote access VPN logs, multifactor authentication logs, application logs and all server logs (including server and service logs connected to mobile operator and carrier networks) for various time periods.

In addition, all identity access control systems were audited to ensure that access was granted in accordance with the roles and permissions. Furthermore, the report provided information on the software development lifecycle, which had been standard since 2015 and, according to Mitto AG's assessment, would have prevented or revealed any unauthorised installation of software for the localisation of mobile subscribers. The report also contained explanations relating to identity and access management for internal and external users at Mitto AG. Here, too, no abnormalities were found.

4.

In a virtual meeting on 13 December 2022 between representatives of the FDPIC, Mitto AG and its legal representatives, certain additional explanations were provided on the report.

## Assessment

Under the Federal Act on Data Protection (FADP, SR 235.1), data processors may only process personal data lawfully and in compliance with the general principles on processing (Art. 4 FADP). They are required to protect the data against unauthorised processing, for example unauthorised access, by taking appropriate technical and organisational measures. In view of the incidents described, the FDPIC carried out a preliminary investigation to determine whether there had been any failures in this regard. Mitto AG complied with the FDPIC's requests in all respects.

In the course of its correspondence with the FDPIC, Mitto AG provided evidence on how the operation of the system is organised. It also explained which measures it can take to prevent or detect undesired or unauthorised modifications to the software of its systems. The evaluation of the existing logging data allowed conclusions to be drawn about access to the systems.

According to Mitto AG, neither the examination of the rules for software modifications nor the evaluation of the instances of access to the systems revealed any indications that would suggest any irregular use of the systems in the manner alleged.

Mitto AG has also stated several times that it is not possible for employees to gain access to the localisation data of SMS recipients without modifying the systems or the software. This statement is substantiated by the information given by the mobile phone providers consulted. Mitto AG ruled out any undetected or unauthorised modification of the software based on the software development cycle introduced in 2015.

The FDPIC arranged for the audits that were required and possible using the resources at its disposal. Based on the information available to the FDPIC, there is no evidence that confirms the suspicion that a violation of data protection provisions occurred. Since the allegations of misconduct by Mitto AG are technically unspecific allegations the FDPIC has exhausted its resources for the time being without substantiating the suspicion of a violation of data protection provisions.

In view of the foregoing, the FDPIC has decided to conclude the preliminary investigation into Mitto AG without making any recommendations.

Yours sincerely

Adrian Lobsiger  
The Commissioner