Final Decision

Complaint against [redacted] –
Personal data breach (Articles 33 and 34), Security of processing (Article 32)

National Ref.: 90.21.22:0005

IMI Case: 121112
IMI A56ID: 112674
IMI A60DD: 514731

On Thursday, 27 June 2019, [redacted] (hereinafter "complainant") lodged a complaint with the Dutch Data Protection Authority against [redacted] (hereinafter [redacted]"). The complaint was submitted to the Hessian Commissioner for Data Protection and Freedom of Information (hereinafter "HBDI") via the EU Internal Market Information System ("IMI").

1. Case Description

The complainant has acquired a [redacted] inverter from the Dutch integration company [redacted]. The acquired inverter can be connected via the Internet to a web portal provided by [redacted]. After the establishment of such a connection, information about the inverter and other personal data could be retrieved via the Internet, e.g. via an associated mobile application (app). In this way, settings of the inverter could also be changed.

At its own initiative, the complainant carried out a comprehensive investigation into the security of this web portal and found that the portal should have significant shortcomings. For example, via an unencrypted HTTP connection and using a very easily exploitable vulnerability, it was possible to gain access to the personal data of other [redacted] customers. Accordingly, the security of that personal data was not sufficiently ensured. In addition, it would also have been possible to change the settings of the inverters of other customers. Furthermore, the web portal was operated by the manufacturer of the inverter, [redacted] in [redacted] Thus, personal data of the complainant were transferred to [redacted] and processed there without it being informed.

The complainant stated that it had informed [redacted] on Tuesday, 27 November 2018, about the serious security vulnerabilities of the web portal by e-mail. The e-mail history has been provided. It is apparent from this that on Wednesday, 28 November

Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telephone +49 6 11 14 08 – 0
Email poststelle@datenschutz.hessen.de · Web www.datenschutz.hessen.de

2018, [redacted] replied to the complainant's notification, in principle confirmed the facts and informed that it was working on a new version of the "app" that would address the problems identified. The complainant and [redacted] remained in the ex-change, with the complainant inquiring several times about the current state of play. The last communication with [redacted] provided by the Complainant is dated Friday, 31 May 2019. It is further alleged that there was a conference call between the complainant and [redacted] on Wednesday, 29 May 2019.

On Friday, 21 June 2019, the incident was reported on the [redacted] website. According to its own information, the complainant was involved in the draft report.

2. Investigation Outcome

In order to clarify the facts, the HBDI contacted [redacted] and asked to comment on the objections raised by the complainant. Furthermore, [redacted] was asked to present the technical and organisational measures taken in the meantime to ensure the security of the processing of personal data.

According to [redacted], it had already started to redesign the IT environment and thus the transfer and processing of personal data before the complainant's notification. Following the complainant's notification, the existing system has been revised immediately in order to eliminate the problems pointed out by the complainant. Afterwards, the new system, which is operated entirely in Germany, was developed and replaced the old system. It has been put into operation in the summer of 2019 and, among other things, transmits the communication between the inverters (or the USB WLAN sticks) and the portal in encrypted form.

In its assessment of the incident, [redacted] assumed that only the complainant had gained access to the system and thus to the data processed therein via the vulnerabilities described. Since the complainant immediately reported the incident to S[redacted] and [redacted] actively cooperated with the complainant, [redacted] assumed that the personal data breach did not lead to any risk to the rights and freedoms of the persons concerned. Therefore, [redacted] did not notify the HBDI of a personal data breach pursuant to Article 33(1) of the GDPR.

[redacted] referred to the complainant's communication with [redacted] from November 2018 to May 2019, which was provided by the complainant and which showed that, at the end, it would have primarily dealt with questions on the current status of the new portal and an allowance for the complainant.

Further, [redacted] provided an overview of the newly designed system architecture of the new portal and the excerpt from the register of processing activities. Based on this information, there are no indications that the new portal does not comply with the state of the art or the requirements of Article 32 of the GDPR.

Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telephone +49 6 11 14 08 – 0
Email poststelle@datenschutz.hessen.de · Web www.datenschutz.hessen.de

3. Decision

(1) The points raised by the complainant are acknowledged in principle by [redacted] and [redacted] has reacted promptly to the complainant's indications in order to remedy the vulnerabilities, informing the complainant - at least upon request - about the progress. Therefore, the HBDI considers it disproportionate to make use of the sanctioning powers to remedy the vulnerabilities.

(2) The HBDI does not agree with [redacted] assessment that the vulnerabilities identified and their exploitation by the complainant resulted in no or only a low risk to the rights and freedoms of data subjects and that it was therefore not necessary to report the incident to the HBDI pursuant to Article 32 (1) of the GDPR. In view of the fact that the GDPR entered into force six months earlier on 25 May 2018, the HBDI notifies [redacted] of this alleged infringement in accordance with Article 58(1)(d) of the GDPR. Furthermore, the HBDI considers the use of further corrective powers to be disproportionate.

(3) Based on the information provided by [redacted], there are no indications that the newly concerted and, according to [redacted], also fully implemented system architecture of the portal for the management of inverters should not meet the requirements of Article 32 of the GDPR. The communication provided by [redacted] with the complainant and [redacted] statement shows that [redacted] takes the issue of data security seriously and has been further sensitised by the investigation of the HBDI. HBDI therefore sees no need to critically question the compliance with Article 33 of the GDPR as part of a further investigation. However, the HBDI proposes to point out to [redacted] that it must ensure the security of the processing permanently by means of an appropriate and effective procedure with-in the meaning of Article 32(1)(d) GDPR.

(4) The HBDI finds that the complaint in this case has been adequately investigated.

(5) The HBDI considers that no further action is required. The investigation shall be closed and [redacted] and the complainant shall be notified accordingly.

On behalf of the HBDI

Wiesbaden, June 30, 2023

Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telephone +49 6 11 14 08 – 0
Email poststelle@datenschutz.hessen.de · Web www.datenschutz.hessen.de