LDA Brandenburg - Stahnsdorfer Damm 77 - 14532 Kleinmachnow

[redacted]

Date:	10 November 2021
Processors:	[redacted]
Phone:	[redacted]
Fax:	[redacted]
Reference:	Mi/ 154/20/0192
IMI:	A60 DD 314880

(Please indicate characters when replying)

Insufficient implementation of technical and organisational measures when operating a web shop - warning pursuant to Art. 58 para. 2 letter b of the General Data Protection Regulation (GDPR)[1]

- Data breach notification on 30 January 2020 and the following correspondence
- last: our hearing on the warning of 14 September 2021

Dear [redacted]

in the above-mentioned matter, the following is issued against [redacted] represented by [redacted] and [redacted]

Notice:

It is established that [redacted] represented by [redacted] and [redacted] has violated Article 25(1) and Article 32(1)(b) of the GDPR in relation to the upload function for image files which was not sufficiently secured by technical and organisational measures, the customer data shop which was not sufficiently protected and the outflow of personal data from the company's web shop in connection with the data protection breach of 26 January 2020.

Due to this infringement, [redacted] represented by [redacted] and [redacted] is warned in accordance with Article 58(2)(b) of the GDPR.

[1] General Data Protection Regulation of 27 April 2016 (OJ EU L 119, 4 May 2016, p. 1; L 127, 23 May 2018, p. 2; L 74, 4 March 2021, p. 35).

Justification:

I.

[redacted] perates a web shop for mobile phone accessories at the addresses [redacted] Customers can buy cases, protective foils, cables, adapters, batteries, chargers, headphones, etc. for mobile phones and tablets. In addition, [redacted] offers its customers the opportunity to design the cases themselves. For this purpose, they can, among other things, upload personal image files to the web shop's internet platform, edit them there and have them printed on (blank) mobile phone cases. For the operation of the web shop [redacted] uses [redacted] based in Poznań (Poland) as a processor.

On 30 January 2020, [redacted] nformed my authority in the context of a data breach notification pursuant to Article 33 of the GDPR that the IT systems of its processor [redacted] were compromised on 26 January 2020. In the process, the customer database of [redacted] was also stolen. In a message sent to [redacted] on 28 January 2020, the attacker(s) threatened to publish the customer data as well as further unauthorised activities on the web shop's platform if a certain amount of money was not paid by 31 January 2020.

[redacted] nformed not only the competent data protection supervisory authority about the incident, but also the customers in accordance with Art. 34 DS-GVO. Subsequently, on 16 February 2020, a data subject filed a complaint against [redacted] with my authority pursuant to Art. 77 DS-GVO, complaining about the company's breach of data protection regulations, in particular the lack of technical and organisational measures.

In order to clarify the facts and to determine the causes of the data breach, my authority contacted [redacted] ithin the framework of hearings on 2 March, 22 April, 20 July and 24 September 2020 with the request to provide the necessary information. The company's statements were dated 23 March, 30 April, 17 August and 14 October 2020 and 8 January 2021 respectively. In the context of the clarification of the facts, it was particularly important to find out how the attack proceeded in detail, which technical and organisational measures the company and the processor had implemented prior to the incident, why these measures were not fully effective and which supplementary measures were necessary to ensure technical data protection and information security or were implemented after the incident.

After evaluating the company's comments, the following emerges:

- According to [redacted] the data protection breach was triggered by a manipulated image file in JPG format, which the attacker(s) had uploaded to the web shop's platform using the function to design their own mobile phone cases. The image file contained hidden commands (script code in the programming language PHP), the execution of which made it possible to read out the customer database of [redacted] The message subsequently sent by the attacker(s) to [redacted] s order processor shows that it would also have been possible to execute other malicious functions (e.g. manipulating database entries or deleting the entire database).

- [redacted] further announced that 76,797 customers from Germany and Austria were probably affected by the incident, including 9,862 people who had created a customer account via the [redacted] site since 19 May 2017. Further people from other EU countries were also affected, including Poland, the Czech Republic, Slovakia and Hungary. In total,

up to 725,697 database entries were expected. The categories of personal data stored in the customer database in question included surname, first name, address, telephone number, e-mail address, user name and password, and, in the case of commercial customers, company name and tax number, insofar as they related to an identifiable natural person.

- The technical basis of the web shop is the open source version (Community Edition) of the product "Magento". At the time of the data protection breach, version 1.9.3.2 was used; during the investigation, version 1.9.4.4 was updated.

- According to [redacted] a number of security measures were implemented in the web shop before the incident. In addition to the standard mechanisms of the "Magento" product, these included authentication of access to servers based on asynchronous cryptographic procedures (via SSH key pairs), logging of all server activities and regular updates to close security gaps.

- As a consequence of the incident, the entire IT system of the web shop was thoroughly checked and a number of additional security measures were implemented. These include the exchange of SSH keys for authorised access, monitoring relevant system files for changes in access keys, checking the system's open ports, checking all system and home directories for malware and unwanted files and deleting them if necessary, and blocking the execution of PHP scripts from certain directories.

In the course of processing the file, [redacted] submitted a list of processing activities pursuant to Article 30 of the GDPR and a processing contract pursuant to Article 28 of the GDPR with [redacted]

In a letter dated 14 September 2021, my authority announced to [redacted] that it would issue a warning for violations of the General Data Protection Regulation pursuant to Article 58(2)(b) of the GDPR. The company did not take the opportunity to comment.

II.

My authority is responsible for monitoring data protection regulations vis-à-vis non-public bodies in the State of Brandenburg in accordance with Article 51 (1) of the Data Protection Regulation in conjunction with Section 40 (1) of the Federal Data Protection Act (BDSG) [2][3]and Section 18 (3) of the Brandenburg Data Protection Act (BbgDSG) and [4]locally in accordance with Section 3 of the Administrative Procedure Act (VwVfG) [5]in conjunction with Section 1 (1) of the Administrative Procedure Act for the State of Brandenburg (VwVfGBbg). [redacted] represented by [redacted] and [redacted] as a legal entity with its registered office in the State of Brandenburg, is a non-public body in the sense of § 1 para. 1 sentence 2, § 2 para. 4 sentence 1 BDSG, which is subject to my supervision.

---

2 Act on the Protection of Personal Data in the State of Brandenburg of 8 May 2018 (GVBl. I/18, [No. 7]) amended by Article 7 of the Act of 19 June 2019 (GVBl. I/19, [No. 43], p. 38).

3 Federal Data Protection Act of 30 June 2017 (BGBl. I p. 2097), as amended by Article 10 of the Act of 23 June 2021 (BGBl. I p. 1858).

4 Administrative Procedure Act for the State of Brandenburg of 7 July 2009 (GVBl. I/09, [No. 12], pp. 262, 264), last amended by Article 6 of the Act of 8 May 2018 (GVBl. I/18, [No. 8], p. 4).

5 Administrative Procedure Act (Verwaltungsverfahrensgesetz) in the version promulgated on 23 January 2003 (BGBl. I p. 102), as last amended by Article 24(3) of the Act of 25 June 2021 (BGBl. I p. 2154).

The legal basis for the warning is Article 58(2)(b) of the GDPR. According to this, the supervisory authority is allowed to warn a controller if it has violated this regulation with processing operations.

The hearing requirement of Section 28 VwVfG in conjunction with Section 1 (1) VwVfGBbg prior to the issuance of an onerous administrative act was taken into account, as my authority gave you the opportunity to comment on the announcement to issue a warning pursuant to Article 58 (2) (b) of the GDPR in the hearing letter of 14 September 2021. You did not make use of the opportunity to comment within the set deadline.

As part of the cooperation pursuant to Article 60 of the GDPR, my authority, as the lead data protection supervisory authority, sent the necessary information and the draft decision with the announcement that a warning would be issued against [redacted] to the other European data protection supervisory authorities concerned for their comments. No relevant and substantiated objections to the draft decision within the meaning of Article 60 (4) of the GDPR were subsequently received.

In the web shop at the above-mentioned internet addresses, [redacted] processes personal data within the meaning of Art. 4 No. 1 DS-GVO. The information collected from the customers of the shop, such as surname, first name, address, contact details, etc., are data of concrete natural persons which serve to identify these persons or enable third parties to do so. The handling of this data by [redacted] includes, among other things, the collection, storage, use, modification and deletion of the data and thus processing operations covered by the definition in Art. 4 No. 2 DS-GVO.

After evaluating the information provided by [redacted] during the above-mentioned hearings on the data protection incident on 26 January 2020, as well as the documents submitted, I have identified violations of the following data protection regulations:

a) Infringement of Article 25(1) and Article 32(1)(b) of the GDPR due to the insufficient protection of the web shop against the uploading of executable code with malicious functions.

Pursuant to Art. 25 para. 1 DS-GVO, the controller (here: [redacted] shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risks to the rights and freedoms of natural persons represented by the processing, implement appropriate technical and organisational measures, both at the time of the determination of the means for the processing and at the time of the processing itself, which are designed to implement the data protection principles effectively and to incorporate the necessary safeguards into the processing in order to meet the requirements of the GDPR and to protect the rights of data subjects.

According to Article 5(1)(f) of the GDPR, the data protection principles include, in particular, that personal data are processed in a manner that ensures appropriate security of such data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage ("integrity and confidentiality").

Article 32 (1) of the GDPR specifies the requirements in such a way that the controller and the processor must take appropriate technical and organisational measures to ensure a level of

protection appropriate to the risk. Pursuant to letter b of the said provision, these measures include measures to ensure the confidentiality, integrity, availability and resilience of the systems and services related to the processing on a permanent basis. According to Article 32(2) of the GDPR, the assessment of the adequate level of protection shall take into account, in particular, the risks associated with the processing, specifically the risks of destruction, loss, alteration or unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

[redacted] offered the customers of its web shop to upload personal files (e.g. image files) to the internet platform operated by [redacted] for the design of mobile phone cases (upload of files). This offer is not objectionable from a data protection perspective. However, [redacted] should have carefully and in detail assessed the risk of misuse of the upload function at the time the service was designed. In the event of an existing, not insignificant risk to the rights and freedoms of the data subjects, it should have planned suitable and appropriate technical and organisational measures to mitigate the risk. This follows from Article 25(1) of the GDPR ("at the time of determining the means of processing").

Furthermore, it follows from the same provision as well as from Article 32 (1) (b) of the GDPR that [redacted] should also have implemented the corresponding technical and organisational measures within the internet platform it offers ("at the time of the actual processing"), in particular to permanently ensure the confidentiality and integrity of the systems and services. In this way, it would have been possible to prevent in a timely and effective manner any unauthorised modification of the system or the services offered through the infiltration and execution of malware and thus a violation of the integrity of the system or the services. The same applies with regard to the prevention of unauthorised access to the personal data stored in the customer database for attackers and thus the prevention of a breach of the confidentiality of the processing.

In the present case, [redacted] either did not assess the risks of compromising the web shop's internet platform by uploading malware via the upload function offered, or assessed these risks as too low and thus incorrect. As a result, [redacted] failed to plan and implement sufficient technical and organisational measures that could have counteracted a compromise.

When assessing a risk to the processing of personal data, both the probability of occurrence and the amount of potential damage must regularly be considered (cf. Art. 25(1) DS-GVO and Art. 32(1) DS-GVO). [redacted] should have been aware that the offer to upload files to the internet platform it operates also attracts attackers who attempt to place software with malicious functions there and execute it in the context of processing personal data. The likelihood of such misuse activities is significant, as confirmed by frequent reports of such security incidents on internet platforms as well as recommendations for countermeasures.[6] The amount of the potential damage was also underestimated by [redacted] After all, more than 76,000 customers of the company were affected by the incident in question here in Germany and Austria alone; according to [redacted] s own information, a total of more than 725,000 customer-related data records could have been read by attackers and used for criminal activities (such as identity theft or phishing).

---

[6] see messages on relevant portals, such as "Attackers could upload malicious code to millions of WordPress websites" (https://heise.de/-4993717), "Infected add-ons found on Mozilla download page" (https://heise.de/-923719), "Google Drive vulnerability makes it easy to infiltrate malware" (https://winfuture.de/news,117795.html), "Protecting against file upload risks" (https://www.all-about-security.de/allgemein/schutz-gegen-die-risiken-bei-datei-uploads/), last accessed on 1 November 2021 in each case.

Since compromising internet platforms by uploading and executing malware is one of the greatest risks in web applications, it is also considered in important standard publications on information security. Examples include the IT-Grundschutzkompendium of the German Federal Office for Information Security[7] (BSI), the handout "State of the Art" of the Bundesverband IT-Sicherheit e. V. (TeleTrust), or the German Federal Association for IT Security (Bundesverband IT-Sicherheit e. V.). [8](TeleTrust) or the documents of the Open Web Application Security Project [9](OWASP). These publications also contain recommendations for effective and suitable countermeasures that help prevent the compromising of an internet platform (such as a web shop) through the infiltration and execution of malware.

For example, the IT-Grundschutzkompendium of the BSI (version 2020) lists in the module APP. 3.1 "Web applications", for example, lists the threats G 0.23 - Unauthorised intrusion into IT systems, G 0.36 - Identity theft and G 0.39 - Malware. The countermeasures discussed in this module include, for example, the mandatory measures APP.3.1.A4 - Controlled inclusion of data and content in web applications, APP.3.1.A16 - Comprehensive input validation and output encoding, and the recommended measure APP.3.1.A22 - Checking web applications for security vulnerabilities. Also the module APP. 3.2 "Web server" of the IT-Grundschutzkompendium also lists G 0.23 and G 0.39 among the threats. The countermeasures include the mandatory measure APP.3.2.A3 - Securing file uploads and downloads and the recommended measure APP.3.2.A14 - Integrity checks and protection against malware. By implementing the aforementioned measures, [redacted] could have effectively prevented the attacker(s) from uploading malware in a manipulated image file to the company's internet platform and executing it there.

Nothing else emerges when the other sources mentioned above are consulted. The handout "State of the Art" of the German Federal Association for IT Security (Bundesverband IT-Sicherheit e. V.). (as of 2021) lists in chapter 3.2.19 "Protection of web applications", among other things, "command injection" - i.e. the introduction of executable malicious code into the application - as a significant threat. As a protective measure, the use of a web application firewall to examine and block potentially harmful data traffic (here: during upload) is recommended.

Furthermore, the Open Web Application Security Project (OWASP) has listed "injection" among the top 10 security risks in web applications for several years - currently (2021) in third place (A03), in the previous edition (2017) in first place (A01). Injection" refers to risks from unvalidated, unfiltered or untreated data provided by users (or attackers). Several Common Weaknesses contribute to the high ranking of the risk, including CWE-77 Command Injection, CWE-94 Code Injection and CWE-96 Static Code Injection. The above descriptions also include recommended countermeasures, in particular input validation. In addition, the test for uploading malicious files is part of the Web Security Testing Guide of the OWASP (point 4.10.9 there), and should therefore be carried out regularly before commissioning and during operation when carefully testing web applications.

The measures listed in the publications mentioned as "mandatory" or "recommended" for the operation of web applications are to be qualified as state of the art. They have been developed from the abstraction of frequent security incidents and countermeasures of responsible persons and have proven themselves in practice. The implementation of the measures by [redacted] would not only have been suitable and appropriate to prevent the data protection breach in

[7] see https://www.bsi.bund.de
[8] see https://www.teletrust.de
[9] see https://www.owasp.org

question. It was also necessary to control the risks for data subjects associated with data processing. With regard to the implementation costs, it can be assumed that the effort would have been reasonable and limited. This is already shown by the short-term action of the company, which already stated in the notification of 30 January 2020 that it would now block the execution of PHP code from certain directories of the file system and thus ensure the integrity of the processing of personal data.

b) Infringement of Art. 25(1) and Art. 32(1)(b) of the GDPR due to insufficient protection of the web shop against unauthorised reading of the customer database.

According to the legal provisions cited above under II a), the controller and the processor are obliged to ensure not only the integrity of the systems and services for processing personal data, but also their confidentiality. This means that personal data must not be disclosed to unauthorised persons or come to their knowledge. As explained above, the technical and organisational protection measures shall be determined and implemented taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risks to the rights and freedoms of natural persons represented by the processing.

The inadequate protection of [redacted] s web shop against the uploading and execution of malicious software also favoured the leakage of the customer database by the attacker(s). However, this part of the data protection breach could have been effectively prevented by appropriate technical measures separately and independently of the uploading of the malware. It must be noted that the company had neither designed appropriate measures at the time of the decision on the means of data processing nor implemented them at the time of the actual processing. Both constitute a violation of the above-mentioned regulations.

For insufficient analysis and evaluation of the risks emanating from the processing of personal data in the [redacted] web shop, their probability of occurrence and the amount of potential damages, please refer to II a).

As above, important information on risks and suitable protective measures according to the state of the art to prevent unauthorised access to personal data can be found in the literature. For example, the IT-Grundschutzkompendium of the BSI (as of 2020) lists the hazards G 0.19 - disclosure of information worthy of protection and G 0.36 - identity theft in module APP.3.1 "Web applications". Among the measures to be taken against the exploitation of these threats, APP.3.1.A2 - Access Control for Web Applications, which restricts users' access to data by means of restrictive permissions, is mandatory. Also to be mentioned is the module APP. 3.2 "Web server" with the obligatory measure APP.3.2.A2- Protection of web server files, which protects confidential data from unauthorised access and also counteracts the G 0.19 threat. The IT-Grundschutzkompendium also provides security measures for the network level, here in the module NET.3.2 "Firewall" for example the compulsory measure NET.3.2.A2 - Defining the firewall rules. Suitable rules must be used to prevent unauthorised connections from the protected network (e.g. connections to attackers for the purpose of data leakage) and data loss (vulnerability G 0.45).

In its publication "State of the art" in chapter 3.2.21 "Server hardening", the Bundesverband IT-Sicherheit e. V. (German Federal Association for IT Security) also recommends a restrictive con-

figuration of authorisations, restrictions in network settings and a corresponding configuration of the firewall to prevent data outflows from databases.

With regard to the Open Web Application Security Project (OWASP), it should be noted that the risk "Broken Access Control", which also includes the unauthorised leaking of information from web applications, is currently ranked number 1 of the top 10 risks. In the previous list from 2017, this risk was ranked 5th. The assigned common weaknesses are, for example, CWE-200 - Exposure of Sensitive Information to an Unauthorised Actor or CWE-402 - Transmission of Private Resources into a New Sphere (Resource Leak).

According to all of this, [redacted] should have been aware that there is a significant risk of customer data being leaked to unauthorised persons when operating the web shop. In particular, the company should have taken protective measures against the unauthorised establishment of a communication connection from the web application to the attacker and the mass leakage of this data, also independently of the measures to protect against the upload of malicious code to the platform. That these measures are state of the art is evident from the best practice recommendations cited above. Their implementation would also have been possible with a reasonable amount of effort. In particular, restricting the possible connection to the firewall and limiting the amount of data transferred from a database could have effectively prevented the data protection breach in the present case.

Due to the aforementioned violations, [redacted] represented by [redacted] and [redacted] is warned pursuant to Article 58 (2) (b) of the GDPR. The warning serves the purpose of bindingly establishing a violation of the legal provisions of the General Data Protection Regulation that has already occurred.

The warning proves to be proportionate in the individual case. It is suitable and necessary in order to make [redacted], represented by [redacted] and [redacted] aware of the infringement and to make them aware of the provisions of data protection law. In order to achieve this purpose, the supervisory authority does not have a milder means at its disposal which would be equally suitable. The warning does not create an immediate obligation to act and is not linked to the initiation of administrative offence proceedings or a fine. Therefore, it is usually used for simple violations that have not led to a significant threat to the fundamental right to data protection.

From the fact that [redacted] represented by [redacted] and [redacted] has not experienced any comparable data protection incident so far and that a high degree of cooperation prevailed during the clarification of the facts as well as during the initiation of necessary measures, I conclude that there is no reason for further remedial measures within the meaning of Article 58 (2) of the GDPR. The complaint of the data subject was also subsequently remedied in this respect.

The warning is also appropriate, i.e. proportionate in the narrower sense. In the required weighing of the conflicting interests, it must again be noted that the intensity of the intervention of the supervisory authority's measure is to be classified as rather low, whereas on the other hand a violation of data protection principles is established. The interest of [redacted] represented by [redacted] and [redacted] to be able to operate its business free of state interference must therefore take a back seat to the interest of the general public to

prosecute a violation of the right to data protection as well as the right to informational self-determination within the framework of the legal provisions.

Remedies:

An action against this decision may be brought before the Potsdam Administrative Court, Friedrich-Ebert-Straße 32, 14469 Potsdam, within one month of notification.

With kind regards

[redacted]