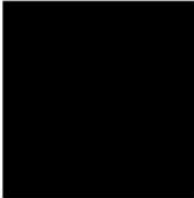

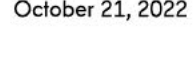





Berliner Beauftragte für Datenschutz und Informationsfreiheit
Friedrichstr. 219, 10969 Berlin



Reference number: 521.14188.13
Department: 
Contact person: 
Telephone: 
Extension: 

Date: October 21, 2022

Reprimand

Complainants:

Your comments of May 19, 2021, July 14, 2021, and January 7, 2022.

Dear Sir or Madam,

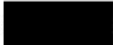
We hereby issue a reprimand to your company for a violation of the General Data Protection Regulation (GDPR).

Justification:

Our intended decision is based on the following considerations:

I.

We have established the following facts:

The complainant received a registration notification from your service  at 3:17 p.m. on February 22, 2021, and a shopping cart notification at 4:27 p.m. on February 22, 2021,

although he had not been aware of your company until then and had not created a customer account himself. On February 23, 2021, the complainant also received a newsletter (10:01 a.m.) and a survey email from [REDACTED] via the service [REDACTED] at the email address [REDACTED]. We have a copy of the e-mail communication with your customer service. This shows that on February 23 and 24, 2021, the complainant contacted the customer service several times by telephone and e-mail and requested information about the data you had stored about him (e-mail of February 24, 2021 at 11:03 a.m.). However, the request for information had initially not been complied with. Furthermore, the complainant asked the customer Service by e-mail to save the "previous data and all associated actions" for the purpose of further clarification. However, on February 24, 2021, your customer service informed the complainant that his customer account had been deleted.

In your above-mentioned comments, you stated the following:

It was true that a customer account had been created at [REDACTED] with the e-mail address [REDACTED] (without a dot between the first and last name). In the context of the communication with the customer service the complainant had called the E-Mail address [REDACTED]. Since then, the customer support staff had not been able to locate a customer account under any of the e-mail addresses provided by the complainant. Due to the misunderstanding in the identification process, the information had not been provided. You stated that your systems did not provide the ability to search for variations of e-mail addresses. Consequently, it had not been possible to verify the identity of the complainant.

Access to the customer account in question had been restricted as a result of the incidents in accordance with the process defined internally within the company, and had therefore not been deleted.

After you had internally investigated the activities of the account in question in more detail and it turned out that they were possibly fraudulent activities, the complainant's actions were interpreted as a request for information pursuant to Article 15 of the GDPR. Subsequently, the complainant was informed on May 19, 2021, about the preparation of the provision of information. The information was ultimately provided to him on May 25, 2021.

The e-mails of February 22, 2022 had been sent on the basis of consent when the account was created. On February 24, 2022, the complainant unsubscribed from the newsletter. As part of ongoing improvements, you would evaluate implementing a double opt-in process.

II.

Legally, we assess the facts as follows: Your company has violated the GDPR.

1. breach of art. 5 para. 1 lit. d, 24 para. 1, 25 para. 1 GDPR

The responsible party pursuant to Art. 5 para. lit. d, 24 para. 1, 25 para. 1 GDPR to implement appropriate technical and organizational measures to ensure and provide evidence that the processing is carried out in compliance with data protection.

██████████ has not taken implemented suitable technical and organizational measures according to Art. 24 para. 1, 25 para. 1 in connection with Art. 5 para. 1 lit. d GDPR taken to verify the e-mail addresses of new customers. When placing an order in your company's online store, customers only had to enter their e-mail address and click once on the newsletter offer. No further verification of the e-mail addresses took place.

A suitable measure to ensure the accuracy of the processed data can be the implementation of a double opt-in procedure (DOI procedure), in particular to obtain consent in accordance with the law, if the creation of the customer account is also intended to send advertising e-mails, as is the case here. ██████████ has deliberately dispensed with such or equivalent procedures for authentication and verification of the e-mail address.

In particular, identity theft poses a special risk to the rights and freedoms of natural persons, as it can result in particular in material damage (see Recital 75). It is therefore incumbent on the responsible party to take appropriate protective measures to prevent cases of identity theft within the scope of its possibilities.

2. breach of Art. 5 para. 1 lit. a, 6 GDPR

a) Welcome email of 22 February 2021 at 15:17, email of 23 February 2022 at 10:01 and email of 24 February 2021 at 10:02.

"Advertising" is defined in Art. 2 lit. a of the EU Directive 2006/114/EC on misleading and comparative advertising of December 12, 2006 as "any statement made in the course of carrying on a trade, business, craft or profession with the aim of promoting the sale of goods or the provision of services, including immovable property, rights and obligations." The continuous e-mails are promotional e-mails in which the benefits of [REDACTED] were obviously to be presented.

According to Art. 5 para. 1 lit. a GDPR, personal data must be processed in a lawful manner. The processing of personal data for advertising purposes is only lawful if there is a legal basis for this according to Art. 6 para. 1 GDPR.

There is already no legal basis for the welcome e-mail as an advertising e-mail. Neither is there a legally valid consent, nor can this welcome e-mail be legitimate as existing customer advertising. Since [REDACTED] has failed to obtain a legally compliant consent by way of the DOI procedure, there is also no undoubtedly provable consent to the other above-mentioned advertising e-mails. [REDACTED] is obliged to prove the existence of consent, Art. 5 para. 2, Art. 7, para. 1 GDPR.

b) Shopping cart reminder from February 22, 2021 at 4:27 p.m.

There is also no legal basis for the shopping cart reminder of February 22, 2021 at 4:27 pm. Neither is there consent of the complainant in the sense of Art. 6 para. 1 lit. a in conjunction with Art. 7 GDPR (see above), nor can this advertising mail be considered legitimate existing customer advertising according to Art. 6 para. 1 lit. f GDPR in conjunction with § 7 para. 3 of the Unfair Competition Act (Gesetz gegen den unlauteren Wettbewerb (UWG)), since the requirements of § 7 para. 3 UWG are not met. [REDACTED] has already not received the e-mail address of the complainant in connection with the sale of a good or service (§ 7 para. 3 no. 1 UWG). A contract between [REDACTED] and the complainant has just not come into being.

c) Satisfaction rating e-mail of February 23, 2021

According to established case law, a satisfaction survey also constitutes advertising. The processing of personal data for the e-mail of February 23, 2021 was therefore unlawful according to the principles outlined above.

According to established case law, customer satisfaction surveys also fall under the concept of advertising, as they at least also serve the purpose of retaining customers and promoting future business transactions. In the present case, the aim is to bind customers to [REDACTED] by potentially improving customer service. There was no consent or other legal basis within the meaning of Art. 6 GDPR for the customer satisfaction survey.

3. Breach of Art. 12 para. 3 in conjunction with Art. 15 para. 1 of the GDPR

Pursuant to Art. 12 para. 3 s. 1 GDPR, the controller shall provide the data subject with information about the measures taken upon request pursuant to Art. 15 to 22 of the GDPR without undue delay, but in any case within one month after receipt of the request. This means that the controller shall provide the information, confirm the deletion or the objection, or at least communicate why this is not possible within the time limit. This period may exceptionally be extended by a further two months if this is necessary, taking into account the complexity and number of requests. However, a routine and blanket extension of the deadline without examining the individual case is not provided for by the GDPR. [REDACTED] also did not inform the complainant about an extension of the deadline and its reasons.

You state that it was initially not possible to process the request for information because there was a misunderstanding in the e-mail correspondence and the associated identification process and the complainant was unable to provide the correct e-mail address (see Article 12 para. 6 of the GDPR).

However, the complainant sent you the e-mail received as an attachment at 10:31 a.m. on February 23, 2021. From this, you could have easily seen the e-mail address used and also that the complainant is the owner of this address. In the case of Gmail addresses, it does not matter how the points are set, since e-mail addresses are only assigned once and points are not taken into account ([REDACTED]).

Consequently, the receipt of e-mails works equally well with the spelling [REDACTED] and [REDACTED]. The fact that both the domain [REDACTED] and the domain [REDACTED] can be used resulted from the communication with your customer service. This would have given cause for a comprehensive search by you. Therefore, the spelling of the e-mail address alone should not have given rise to reasonable doubts about the identity

of the complainant, Art. 12 para. 6 GDPR, especially since the actual e-mail address also resulted from the advertising e-mail sent by the complainant.

The responsible party must take suitable technical and organizational measures in accordance with Art. 24 GDPR in order to fully implement a request for information. In answering the request for information, [REDACTED] could reasonably be expected to rely not only on the primary identification feature of the e-mail address. When reviewing the database, it was clear that there was an almost identical e-mail address with the name of the complainant. In any case, further clarification of the facts should have been carried out immediately, and in particular the advertising e-mail sent by the complainant should have been examined at this point at the latest.

In particular, the customer service was able to make an assignment to the e-mail address actually used in the e-mail of February 24, 2022, since it was announced in this e-mail that "an account could be found with your e-mail address". This also indicates that there was no reasonable doubt as to the identity of the complainant or that the complainant could not be identified. Nevertheless, the further response to the request for information was not pursued promptly and on time, but took place only three months later.

Consequently, the response to the complainant's request for information of February 24, 2022, was significantly delayed on May 25, 2021. This constitutes a breach of Article 12 para. 3 of the GDPR in conjunction with Article 15 of the GDPR.

Furthermore, the information provided was insufficient. Information pursuant to Article 15 para 1 lit. a GDPR is missing, except with regard to third parties, where the purposes are stated only in English on the one hand and, on the other hand, at least in part too imprecisely. Information pursuant to Article 15 para 1 lit. b GDPR is obviously incomplete. The information pursuant to Article 15 para 1 lit. c GDPR is inadequate; the recipients are only named in keywords and only for third parties as recipients. The information pursuant to Article 15 para 1 lit. d GDPR is only generalized and essentially even without the criteria for the storage period, in no case as required with a specific deletion date. The information according to Article 15 para 1 lit. e and f GDPR is incomplete and partly misleading. The information pursuant to Art. 15 para 1 lit. g and h GDPR is missing. The same applies to the information pursuant to Article 15 para. 2 of the GDPR. Furthermore, the information is also incomplete with regard to the specific data processed. For example, bank details, content of

the order and communication are missing. If you want to rely on Article 15 para. 4 GDPR with regard to the bank details, you would have to do so explicitly and give reasons instead of leaving out the information implicitly.

The right to information has therefore not yet been fulfilled. We are refraining from taking supervisory measures in this respect only because the complainant is satisfied with the insufficient information provided.

III.

As a result, we do not intend to take any further supervisory measures on account of the violation, but to leave it at a reprimand. The reprimand is based on Art. 58 para. 2 lit. b GDPR.

As the intentional nature of the infringement cannot be proven, since no (equivalent) previous infringement is known and measures to mitigate the infringement are already being examined, a reprimand is issued in this case.

We assume that you will comprehensively review your processing of personal data and carry it out in a legally compliant manner in the future and implement appropriate measures to protect the rights of the data subjects. In particular, you have indicated that you are currently evaluating the implementation of a double opt-in procedure as part of the ongoing improvements to the technical and organizational measures.

In addition, we would like to point out that if consents are obtained digitally, the implementation of a double opt-in procedure is strongly recommended, as you must prove consent in accordance with Art. 5 para 1 lit. a, Art. 7 para 1 GDPR.

We would also like to point out that no legal basis is apparent for the storage of IP addresses, at least in the form apparent from the information. In addition, we assume from experience that considerably more personal data is transmitted to the third parties named in your disclosure than stated.

We would also like to point out that there are concerns as to whether the transfers of personal data to third countries that you have apparently made meet the legal requirements. We request that you check this immediately and, if necessary, terminate any identified unlawful

transfers without delay. For your checks, we refer you to Recommendations 01/2020 of the European Data Protection Board and therein in particular to Application Case 6 of Annex 2.

With regard to your use of the [REDACTED], but also with regard to the use of all other service providers, we ask you to check whether you have concluded the order processing agreement required under Article 28 para. 3 GDPR and checked the service providers, in particular under Article 28 para. 1 GDPR, or whether there is an alternative legal basis for the transfer to the service providers. To make your work easier, we have enclosed a checklist and instructions for completing it for the review of order processing contracts.

In the certain expectation that you will comply with the data protection regulations in the future, we consider the matter closed.

Legal Remedies

An action against this decision may be brought before the Berlin Administrative Court. It must be filed in writing - also as an electronic document using a qualified electronic signature (QES) - or with the clerk of the court within one month of notification of this decision at the Berlin Administrative Court, Kirchstraße 7, 10557 Berlin. Please note that if the action is filed in writing, the time limit for filing an action is only met if the action is received by the Administrative Court within this time limit.

Yours sincerely

[REDACTED]