Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berlin Commissioner for Data Protection and Freedom of Information

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to disabled members of the public.

Contact us

Phone: +49 (0)30 13889-0
Fax: +49 (0)30 215 50 50

Use our encrypted contact form for registering data protection complaints:
www.datenschutz-berlin.de/beschwerde.html

For all other enquiries, please send an e-mail to:
mailbox@privacy.de

Fingerprint of our PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to Kochstraße / Bus number M29 and 248

Visit our Website

https://privacy.de

521.10344.26
631.65
CR 85084
DD 339845
IC 416091
RD 431505

14 September 2022

FINAL DECISION

[redacted]

To the legal representation of [redacted]

Reprimand
Your letters of 21 October 2021, of 21 December 2021 and of 8 June 2022

Dear [redacted],

We hereby issue a reprimand to [redacted] for an infringement of the General Data Protection Regulation (GDPR).

Reasoning:

Our decision is based on the following considerations:

I.
We have established the following facts:

The complainant states that [redacted] asked him to update his postal address when he registered for his existing customer account on the company's website on 2 October 2018. In doing so, a telephone number was also collected as a mandatory field. The complainant objects to the compulsory collection of his telephone number as a mandatory field. He sees this as an infringement of the provisions of the GDPR.

The practice of processing telephone numbers has – based on the complaint discussed here – been the subject of correspondence with you and your client for some time (our reference 501.118). According to your client's statement (your letter of 18 March 2020), a telephone number is compulsorily collected from the d when a new means of payment is created. We therefore assume that the complainant's statement of the facts is correct.

The complainant's statement of the facts was not disputed by you or your client in your letter of 21 October 2021 mentioned above.

In its letter of 19 November 2018, [redacted] informed us that it uses the telephone numbers in its customer service if a user has a problem that cannot be solved by e-mail or chat. In such cases, the employees [redacted] also support the users personally on the phone. The letter further states that the collection of the telephone number was permissible under Article 6 (1) GDPR.

In its letter of 12 March 2019, [redacted] adds that the relevant legal basis is "contractual performance". We therefore assume that [redacted] bases the collection of the telephone number as a mandatory field for ordering processes in its internet offer on Art. 6 (1) (b) GDPR.

In your letter of 18 March 2020, you also state that the collection of the telephone number as a mandatory field is necessary when a means of payment is created for preventing misuse or fraud. Thus, in the event of suspected third-party access to a customer's account or in the event of an incorrect debit and corresponding blocking of the account, "... so that access via e-mail address is no longer possible ..." the customer could be notified by SMS. Against this background, the processing of the telephone number and its collection as a mandatory field when registering a means of payment was, according to you, necessary for the implementation of your client's user contracts and thus permissible under Article 6(1)(b) GDPR.

In your letter of 6 January 2021, you further add that the protection of customers is one of the contractual accessory obligations that [redacted] must fulfil towards its customers. Sufficient and equally effective protection could not be achieved solely by using the deposited e-mail address as a means of contact.

You state that it is recognised in the legal literature that the characteristic "necessity" should not be interpreted too narrowly and that the examination therefore does not require consideration of the principle of proportionality. Data processing would also be necessary if it appears reasonable from the objective point of view of a reasonable third party.

Furthermore, according to you, the processing of the telephone number was also proportionate in a narrower sense and thus necessary: only the telephone number would enable a quick and direct contact with the customers in the event of possible misuse. If [redacted] could only inform the customer by e-mail, such contact would take several hours or - if a customer was absent, for example, due to holidays or other reasons - even several days.

In addition, you state, that contacting the customer by e-mail in the event of misuse would not be effective in those cases where there may have been unauthorised access to the customer's e-mail account as well. It is not beyond life experience that a customer may use the same password for several accounts. In such cases, unauthorised access is also possible to the customer's e-mail account. This does not make it impossible to notify the customer by e-mail, but it does not make it as secure as contacting the customer by telephone. In your experience, hacking a mobile phone still requires more effort than hacking an e-mail account or any other user account.

In addition, only a telephone call would allow a quick authentication of the customer, as the customer could authenticate himself to [redacted] customer service, for example, by giving his date of birth or other details. This, too, could not be guaranteed by contacting the customer by e-mail. You further state that the data protection authorities recognised that the telephone number is used, for example, when asserting data subjects' rights, in order to clearly identify the data subject. For example, in the banking or telecommunications sector, but also in other areas, contact by telephone is not unusual in order to ensure additional security.

Alternatively, you claim, the practice of your client described above could be based on its legitimate interests within the scope of Article 6(1)(f) GDPR.

With regard to our letter of 30 September 2021 (reference: 521.10344.10) prior to this reprimand, you informed us in your above-mentioned letter of 21 October 2021 that your client had already initiated the process of erasing the complainant's telephone number. You confirmed the erasure of the complainant's telephone number on 21 December 2021 and its notification on the same day to us in a letter dated 8 June 2022.

II.
Legally, we assess the facts as follows: [redacted] has infringed the GDPR.

1. <u>Processing of the telephone number for the performance of the contract (Art. 6 (1) (b) GDPR)</u>

a. Processing of the telephone number for customer service purposes

Art. 6 (1) (b) GDPR cannot be considered as a legal basis for the performance of customer service in the present case, as the mandatory provision of the telephone number is not necessary for the performance of customer service within the scope of the aforementioned regulation. The other communication channels available to [redacted] (and in particular the possibility for data subjects to contact [redacted] themselves by telephone or email for customer service purposes) are sufficient for these purposes.

In its current guidelines on Article 6(1)(b) GDPR, the European Data Protection Board also assumes for online services that this general permission cannot justify data processing for purposes of service improvement (Guidelines 2/2019 for the processing of personal data pursuant to Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version 2.0, 8 October 2019, para 49).

b. Processing of telephone numbers to combat fraud and abuse

Also the processing of personal data for the purpose of combating fraud and abuse cannot be based on Art. 6 (1) (b) GDPR:

aa) The legislator itself already classifies the processing of personal data to the extent strictly necessary for the prevention of fraud as a legitimate interest of the respective controller (recital 47, sentence 6).

bb) The Art. 29 working party had already stated with regard to the largely identical provision in Art. 7 of Directive 95/46/EC that the fight against fraud was a "... further typical area which is likely to go beyond

what can be regarded as necessary for the performance of the contract" (Art. 29 Working Party, WP 217, p. 22) and declared only consent, a legal obligation or a legitimate interest of the controller (Article 7(a), (c) or (f) of Directive 95/46/EC) applicable as a legal basis. This interpretation of the Article 29 Working Party has been reaffirmed by the European Data Protection Board (EDPB) for the provision of online services to data subjects (Guidelines 2/2019, version 2.0, October 2018, para. 28 f.).

cc) It is also recognised in the legal literature that fraud or abuse prevention cannot be based on Art. 6 (1) sentence 1 lit. b GDPR.

dd) According to the explanations in its privacy policy, your client itself also considers the detection and prevention of fraud and abuse - correctly - as its legitimate business interest [redacted]

In summary, Art. 6 (1) (b) GDPR cannot be considered as a legal basis for the implementation of the customer service or for the prevention of abuse or fraud.

2. Processing of the telephone number based on Art. 6 (1) (f) GDPR

The obligatory provision of the telephone number for the performance of customer service and/or for the prevention of abuse or fraud cannot be based on Art. 6 (1) (f) GDPR:

a. Processing of the telephone number for customer service purposes

It is true that [redacted] has a legitimate - economic - interest in collecting and processing the telephone number in the context of customer service in order to ensure customer satisfaction. However, the necessity for the compulsory collection of the telephone number is lacking.

Regarding the term necessity, the Conference of Independent Data Protection Authorities of the Federation and the Länder states in its guidance for telemedia providers (as of March 2019, p. 13): "Necessity means that the processing is **suitable** to achieve the interest (motive/benefit of the processing) of the controller, **whereby no milder, equally effective means is available**. This means that the controller must limit the processing to what is necessary" (emphasis by the author).

In addition, the overriding objective of Art. 5 (1) (c) GDPR ("data minimisation") must be taken into account when interpreting the provision.

There is therefore no room for an expansion of the concept of necessity - as proposed in your letter of 6 January 2021 ("... necessary and thus also required is the data processing even if it appears reasonable from the objective point of view of a reasonable third party") - even if this is occasionally advocated in the legal literature. This legal opinion is

based on interpreting a European law concept according to the standards of German law. According to the established case law of the CJEU, this is inadmissible.

The processing of the telephone number is also not, as you state in your letter of 6 January 2021, "proportionate in the strict sense and thus necessary":

Customer satisfaction can just as well be ensured by [redacted] making it optional for its customers to provide a telephone number for the aforementioned purposes, so that those customers who wish to make use of this service offer can provide their telephone number and those customers who do not wish to do so do not have to do so. This is a milder and equally effective means compared to the compulsory processing of the telephone number for customer service purposes.

As a result, the compulsory collection and further processing of the telephone number of the data subject for customer service purposes is not necessary and can therefore not be based on Art. 6 (1) (f) GDPR.

b. Processing of telephone numbers to combat fraud and abuse

It is true [redacted] has a legitimate - economic - interest in collecting and processing the telephone number to combat fraud and abuse. However, the mandatory collection of the telephone number lacks the necessity required by law for lawfulness also here.

The processing of the telephone number for this purpose is also not, as stated by you in your letter of 6 January 2021, "proportionate in the strict sense and thus necessary":

The description of this in your letter of 6 January 2021 apparently assumes that the company's customers can be reached by telephone at any time. This in itself contradicts general life experience, especially in the case of working people. Thus, with regard to the entirety of the customers, there are already doubts about the suitability of the processing with regard to the intention declared by your client to contact the customers "in real time" in case of suspicion of fraud or abuse.

At the same time, you state that a notification by e-mail could take hours or even days in the case of absence due to holidays. We consider this assumption incorrect as well. On the contrary, large parts of your client's customers probably have a smartphone and use your client's services via it. These devices also allow the immediate receipt of e-mails - even while on holiday. The additional processing of the telephone number for sending SMS is therefore undoubtedly not necessary, at least with regard to these customers. Furthermore, your client is free to send the notifications in question to the customers via the apps of your client's company used by these customers.

This means that the vast majority of customers should be able to be notified in the event of fraud and abuse without the compulsory collection and use of a telephone number.

In addition, when using landline telephone numbers, it should be noted that your argumentation does not apply in this respect.

Your client is also free to obtain the (voluntary) consent of those customers who cannot be reached in this way, after informing them of the intended processing.

Also, when using the e-mail addresses stored by the customers for their notification in case of suspected fraud or misuse, there is usually no additional requirement for their authentication, as you seem to assume (your letter of 6 January 2021, page 4, 2nd paragraph).

As a result, the above-mentioned measures provide your client with milder and equally effective means to realise its legitimate interest in combating fraud and abuse. Forced processing of the telephone number is therefore not necessary within the scope of Article 6 (1) (f) GDPR.

Even if, in the case of Art. 6 (1) (f) GDPR, one were to assume a necessity and thus a legitimate interest of your client, the weighing of legal interests would in any case be to the detriment of your client. The interest or fundamental rights and freedoms of the data subject in not providing his or her telephone number outweigh the legitimate interests of your client in collecting compulsorily the telephone number for the purpose of customer service and for the prevention of abuse or fraud. Here, too, it must be taken into account - to the detriment of your client - that it can resort to other communication channels for the aforementioned purposes. In addition, the protection of your client's financial interests is satisfied by blocking the affected accounts. In this case, the blocking is at the expense of the data subject whose account has been misused. As soon as he or she has an interest in the further use of your client's services, he or she can be informed directly by your client anyway, including the possibility of offering telephone contact if necessary.

With the measures outlined above, a certain number of customers may remain in relation to the total number of customers of the company who do not give their consent to the processing of a telephone number for the purpose of fraud and abuse prevention. However, the decision on this must be left to the individual customers. The fact that it may not be possible to contact all clients immediately in the event of an attempt at fraud or abuse suspected by your client does not justify the compulsory processing of the telephone numbers of all clients.

As a result, the compulsory processing of a telephone number of customers of [redacted] for the purposes of customer service or the prevention of fraud and abuse can neither be based on Art. 6 (1) (b) GDPR nor on Art. 6 (1) (f) GDPR.

3. <u>Processing of the telephone number based on Art. 6 (1) (a) GDPR</u>

In this respect, the only possible legal basis for the processing of the telephone number in the context of orders on your client's website is consent pursuant to Art. 6 (1) (a) GDPR. Consent within the scope of the GDPR must be a **voluntary** expression of will "... for the specific case, given in an informed manner and in an unambiguous manner ..." (Art. 4 (11) GDPR), which must also fulfil the conditions of Art. 7 GDPR. Consent would also have to be designed in such a way that it can be given separately for the named processing purposes (customer service on the one hand and fraud and abuse prevention on the other).

However, according to the information available to us, [redacted] did not obtain the complainant's legally valid consent to the collection and processing of his telephone number at all in the present case.

4. Result

The processing of the complainant's telephone number for customer service purposes and to combat fraud and abuse cannot be based on either Art. 6(1) (b) or Art. 6 (1) (f) GDPR. Moreover, your client has not obtained legally valid consent from the complainant for this. No other legal basis is apparent.

The processing of the complainant's telephone number for customer service purposes and to combat fraud and abuse thus took place without the necessary legal basis and infringed the provisions of the GDPR (Art. 5 (1) (a), 6 (1) GDPR).

At the same time, the compulsory processing of the complainant's telephone number breached your client's obligation to minimise data under Art. 5 (1) (c) GDPR.

Your client was therefore obliged to delete the complainant's telephone number, as it was or is being processed unlawfully (Art. 17 (1) (d) GDPR).

III.
As a result, we decided not to take any further supervisory measures due to the infringement in this individual case, but to leave it at a reprimand for the time being.

The reprimand is based on Article 58 (2) (b) GDPR.

Taking into account the specific circumstances of the established facts, we consider a reprimand to be appropriate after completing our investigation. This is the first time we have identified such a breach by [redacted]. When approached by us, your client was reasonable, deleted the complainant's telephone number and informed the complainant accordingly without delay after the erasure had taken place.

With regard to the present individual complaint,, we thus consider the matter to be closed.

However, based on the correspondence with you and your client on the matter to date, we also assume that the compulsory collection and use of telephone numbers is not only taking place in the individual case in question here, but is rather a common practice on the part of your client. We recommend that your client immediately check this and also immediately delete the other telephone numbers of other clients that may have been stored without a legal basis (i.e. without the effective consent of the data subjects). We will review your client's general practice with regard to the collection and use of telephone numbers in the near future, also irrespectively of complaints. Should we find continued infringements of the applicable data protection law, we expressly reserve the right to take further supervisory measures.

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 by means of 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. It is pointed out that in the case of filing an action 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.

Kind regards,