Republik Österreich
Datenschutz behörde

Barichgasse 40-42
A-1030 Vienna
Tel.: + 43-1-52152 [redacted]

E-mail: dsb@dsb.gv.at

GZ: D155.062
2021-0.870.507

Clerk: [redacted]

Data Protection Complaint

[redacted] (A56ID 290715)

F I N A L D E C I S I O N

The Data Protection Authority decides on the data protection complaint of [redacted] (complainant) of 19 February 2021 against [redacted] (opponent) for an infringement of the right to secrecy (Austrian fundamental right to data protection) as follows:

1. The complaint is partially upheld and it is declared that the opponent has infringed the complainant's right to secrecy by processing his tax, income and bank account details, which the complainant submitted on 26 December 2020 and 27 January 2021, following their request, without any legal basis.

2. The opponent is requested to delete the data referred to in paragraph 1 within a period of four weeks.

3. The remainder of the complaint is dismissed as unfounded.

Legal bases: Article 4, Article 5(1)(c) and (e), Article 6(1)(a) and (e), Article 51(1), Article 57(1)(f), Article 58(2)(c) and Article 77(1) of Regulation (EU) 2016/679 (General Data Protection Regulation, 'the General Data Protection Regulation'). GDPR), Abl. No. L 119, 4.5.2016, p. 1; §§ 1, 18(1) and 24(1) and (5) of the Austrian Federal Act concerning the Protection of Personal Data (DSG), BGBl. I No 165/1999 as amended; §" 1(1), § 2(1), § 5, § 6, § 7(1) and § 21(1)(1) and (6) of the Austrian Financial Market Money Laundering Act (FM-GwG), BGBl. I No 118/2016 as amended.

R E A S O N I N G

A. Arguments of the parties and course of proceedings:

1. The Data Protection Authority was notified of the complainant's complaint of 19 February 2021 by a notification from the Hungarian supervisory authority pursuant to Article 56 in conjunction with Art. 60 GDPR of 20 April 2021.

In summary, the complainant claimed that the opponent had requested from the complainant his personal income and tax return data. It has also requested access to his bank statement. In addition, the data was requested via e-mail, i.e. an insecure channel. The complainant has been a customer of the opponent since 2006 and has notified the opponent of his new address in Budapest two months ago. Upon request of the opponent, the complainant provided information on his tax return and his company registrations. Then the complainant was asked to translate the documents, which the complainant had done. However, the opponent refused to accept them and declared the complainant's credit card invalid due to failure to meet the "Know-your-Customer" (KYC) requirements. In all those years, the complainant had received almost EUR 100.000 from the opponent's credit card.

2. At the request of the Austrian data protection authority, the opponent stated in its submission from 30 August 2021, that as an Austrian bank, it was subject to the due diligence obligations for banks and that, pursuant to Paragraphs 5 et seq. of the the Austrian Financial Market Money Laundering Act (FM-GwG), it was required to obtain certain information from customers in order to prevent money laundering, terrorist financing and similar criminal offences. This includes getting an idea of your customers at regular intervals. This obligation stems from paragraph 7(6), sentence 1, of the FM-GwG. The complainant submitted those documents in Hungarian, so the opponent was legally obliged to insist on a certified translation.

On the basis of Article 6(1)(c) of the GDPR in conjunction with paragraph 7(6) sentence 1 FM-GwG, the opponent is entitled to obtain and process information about the data subjects. Moreover, the complainant was under no obligation to send the data in an unencrypted format. The complainant would also receive documents in password-protected form or by post.

3. By submission of 29 September 2021, submitted by the Hungarian supervisory authority on 2 October 2021, the complainant summarized that it was not clear from the KYC conditions that the complainant would have to provide employment details and income evidence on a regular basis. An official translation costs EUR 100 per page. The opponent did not give instructions to the complainant to upload sensitive documents securely. The opponent requested details by e-mail, which the complainant provided, and therefore the opponent did not act in accordance with the GDPR.

B. Subject of complaint

The subject of the complaint is whether the opponent has thereby violated the complainant in the (Austrian) fundamental right to data protection pursuant to § 1 para. 1 DSG respectively has infringed

Article 6 GDPR (lawfulness of processing) by requesting and processing his tax, income and account data received per e-mail.

C. Findings of the case

1. The complainant has been a customer of the opponent since 2006, which is a bank and credit institution from which he had a credit card.

2. The complainant moved from Vienna to Budapest in 2007 and informed the opponent of this.

3. In December 2020, the complainant informed that he had moved within Budapest.

4. Beginning with 18. December 2020, the opponent requested the complainant to provide information on his relationship with Austria and to provide several documents relating to his income and tax information. The complainant followed this request on 26 December 2020 and 27 January 2021, and submitted his income tax returns as well as a financial statement and a bank statement in Hungarian.

5. After the complainant was not willing to provide the Hungarian documents in a certified translation, the opponent dissolved the business relationship with the complainant.

6. The opponent did not ask the complainant to send the documents in question exclusively by e-mail.

7. In the course of the 14-year business relationship, the complainant has spent approximately EUR 100.000 via the opponent's credit card.

Appraisal of evidence: The findings are based as far as uncontested on the written statements of the parties. The findings on point 4 are based on the correspondence between the complainant and the opponent of 18, 19, 22, 26 and 28. December 2021 and 27 January 2022 submitted by the complainant. Points 2 and 6 are based on the complainant's statement, which was not disputed by the opponent.

D. Legal conclusions

Point 1 of the decision

Pursuant to Section 1(1) of the DSG, every person shall have the right to secrecy (fundamental right to data protection) of the personal data concerning that person, especially with regard to the respect for his or her private and family life, insofar as that person has an interest which deserves such protection. This means the protection of the data subject against the identification of his or her data and the protection against the disclosure of the data obtained about him. In purely conceptual terms, this process therefore presupposes the processing of personal data at the controller.

Pursuant to Section 1(2) of the DSG, restrictions on the right to secrecy are permitted only if the use of personal data takes place in the vital interest of the data subject or with his/her consent, in the case of overriding legitimate interests of another person or where a qualified legal basis exists.

The GDPR and in particular the principles enshrined therein must be taken into account in order to interpret the right to secrecy (cf. decision of the Austrian Data Protection Authority of 31 October 2018, GZ DSB-D123.076/0003-DSB/2018).

In the case of cross-border processing, such as here, there is in any case a violation of the fundamental right to data protection if Article 6 GDPR has been violated.

It must therefore be examined whether the processing of the proceedings can be based on one of the grounds of lawfulness referred to in Article 6 (1) of the GDPR.

Regarding the consent:

In Article 4 (11) GDPR, consent is defined as “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

According to Art. 7 (4) GDPR and taking into account Art. 4 (11) and recital 43 GDPR, consent must be voluntary and must not be linked to the performance of a contract, although this consent is not necessary for the performance of this contract. Consent is involuntary if a disadvantage is to be expected if the consent is not given (cf. the decision of the Austrian Data Protection Authority of 16 April 2019, GZ DSB-D213.679/0003-DSB/2018).

In the present case, the question arises whether the complainant has freely given consent to the processing of his personal data in question or whether it has been valid and complies with the requirements laid down in the GDPR.

The complainant made it clear in his submission that he did not voluntarily consent to the processing of his transmitted data, as he would have expected a disadvantage if his income and financial data were not transmitted.

On vital interests:

In any event, the use of the data in question is not in the vital interest of the complainant.

The legal basis:

The opponent claimed that it was obliged to review its customers under the FM-GwG.

According to Art. 6(1)(c) GDPR, processing is lawful if it is necessary to fulfil a legal obligation to which the controller is subject.

Applicable legislation of the FM-GwG:

Paragraph 5 of the FM-GwG, together with its heading, reads as follows:

Application of due diligence obligations

§ 5. The obliged entities shall apply due diligence obligations towards customers in accordance with § 6 in the following cases:

1. when establishing a business relationship;

Savings deposit transactions pursuant to Section 31(1) of the BWG and transactions pursuant to Section 12 of the Depot Act shall always be regarded as a business relationship;

2. in the case of all transactions not falling within the scope of a business relationship (occasional transactions),

a) the amount of which amounts to at least EUR 15 000 or euro equivalent, irrespective of whether the transaction is made in a single operation or in several transactions between which a link is manifestly present; or

B) which are transfers of funds within the meaning of Article 3(9) of Regulation (EU) 2015/847 of more than EUR 1 000;

if the amount is not known in the cases referred to in point (a) before the commencement of the transaction, the due diligence obligations shall be applied as soon as the amount is known and it is established that it is at least EUR 15 000 or equivalent of euro;

3. for each deposit on savings deposits and at each disbursement of savings deposits, where the amount to be deposited or withdrawn is at least EUR 15 000 or equivalent;

4. if there is a suspicion or reasonable reason to believe that the customer belongs to a terrorist organisation (Section 278b StGB) or that the customer is objectively involved in transactions that serve the money laundering (Section 165 of the Criminal Code — including assets that result from a criminal act of the offender himself) or terrorist financing (Section 278d StGB);

5. in case of doubt as to the authenticity or adequacy of previously received customer identification data.

Paragraph 6(1) and (2) of the FM-GwG, together with the heading, read as follows:

Scope of due diligence obligations

§ 6. (1) The customer's due diligence obligations include:

1. Establishing the customer's identity and verifying identity on the basis of documents, data or information originating from a credible and independent source, including electronic means for identification and relevant trust services in accordance with Regulation (EU) No 910/2014 and other secure remote or electronic identification procedures in accordance with paragraph 4;

2. Establish the identity of the beneficial owner and take appropriate measures to verify his identity, so that obliged entities are convinced of knowing who the beneficial owner is; in the case of legal entities, trusts, companies, foundations and similar legal arrangements, appropriate measures are taken to understand the client's ownership and control structure. Where the identified beneficial owner is a member of the top management level pursuant to Section 2(1)(b) of the WiEReG, obliged entities shall take the appropriate measures necessary to verify the identity of the natural persons belonging to the top management level and shall keep records of the measures taken and of any difficulties encountered during the review operation. An appropriate measure is access to the register of beneficial owners in accordance with § 11 of the WiEReG;

3. Evaluation and collection of information on the purpose and nature of the business relationship;

4. Obtaining and verifying information on the origin of the funds used; such information may include, inter alia, the professional or business activity, income or results of business or the general financial situation of the client and its beneficial owners;

5. Identification and verification of the identity of the trustee and the trustee in accordance with paragraph 3;

6. continuous monitoring of the business relationship, including a review of transactions carried out in the course of the business relationship, in order to ensure that they are consistent with the obliged entities' knowledge of the customer, its business activities and its risk profile, including, where necessary, the origin of the funds;

7. periodically verify the existence of all information, data and documents required by this Federal Act, as well as updating this information, data and documents.

[...]

Paragraph 7(6) of the FM-GwG, together with its heading, reads as follows:

Date of application of due diligence obligations

§ 7. (1) The determination and verification of the identity of the customer, the beneficial owner, the trustee and the trustee (Section 6(1)(1), (2) and (5)) and the collection and verification of information about the purpose and the intended nature of the business relationship and the origin of the funds used (Section 6(1)(3) and (4)) must be made before establishing a business relationship and before carrying out an occasional transaction. The determination and verification of the identity of a natural person authorised to represent (Section 6(1) final part) must be carried out if the latter relies on his or her power of representation. At the beginning of a new business relationship with a legal entity pursuant to § 1WiEReG, the obliged entities must obtain an extract from the register of beneficial owners pursuant to § 9 or § 10 of the WiEReG as proof of the registration of the beneficial owners. At the beginning of a new business relationship with a company, trust, foundation, legal person comparable to a foundation, or with a similar trust-like legal arrangement established in another Member State or in a third country comparable to a legal entity within the meaning of Paragraph 1 of the WiEReG, obliged entities must obtain proof of registration or extract, provided that its beneficial owner must be registered in a register corresponding to the requirements of Articles 30 or 31 of Directive (EU) 2015/849.

[...]

(6) The obliged entities must apply the customer due diligence obligations not only to all new customers, but also to the existing clientele on a risk-based basis at an appropriate time. This is particularly the case where relevant circumstances change in the case of a customer, or where the obliged entity is legally obliged to contact the customer during the relevant calendar year to verify any relevant information about the beneficial owner or owners, or where the obliged entity is required to do so in accordance with Council Directive 2011/16/EU.

Paragraph 21(1)(1) and (6) of the FM-GwG, together with its heading, reads as follows (*emphasis added by the Data Protection Authority*):

Storage obligations and data protection

§ 21. (1) The obliged entities shall keep:

1. Copies of the documents and information received that are necessary for the fulfilment of customer due diligence obligations, including electronic means for identification and relevant trust services in accordance with Regulation (EU) No 910/2014, as well as other secure means of identification remotely or electronically in accordance with § 6(4), for a period of ten years after the end of the business relationship with the customer or after the date of an occasional transaction;

[...]

(6) The processing of personal data on the basis of this Federal Act, for the purpose of preventing money laundering and terrorist financing, is to be regarded as a matter of public interest in accordance with Regulation (EU) 2016/679. The safeguarding of public interests pursuant to Article 23(1) of Regulation (EU) 2016/679 may exist if the refusal to provide information (Section 20(1)) is necessary for the secrecy of transactions for the purpose of exercising Section 16 and Section 17 in order to:

1. enable the obliged entity or the FMA to properly perform his or her duties for the purposes of this Federal Act; or
2. not to impede administrative or judicial investigations, analyses, investigations or proceedings for the purposes of this Federal Act and to ensure that the prevention, investigation and detection of money laundering and terrorist financing is not jeopardised.

On the matter:

As a credit and financial institution pursuant to Paragraph 1(1) of the FM-GwG, the opponent is obliged to comply with the FM-GwG and acts as a credit institution within the meaning of Paragraph 1(1) of the BWG. As such, the opponent is subject to the due diligence obligations under FM-GwG and in accordance with the BWG.

In general, it should be noted that the FM-GwG aims to prevent money laundering and terrorist financing and therefore imposes certain due diligence obligations on credit (banking) institutions.

The opponent's statutory duty of care arises from Paragraph 6(1)(1) of the FM-GwG and includes the 'determination of the customer's identity and verification of identity on the basis of documents, data or information originating from a credible and independent source'.

Paragraph 6(1)(6) of the FM-GwG is one of the key standards in the assessment of legal obligations for the prevention of money laundering and terrorist financing. Accordingly, customer due diligence shall include the continuous monitoring of the business relationship, including a review of transactions carried out in the course of the business relationship, in order to ensure that they are consistent with the knowledge of the obliged entities about the customer, its business activities and its risk profile, including, where necessary, the origin of the funds.

For example, Paragraph 5(1) of the FM-GwG regulates an obligation on the opponent to apply the due diligence obligations laid down in Paragraph 6 of the FM-GwG in the event of establishing a permanent business relationship, whereby this obligation arises according to the materials already before the establishment of the business relationship. The application of the due diligence obligations should therefore already be concluded with the conclusion of the contract (*see Hörtner in Hörtner/Trautmann*, Praxishandbuch FM-GwG (2020) § 5, paragraph 2 (as at 1.10.2020, rdb.at).

At the time of the transfer of the data, the complainant was already a long-standing customer of the opponent, who regularly used the opponen's credit card, therefore the scope of Paragraph 5(1) FM-GwG cannot be considered.

Although the complainant has argued that he spent a total of EUR 100.000 on the credit card during the 14-year business relationship, however, not every transaction constitutes a transaction in favour of the above-mentioned frowned upon purposes.

Nor did the opponent submit that those transactions were occasional transactions or transactions outside a business relationship with an amount exceeding EUR 15.000 or transfers of funds within the meaning of Article 3(9) of Regulation (EU) 2015/847 of more than EUR 1.000. There are no other indications for the opposite. Thus, the scope of Paragraph 5(2) of the FM-GwG is also excluded.

The scope of Paragraph 5(3) of the FM-GwG is also excluded, since there are also no indications here.

Pursuant to Section 5(4) FM-GwG, the obliged party must already apply due diligence measures in the event of suspicion of money laundering or terrorist financing. However, there are no indications to the

complainant regarding money laundering or terrorist financing, nor have they been put forward by the opponent.

Pursuant to § 7(6) FM-GwG, the opponent has to apply the customer due diligence obligations not only to all new customers, but also to the existing customers at an appropriate time on a risk-based basis. This is especially the case if significant circumstances change with a customer.

The complainant has been living in Budapest since 2007, therefore his place of residence has not changed.

The opponent did not put forward any reason why it had to apply due diligence obligations or what relevant circumstances have changed to the complainant that the opponent had to assume a risk of money laundering or terrorist financing.

In this context, reference should also be made to the principle of data minimisation in accordance with Article 5(1)(c) of the GDPR, according to which the processing of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

In addition, both the circular of Austrian Financial Market Authority (FMA) 09/2018 and the case law of the Austrian Federal Administrative Court (BVwG) speak of risk-oriented and appropriate (adequate) measures:

"Client-level risk assessment is the basis for a risk-oriented and appropriate application of due diligence. Obliged persons must be able to demonstrate the adequacy of the measures implemented by the FMA" (cf. circular FMA 09/2018, p. 10).

'The risk assessment procedure installed during the period in XXXX, which made it possible to identify business relationships established by way of distance business which, by their very nature, constitute an increased risk and are also considered to be 'higher risk' under the XXXX internal working instructions, was not appropriate and appropriate in the actual risk assessment of long-distance customers' (cf. BVwG, W210 2000428-1, 19.09.2014).

With regard to the customer with the number XXXX ("XXXX"), XXXX has since 01.09.2010 failed to take risk-based and appropriate measures to verify the identity of the beneficial owner of the customer, so that he is convinced of who the beneficial owner of that customer was (cf. BVwG, W210 2000428-1, 19.09.2014).

There is no evidence from the findings established and from the arguments of the parties that the complainant has placed a conspicuous conduct or conspicuous transaction or that he was at all assessed as a risk by the opponent. Therefore there are no indications or reasonable grounds to believe that the complainant belongs to a terrorist organisation within the meaning of Paragraph 278b of the Austrian penal code (StGB) or that he is objectively involved in transactions that serve the money laundering pursuant to Section 165 of the StGB — including elements of assets resulting from a criminal act of the offender himself — or the financing of terrorism pursuant to § 278d StGB.

Regarding the legitimate interests:

The opponent has also not raised any legitimate interests that outweigh an infringement of the right to secrecy.

Result:

The Data Protection Authority therefore concludes that due to the examination of the requirements of the FM-GwG, the application of due diligence obligations to the relevant data processing (income and tax information of the complainant) was not applicable. Therefore, the processing in question of the complainant's personal data took place without the existence of a qualified legal basis.

The decision was therefore appropriate.

Point 2:

Since the conditions for the processing of the data subject to the procedure were not met, they were processed unlawfully from the beginning, which is why they must be deleted in accordance with Article 17(1)(d) of the GDPR.

The data protection authority therefore makes use of its power in accordance with Article 58(2)(g) of the GDPR (for the admissibility of an official order see the decision of the Austrian Federal Administrative Court of 4 June 2019, GZ W214 2213623-1).

Point 3:

Insofar as the complainant complains that the opponent has violated his privacy, since his financial data had been requested via an unsecured channel (by e-mail), no specific violation of rights was identified, especially since the GDPR cannot be derived from a legal claim for compliance with certain data security measures (decision of the Austrian Federal Administrative Court of 9. December 2021, GZ W214 2225733-1).

In addition, there are no indications that these emails have been disclosed to unauthorized third parties.

It was therefore appropriate to decide in accordance with the judgment.

23. Juni 2022

Für die Leiterin der Datenschutzbehörde:

[redacted]