

GZ: DSB-D123.482/0005-DSB/2019 from April 2nd, 2019□

[Note editor: Names and companies, legal forms and product names,□

Addresses (incl. URLs, IP and e-mail addresses), file numbers (and the like), etc.,□

as well as their initials and abbreviations can be used for pseudonymization reasons□

be abbreviated and/or modified. Obvious spelling, grammar and□

Punctuation errors have been corrected.]□

NOTICE□

S P R U C H□

The data protection authority decides on the data protection complaint of Mag. Michael□

A*** (Appellant), represented by Attorney Peter B***, August 27□

2018 against N*** Aktiengesellschaft (Respondent), represented by C***□

Rechtsanwälte GmbH, due to infringement of the right to secrecy and infringement□

the information obligation as follows:□

- The appeal is dismissed.□

Legal bases: Sections 1 (1) and 24 (1) and (5) of the Data Protection Act (DSG),□

Federal Law Gazette I No. 165/1999 as amended, Art. 4 Z 1 and 2, 6 and 13 of Regulation (EU) 2016/679□

(General Data Protection Regulation - GDPR), OJ No. L 119 of 4.5.2016, p. 1.□

REASON□

A. Submissions of the parties and course of the proceedings□

1. In a letter dated August 27, 2018 initiating the proceedings, the□

Complainant violated the duty to provide information and the legality of the□

Processing in accordance with Art. 6 GDPR and essentially argued that he had the□

Habit of his purchases from the private labels and subsidiaries of the D***□

International AG mainly cashless payments by card. The Complainant□

do not have a valid customer card of the respondent. With every cashless□

Payment process in the branches of the Respondent will be before the actual□

payment process at the card terminal, a regular customer query is displayed, in which the automated data processing for the complainant without a doubt manifest. It was completely unclear to the complainant whether there was a link between the "regular customer" query for cashless payments and the customer loyalty program exists and whether there are group-wide links.

In particular, it seems unclear which data from the Respondent at this

Regular customer query would be collected or stored. By email dated June 11, 2018

the complainant asked the respondent to provide information about the

to grant the above data processing. I have the answer

Respondent informed the following: "When paying with a debit card

queried by the debit card terminal whether there is a so-called

'Company bit' is stored, i.e. whether the customer card is stored on the ATM card.

No data is processed in this context. It doesn't come to anyone

Allocation of payment data. The mere query as to whether there is one on the ATM card

stored on the customer card is by no means unlawful." The complainant never

his consent to the automated regular customer query by a customer terminal

granted to the branches of the Respondent. The complainant wrote

of June 12, 2018 this unlawful data processing expressly

objected. The Respondent failed to do so, according to her

Information obligation (as part of the data protection declaration) to state the purposes for

which the complainant's personal data would be processed. the

The regular customer query shown is clearly a processing of data

to qualify. According to Art. 6 Para. 1 GDPR, data processing is only then

lawful if one of the conditions of subparagraph lit. a to f is met. in the

The result of the data processing is neither from the data protection declaration nor from one

consent covered.

2. With a statement dated October 30, 2018, the Respondent led□
summarized, it operates in its capacity as a retail business□
with branches throughout Austria a customer loyalty program, for which by the□
Respondent customer cards would be issued. At the request of the customer□
the debit card can also be used as a customer card. In such a case will□
The "company bit" is activated once on the ATM card and a memory area is activated.□
The initialization of the "company bit" on the ATM card takes place at the cash registers□
Respondent. In the case of cashless payment transactions, the payment terminal is used□
checks whether the "company bit" function is activated. If so, it will be checked whether□
the memory area mentioned is activated on the ATM card. be this function□
not activated, no further queries or data processing would be carried out□
will. As information to the customer who uses the ATM card, the□
Text "Regular customer query carried out" displayed on the ATM card terminal. Included□
but, contrary to the complainant's representation, would not be personal□
data processed. Only if the memory area is activated will from□
the respondent - in a second step - a numerical code stored there□
read from the chip. Only this numerical code enables the result - after various□
technical intermediate steps - the assignment of the ATM card as a customer card to the□
respective member of the Respondent's customer club. Because in the representational□
If no data processing takes place because the complainant is not on□
The Respondent's customer loyalty program is involved□
Respondent not responsible for data processing and they would□
therefore not the associated obligations such as information obligations in particular□
in accordance with Art. 13 and 14 GDPR.□

3. In a letter dated March 5, 2019, the Respondent supplemented its statement□
in technical terms and transmitted the processor agreement between□

the operator of the card terminal and the respondent. Summarized

the Respondent stated again that no processing

personal data of the complainant had taken place. About misunderstandings

regarding cashless payment and data processing

To prevent the Respondent and to comply with the transparency requirement in accordance with Article 5 (1) lit

GDPR even better, the Respondent has her

Data protection declaration to include a corresponding paragraph on the use of the

Debit card added as a customer card for the customer loyalty program. This is

also subsequently brought to the attention of the complainant.

4. As part of the hearing of the parties, the complainant led by letter dated

March 26, 2019 in relation to the information obligation pursuant to Art. 13 GDPR

summarized from that it was "irrefutable fact" that the Respondent

before changing the data protection declaration, their obligation to provide information in accordance with Art. 13 GDPR

hurt. To protect his legitimate interests, he desires

Complainant, the determination of the breach of the information obligation. In relation to

The complainant essentially explained the violation pursuant to Art. 6 GDPR,

that the Respondent processed personal data without a

appropriate wording in their privacy policy. the to

The "regular customer query" criticized by the complainant has been right since the beginning

December 2018 no longer as an "insert" at the Respondent's payment terminal

been displayed. However, two separate data queries would very well be carried out.

The complainant assumes that the Respondent's unlawful

Data processing simply continued without adding the word "regular customer query".

have. Furthermore, personal data would be processed. through the

Querying the so-called "company bit" can be assigned to a natural person

an identification number or their identification done, this also with the

"Pseudo-anonymization" is the case. The sense and purpose of the regular customer query is

to identify a natural person and the existence of a membership in

Check the Respondent's customer loyalty program. It's about

the query of the "company bit" by no so-called "pseudo-anonymization", since straight

this should enable the attribution of a natural person. the

Querying the so-called "company bit" is therefore always considered processing

to qualify personal data.

5. In addition, the complainant stated in a letter dated March 28, 2019 that

it has now emerged that the Respondent has changed its privacy policy

have not changed. The Respondent did this simple task within

not done for three weeks. The complainant is therefore still iSd

Information obligation according to Art. 13 DSGVO complained.

B. Subject of Complaint

The subject of the complaint is the question of whether the Respondent

Query of the "company bit" as part of the regular customer query for cashless payment

violated the complainant's right to secrecy. Furthermore

The question arises whether the complainant due to an insufficient

Privacy policy related to the "regular customer query" at the payment terminal in

his right to information according to Art. 13 GDPR has been violated.

C. Findings of Facts

The Respondent is a retail company

branches throughout Austria. The Respondent operates in the course of this activity

Customer loyalty program that customers present one of the

Customer card to be issued by the Respondent, discounts and other advantages

granted. At the customer's request, the ATM card can be used as a customer card

will.

If the debit card is used as a customer card, the "company bit" on the

Customer's ATM card activated.

The file "EF_RFU2" is located on the ATM cards issued in Austria,

consisting of 196 bytes. It contains the regular customer number, the dealer bitmap

and the dealer data. Of these, 8 bytes are used for the regular customer number, 8 bytes for

the bitmap for company bits, and 180 bytes for the dealer data.

The "EF_RFU2" file is neither freely readable nor freely writable.

The "EF_RFU2" file and the bitmap appear as follows:

[Note: The graphic files originally reproduced here

(Screenshots) with a tabular representation of the files in question can be found in the

RIS are not shown.]

A byte consists of 8 bits (note: one bit corresponds to one character). bytes 0 to 7

therefore a total of 64 bits, with only bit 1 for using the

Regular customer query is assigned to the Respondent. All other bits

correspond to the value 0 and are not assigned. In the course of the regular customer query at

Bit 1 of the payment terminal is used to determine whether the debit card for the

The Respondent's customer loyalty program was initiated.

If the regular customer function is activated on the ATM card, the

Initialization the bit (bit 1 of the bitmap) set to 1 and the part of the cash register

transmitted data is written to the card. This initialization takes place

only if the cardholder actively supports the use of the respective

regular customer program and has agreed to use the ATM card instead

the customer card wishes.

In the course of querying regular customers, the cash register can use the terminal

query whether the regular customer function on the cardholder's ATM card

is being used. The terminal then reads the encrypted data from the card

and checks whether the correct company bit is set. After the check has been carried out, this will be sent

Terminal either only the message "not a regular customer" or "regular customer" to the

Cash register return. For this purpose, the technical process is as follows

represents:

[Note: The graphic file originally reproduced at this point

(Screenshot) with a tabular representation of the process in question can be found in the

RIS are not shown.]

As part of the regular customer query, the cash register sends the order record "Stkf-

Query without card return" to the terminal:

[Note: The graphic files originally reproduced here

(Screenshots) with a tabular representation of the process in question can be found in the

RIS are not shown.]

The terminal's response record to the cash register does not contain customer data, but

only the terminal ID, date and time.

Only in the event that the ATM card was initialized as a customer card, the

data written during initialization is returned to the cash desk.

The Complainant participates in the Respondent's customer loyalty program

not part. The "company bit" is not activated on his ATM card (i.e. set to 0).

Evidence assessment: The findings regarding non-participation on

The Respondent's customer loyalty program is based on

consistent submissions of the parties to the proceedings in their letters to the

Data Protection Authority. The findings regarding the technical process of the

Regular customer query based on the statement of the Respondent of

March 5, 2019, which is comprehensible and understandable even for laypeople

Functionality of a company bit and the technical process of activation

and non-activation of the "company bit" as part of the regular customer query

has. The complainant also agrees with these statements in the context of the hearing of the parties□

not opposed. The complainant's argument that a□

The main purpose of the regular customer query for cashless payments is□

Establishing a personal reference may not be convincing either, since this query□

says nothing about whether the customer generally participates in the customer loyalty program.□

In addition to using the ATM card as a customer card, the Respondent gives□

separate customer cards.□

D. In legal terms it follows that:□

The data protection authority assumes that a data subject refers to each□

Provision of the GDPR also apart from the rights of data subjects under Chapter III□

may, if this results in a possible violation of the right□

Confidentiality according to § 1 Para. 1 DSG (cf. the decision of□

30 November 2018, GZ DSB-D122.931/0003-DSB/2018). In the present case□

the complainant's arguments with regard to a violation of the□

Information obligation according to Art. 13 DSGVO as well as regarding the submission of a□

Violation according to Art. 6 GDPR in relation to the right to secrecy according to § 1□

check DSG.□

Processing of personal data:□

According to § 1 Para. 1 DSG everyone has, in particular with regard to the respect of his□

Private and family life, right to secrecy of those concerning him□

personal data, insofar as there is a legitimate interest in it. underneath□

is the protection of the data subject against the determination of his data and the protection against the□

to understand the transmission of the data determined about him. Purely conceptually, this□

Process thus processing of personal data by the person responsible□

in advance. Art. 1 para. 1 GDPR also stipulates that the regulation contains provisions on□

protection of natural persons in the processing of personal data.□

Prerequisite for a violation of the right to secrecy according to § 1 DSG

as well as information according to Art. 13 DSGVO can possibly exist at all

thus the processing of personal data by the person responsible.

Personal data are according to the definition of Art. 4 Z 1 DSGVO

any information relating to an identified or identifiable natural person

relate. A natural person is considered to be identifiable if

directly or indirectly, in particular by means of assignment to an identifier or to several

special characteristics can be identified.

Any processing is carried out with or without the aid of automated procedures

Process or any such series of processes understood in connection with

personal data such as the collection, recording, organization,

Arranging, storing, adapting or changing, reading out, that

query, use, disclosure by transmission, dissemination or any

other form of provision, matching or linking, restriction,

erasure or destruction (cf. Art. 4 Z 2 leg.cit).

In the matter:

The data processing that is the subject of the proceedings relates to the query regarding the

Regular customer status in the course of cashless payment at a retail checkout

Respondent. In this case, an order is sent from the cash desk to the

payment terminal sent. This then reads out whether bit 1 in the file "EF_RFU2"

is enabled or has the value 0. In the present case, the

Complainant does not participate in the customer loyalty program of the Respondent,

which is why no customer card is activated on his ATM card. the

Handelskasse therefore receives cashless payment by the complainant dated

Terminal only sent the message "not a regular customer".

The reply sentence of the terminal at the Respondent's checkout does not contain any

customer data, only the terminal ID and the date and time. At the□

Note "not a regular customer" and the terminal ID is the date and time□

without the addition of further data, there is no information relating to a□

identified or identifiable natural person. More data will be□

not processed in the processing that is the subject of the procedure.□

As a result, the complainant - for lack of processing of his□

personal data - in the course of the regular customer query with the cashless□

Pay neither in his right to secrecy according to § 1 DSG in conjunction with Art. 6 DSGVO,□

nor are violated in his right to information according to Art. 13 DSGVO.□

Any processing of personal data in the context of cashless□

Paying is not part of the proceedings.□

Since the complaint turns out to be unjustified, it was in accordance with Section 24 (5) DSG□

to reject.□