GZ DSB-D216.697/0011-DSB/2018 from 26.11.2018

[Note editor: names and companies, legal forms and product names, addresses (incl.

URLs, IP and email addresses), file numbers (and the like), etc., as well as their initials and

Abbreviations may be abbreviated and/or changed for reasons of pseudonymization.

Corrected obvious spelling, grammar, and punctuation errors.]

NOTICE

S P R U C H

The data protection authority decides on the data protection complaint of Dr. Richard A***

(complainant) of March 23, 2018 against the Federal Ministry of Finance

(Respondent) as follows:

1. The complaint is upheld in the main question and it is established that the

Respondent thereby infringed the complainant's right to secrecy,

by using this personal data of the complainant for the purpose of reconnaissance

suspected of committing criminal offences.

2. The complaint is rejected in the ancillary questions.

Legal basis: §§ 1, 6 para. 1 Z 2, 8 para. 4 and § 14 of the Data Protection Act 2000 (DSG 2000),

Federal Law Gazette I No. 165/1999 in the version of Federal Law Gazette I No. 83/2013; Section 24 (1) and (5) of the Data Pro

No. 165/1999 as amended.

REASON

A. Submissions of the parties and course of the proceedings

1. With a submission dated March 23, 2018 as part of a control and ombudsman procedure in accordance with Section 30

DSG 2000, the complainant submitted in summary that he was an employee of [note

Processor: Complainant's office name] of the Respondent. If employees

so does he himself, on tax data in the so-called system AIS-DB2 ("delivery information system

of the Federal Government"), these accesses would be logged. This log data

However, according to § 14 DSG (probably meant: DSG 2000) would have to be deleted after three years. The

Office for Internal Affairs of the Respondent (hereinafter: "BIA") check these accesses
(Log file analyses) not only according to the DSG, but also use these log file analyzes for official
and criminal purposes. The respondent saves the log file data without reason and
nationwide over a much longer period of time than the permitted three years. Also older data
would serve as servants without a judicial or criminal order from the public prosecutor's office
held and processed by the respondent. In the specific case Gz. BMF
*03*4/00*4-BIA/2017 the respondent has so far denied all access to the files. the
Data protection authority may the legality of the storage and use of the log file data
checked by the BIA or the respondent. Attached to the input is a screenshot that
Events from 2011 relating to the complainant.
2. In a statement dated May 28, 2018, the Respondent summarized that
this on October 2, 2017 a review of the access made by employees of the finance department
to the AIS in respect of a specific taxpayer and all legal entities
which this taxpayer would be involved, caused by the BIA. The establishment of the BIA
takes place on the basis of § 7 BMG, whereby the BIA also monitors the legality of
access to the Respondent's databases. Organizationally, the BIA
according to the Respondent's current business division in Section I of the
Respondent settled. The background to this log file analysis is that a member of parliament
National Council would have made exact tax data of this taxpayer public, so that the suspicion
a criminal act, inter alia, according to §§ 302, 310 StGB and to unauthorized access to the
database existed in the AIS. The log file analysis carried out by the BIA as a result
revealed that, in addition to other employees of the respondent, the complainant also referred to the
accessed data. The question of who accessed the database is a necessary one
Preliminary question to clarify the question of whether unauthorized access has occurred.
The fact that access by employees of the respondent to the AIS in log files
would be logged and documented, do not constitute an interference with the basic rights of these employees

Secrecy of your personal data, but is one in § 14 para. 2 Z 7 DSG 2000

expressly provided measure to ensure data security. With a note on the

Judiciary of the DSK it was stated that the use of this log data to check a

concrete suspicion of illegal access and illegal use of the control data

is in any case covered by Section 14 (4) DSG 2000. Also, from § 14 paragraph 5 DSG 2000 no

Obligation of the client can be derived, the log data at least after three years

Clear. This three-year period may be deviated from to the extent that the

The dataset concerned by logging is permitted to be deleted earlier or retained for a longer period of time

become. This means that the log data on access to a data set in the AIS as long as

could be retained than the underlying dataset was to be retained in the AIS. be it

to state that the storage of the log files (protocol data) about access to the AIS in concrete terms

Case beyond the three-year period is admissible because also of the logging

continue to store the affected database and use the log data in

Connection with the suspicion of unauthorized access and use of the data subject

database is in any case permissible. Which position within the respondent with the

Checking the log files is commissioned is a question of the business division according to § 7 BMG. in the

Furthermore, with reference to the case law of the DSK, in view of § 8 para. 3 no. 6 DSG 2000

confidentiality interests worthy of protection have not been violated in the present case, since the

Log data and their verification only affect the exercise of the public function

had that the complainant held as a tax officer and in which he was too special

Obligation to comply with the law. A violation of the rights of those affected would therefore not exist.

3. With the order to remedy defects dated July 9, 2018, the data protection authority pointed out that

according to the legal situation applicable from May 25, 2018, the previous one according to § 30 DSG 2000

Control and ombudsman procedure as a complaint procedure according to § 24 DSG, Federal Law Gazette I No. 165/1999

as amended, is to be continued and the complaint is to be specified in accordance with Section 24 (2) DSG.

4. The complainant submitted with opinions dated August 4, 2018 and September 27

in summary, first of all that there was a violation of Art. 6 GDPR (§ 14 DSG 2000). In
Specification of the facts was stated that a member of the National Council in the course
a parliamentary request in early October 2017 from Mr. Walter F***'s tax data
have. In the course of this parliamentary question would be corresponding comprehensive
Reporting in various media. In the course of the professional activity of
The complainant's official reason for accessing various tax data from Mr. Walter
F*** on December 6, 2016 in the AIS. The AIS is an application with various tax
"Collections" and also other documents concerning taxpayers. Legally or in
This database is not anchored or regulated by regulation. What ultimately the AIS-DB2 in
The meaning of the DSG cannot be seen from the Respondent's statements. Therewith
must first be made clear by the Respondent that the compilation AIS-DB2 is actually in
falls under the DSG in its entirety. Noting a decision by the Independent
Finance Senate (hereinafter: "UFS"), the complainant explained that in this decision
Working device and the storage in it will be referred to as "legal nullity" and the
Respondent had to explain in more detail why log files were kept at all. May be
the AIS-DB2 no, or only a partial application, which falls under § 14 DSG 2000, is one
Logging by means of log files is (in part) not permitted on the merits and therefore
unlawful.
In October 2017 and in the course of the National Council elections and the media
Reporting, there was increased pressure from politicians, the "F *** case" before the
having to explain the National Council election. For this purpose, on October 4, 2017, the
Respondent to the Economic and Corruption Public Prosecutor's Office (hereinafter: "WKStA")
been. Almost at the same time, the Respondent issued an investigation order to the BIA. It
an analysis of the data access to the tax number of Mr. Walter F*** should be carried out.
Furthermore, all legal entities in which Mr. Walter F*** is involved should also be one
analysis for unjustified data access. Corresponding screenshots showing this

documenting internal correspondence are attached to the file. The complainant refers to this as “first

Respondent's order to investigate his person".

The Respondent thus has an investigation order under Section 310 of the Criminal Code under cover

of the log file evaluation according to the DSG 2000. The Respondent is responsible for investigations

Criminal Code offenses not responsible. According to § 14 para. 2 Z 7 DSG 2000, a log is to be kept so that

actually performed usage processes, such as in particular changes, queries and

Transmissions are traced to the necessary extent with regard to their admissibility

could. Typically, a system logs all authentication attempts (especially

failed logins), but do not keep a record of which user is listed and when

which data set I have accessed. This is mainly due to the fact that the

information security is not concerned with questions of the legality of data use. Under

A note on the judicature of the DSK was that a search for the respondent

or the BIA according to offenders, a group of offenders or a perpetrator by means of log file data after

DSG 2000 - as in the present case - is inadmissible. That the Respondent the log data

according to the DSG 2000 also for "criminal justice" - without a public prosecutor's order and without

judicial approval - would also result clearly and comprehensibly from the

Criminal act of the StA Vienna. In this process, the team leader of the BIA, ** Peter I***, would have had no

communicated to the Vienna Public Prosecutor's Office without any legal basis, as requested by the public prosecutor,

that the circle of perpetrators could be narrowed down to four people on the basis of internal surveys. A

A corresponding screenshot, which documents this correspondence, is attached to the file.

The use of log data analysis to obtain leads or evidence

for the punishability of a data access - from a different aspect than the directly official - is

only permitted in the cases listed in Section 14 (4) DSG 2000, these would be the

"Preventing or prosecuting a crime according to § 278a StGB (criminal organization) or

a crime punishable by imprisonment for a period exceeding five years”. the

Further use of the evaluation results of the log data for the purpose of investigation

Section 310 of the Criminal Code represents an inadmissible extension of the original purpose of use, since according to

§ 14 para. 4 DSG 2000 further use "for a reason other than that of examining the

Authorization to access" would be considered incompatible with the original purpose of the investigation. through the

Use of the log data for the search for criminal offenses is therefore in the right to

The complainant's secrecy was inadmissibly interfered with.

In addition, there is also a "second investigative order by the respondent against the

complainant". So the ** T*** gave the order on October 5, 2018 by telephone, a

Conduct an overall analysis of the complainant. Thus be to the person of

Complainant an "overall screening" of the last at least 7 years has been carried out. At the

October 10, 2017 he was on the "case F ***" by organs of the BIA with reference to criminal offenses

been subpoenaed. The criminal proceedings, which the respondent to the StA u.a. against the

person of the complainant had initiated, was otherwise discontinued. Nevertheless arise

here, too, it is clear that the complainant is being investigated on the basis of criminal law

had been and the log data had been used illegally for the purposes of the Criminal Code.

From § 14 para. 4 in conjunction with para. 5 DSG 2000 it follows that during a three-year period

Period of time log data should be used to establish the legitimacy of access to the through

Access logging to control secured database and in the absence of more detailed information

statutory regulation of any kind that the client of the data application deems appropriate,

whereby the principle of proportionality and the prohibition of excess apply as a limit. On the one hand they would be

3 years exceeded and on the other hand against the principle of proportionality or the prohibition of excess

been violated because an overall analysis would have been carried out over 7 years.

Another application of the Respondent would be the so-called "financial applications".

In this regard, there had also been an unlawful interference with the complainant's rights. for

such an evaluation would include the personal identification, the e-mail address, the

Social security number and first and last name of the employee are required. Both

Financial applications have the respondent or the BIA an inadmissible dragnet

performed. An analysis of log data for the purpose, not just the legality of

to check data access, but according to certain patterns in the behavior of those authorized to access

to search that would allow conclusions to be drawn about otherwise illegal behavior of the persons concerned,

in any case exceeds the legitimate control purpose described in Section 14 (4) DSG 2000. In

Another document from the Respondent or BIA shows that with the help of

of log data according to the DSG and with the help of tax data, which according to § 48a dem

would be subject to "tax secrecy" following any "potential criminal offences".

Complainant" would have been wanted. A corresponding screenshot of this internal

Correspondence documented, attached to the file. In addition, the Respondent had

Order given to search for queries regarding the U*** Group, which is related to the subject

thing would have nothing to do with. In the "BIA-Akt" it is stated that on the part of the

complainant did not give any access (probably meant: concerning the U*** group).

In addition, the application is made to determine by way of a notice that "the log file decree of the

BMF of June 21, 2017 BMF-320700/0004-I/1/2017 on the basis of the DSG is illegal because it also

includes legal entities and partnerships that do not fall under the scope of protection of

§ 1 DSG fall".

5. The Respondent replied in summary in a statement dated September 28, 2018,

that the facts fall within the temporal scope of the DSG 2000 and thus before the

GDPR fall. In terms of substantive law, the provisions of the DSG 2000 would therefore apply.

With reference to the judicature of the DSK, the use of log data for the purposes of

Control of the admissibility of the use of the database according to § 14 paragraph 4 DSG 2000 permitted

and there would be a violation of the fundamental right to data protection of the employee concerned by the

Screening of the complainant justified by § 14 para. 2 no. 7 DSG 2000,

in particular with regard to § 8 para. 3 no. 6 DSG 2000. In addition, be from the

Competence of the data protection authority for matters of data protection no control authority

to other authorities. It also corresponds to the judicature of the OGH on § 85 GOG,

that the use of data in court proceedings is justified if the data

conceivable subject matter of the proceedings, but it is not the purpose of the proceedings pursuant to Section 85

GOG is to control the upstream court process. The extensive explanations of

Complainant to administrative procedure would therefore go nowhere, because it does not matter

the data protection authority is to control this procedure.

Contrary to the complainant's statements, the AIS would very well contain personal data

data are recorded. The DSK has already dealt with complaints in connection with the AIS

dealt with and decided on the content using the DSG 2000. The part of

The decision of the Independent Finance Senate mentioned by the complainant makes statements on the

Use of data from the "AIS-DB" as evidence in the tax procedure, from which no

it can be deduced that the AIS does not contain any personal data.

On October 2, 2017, the Respondent had a review carried out by employees of the

Finance departments access the AIS with regard to a specific taxpayer and

of all legal entities in which this taxpayer was involved.

It is noted that a statement of facts was sent to the WKStA on October 4, 2017

(concerning UT because of § 310 StGB). The termination of the investigation against the

Complainant because of § 302 StGB was made with the notification of the StA Vienna on April 23, 2018.

Background to this review, initiated by the respondent on October 2, 2017

AIS access made is that – after a member of the National Council exact tax data

made this taxpayer public - there was a suspicion that employees of the

Respondent's unauthorized access to the database of the AIS with regard to this

taxpayers would have made, which is why the initial suspicion of criminal acts

have passed. There is also an inevitable result in the event of unauthorized access to AIS databases

the suspicion of the existence of a breach of official duty iSd §§ 43 f BDG 1979. Therein a by the

Respondent issued investigation order according to § 310 StGB "under the guise of

Log file evaluations according to the DSG 2000" is just as misguided as the insinuation that in

this examination procedure carried out (examination by means of log file analysis, whether not official

initiated access to tax data of a taxpayer would have taken place) is a criminal offence

procedure to recognize.

The BIA is responsible for monitoring the legality of access to databases

Respondent. Furthermore, the BIA is responsible for examining concrete suspected cases

as to whether there is an obligation to report under Section 78 of the Code of Criminal Procedure. The one carried out by the BI

Log file analysis showed that the complainant - along with other employees of the

Finance departments – accessed the data. The fact that access by employees of the

Respondent to the AIS would be logged and documented in log files, do not constitute an intervention

in the basic right of these employees to secrecy of their personal data, but

is a measure expressly provided for in Section 14 (2) Z 7 DSG 2000 to ensure the

data security. With reference to the judicature of the DSK, it follows from this provision that

that the general, ongoing control of the log data is a legal obligation of the

client, which exists entirely independently of actual incidents. The ones from

Analysis of his query behavior ("overall screening") and the examination cited by the complainant

of the access behavior in individual cases (“taxable group”) is determined by the BIA with regard to the

Legality or permissibility of access to BMF databases for purely business-related purposes

Queries are made. With regard to the period of storage of the log file data, reference is made to the previous

Proceedings referenced.

6. In a statement dated October 30, 2018, the complainant submitted in summary that

the Respondent or the BIA allowed him to inspect the files for a period of six months

8000-page BIA file refuse. If the inspection of files obviously concerns DSG matters, the

to influence the data protection authority so that the files can be inspected in a timely manner. It will

Therefore, the request was made that the data protection authority decide whether the

Procedure of the BIA, which obviously affects the DSG, in the competence of the data protection authority

cases. It is unclear what role the BIA has in the sense of the DSG. The BIA sees itself as “extended

Arm” of the StA Vienna. Even after reporting to the StA Vienna, the complainant was on base

of the BDG have been heard by the BIA.

Furthermore, the respondent refers to the case law of the DSK from 2005, meanwhile

technically, however, some things have changed. In addition to DB2 would be the financial applications

been massively expanded and partially implemented in the DB2, so that the statements of the time

DSK for DB2 would be outdated from a technical point of view.

The data protection authority may also find that the respondent is unlawful

Log data of employees iSd § 14 Abs. 2 Z 7 DSG 2000 create, save and misappropriated

use which "do not contain any data within the meaning of § 1 DSG (personal data) and therefore not

may be subject to logging and recording.” In addition, the

Respondent Log data according to the DSG with tax data according to the BAO (which is defined by § 48a BAO

would be protected) and link tax documents together to turn after any

investigate potential criminal offenses committed by the complainant.

B. Subject of Complaint

In accordance with the defect rectification order from the data protection authority of July 9, 2018

In his statement of August 4, 2018, the complainant initially claimed a “violation of Art. 6

GDPR (§ 14 DSG 2000)” but subsequently limited himself to one

Infringement of the right to secrecy according to § 1 Para. 1 DSG.

Based on the submissions of the complainant, the main question is therefore whether the

Respondent violated the complainant's right to secrecy by

Protocol and documentation data concerning the complainant in a with § 8 para. 4 DSG 2000

used in an incompatible manner.

As ancillary question 1, the complainant's application is to be dealt with, with a notification about it

to discuss whether the respondent is also unlawfully creating log data from employees,

stored and used for purposes other than intended.

As ancillary question 2, the complainant's application is to be dealt with, in terms of a notification

to discuss whether the "procedure of the BIA" falls within the competence of the data protection authority.

As ancillary question 3, the complainant's application is to be addressed by official decision,

that "the log file decree of the BMF of June 21, 2017, GZ BMF-320700/0004-I/1/2017, on the basis of

DSG is illegal because it also includes legal entities and partnerships, which

do not fall under the scope of § 1 DSG".

C. Findings of Facts

1. The Complainant is an employee of the Respondent. After known in 2017

was that exact tax data of a taxpayer were made public, the headed

Respondents took appropriate action in October 2017. The database of

The federal tax information system (“AIS”) should be based on an analysis of the log data

unauthorized access by employees of the respondent with regard to this taxpayer

checked and illegal accesses investigated. The Office of Internal Affairs (“BIA”)

is an internal organizational unit of the respondent and was involved in clarifying this incident

essentially involved. The complainant has access to the AIS or to the data set of this

taxpayer. The log file analysis carried out showed that - in addition to other employees of the

Respondent - also the complainant on the data of the named taxpayer in the

had accessed past.

Evidence assessment: The findings, which are undisputed in this respect, are based on the opinion of the

Respondent dated May 28, 2018 and the complainant's statement dated

August 4, 2018.

2. The Respondent used these log data concerning the Complainant

October 2017 also to the suspicion of committing a crime, in particular with regard to § 310

StGB to investigate.

The Respondent returned on October 24, 2017 and November 2, 2017 with regard to the internal

Surveys report to the StA Vienna. On November 2, 2017, the Respondent reported to the

StA Vienna that "the group of perpetrators can be narrowed down to four people on the basis of internal surveys".

At this point in time, there was already a corresponding procedure at the StA Vienna for the GZ. *3UT *2*2/17n

pending.

Evidence assessment: These findings result from the submitted documents

Parties to the proceedings, in particular the complainant's statement of August 4, 2018 including

Side dishes.

D. In legal terms it follows that:

D.1 On the legal situation

This complaint is procedurally based on the new legal situation in accordance with Section 24 (1) and (5) DSG,

Federal Law Gazette I No. 165/1999 as amended. In terms of substantive law, however, the matter is after the October

2017, the date or period of the alleged violation of the right to confidentiality,

applicable provisions of the DSG 2000, Federal Law Gazette I No. 165/1999 as amended by Federal Law Gazette I No. 83/2013

D.2 On the competence of the data protection authority in the main question

The Respondent submits that the data protection authority in the present main issue

is not responsible for the decision, refers to the stRsp of the data protection authority

“Excessive prohibition” and carries a notice from the former data protection commission (hereinafter: “DSK”)

of December 16, 2005, K121.040/0018-DSK/2005.

However, the Respondent is countered with the fact that the main question in question is not

refers to the conduct of the procedure or the result of the procedure (such as the result of a

administrative or criminal proceedings) of other competent authorities.

Rather, it must be checked whether the log data relating to the complainant is in accordance with § 14

Para. 4 DSG 2000 agreed manner were used.

Furthermore, it should be pointed out that in the - cited by the Respondent himself -

DSK decision of December 16, 2005, the determination was requested that the "suspicion of

Abuse of office was never given” or it was requested to check whether “about the content of a

Disciplinary report is based on facts and these facts have been legally correctly assessed" and

the DSK dismissed the complaint with reference to the judicature of the prohibition of excess

has. In the same decision of December 16, 2005, the DSK went with regard to the use of

Log data for the purpose of checking operator tests, however, precisely from one area of responsibility

and dealt in detail with the provision according to § 14 para. 4 DSG 2000.

The data protection authority is therefore responsible for the main question in question.

D.3 Regarding the competence of the data protection authority in subsidiary question 1

If the complainant requests that a decision be taken on whether the

Respondent unlawfully also creates, stores and "log data of employees".

misused, it must be countered that the complainant is not a representative

of all affected employees of the respondent and such a "popular lawsuit" (i.e. a

Complaint brought by someone who is not the only one affected) is not admissible (cf. the

DSK notification dated March 30, 2012, K121.765/0008-DSK/2012).

This is clear from the fact that a complaint under Section 24 (1) DSG (or Section 31 (2) DSG 2000) can only be made by

can be made of a person who claims, in his or her jurisdiction, from the actions of a

to be affected by data protection law. In the present case

to limit the object of the complaint to the fact that the use of personal data by

Complainant by the Respondent is up for discussion

The appellant's application was therefore to be rejected in accordance with the verdict.

D.4 Regarding the competence of the data protection authority in subsidiary question 2

If the complainant requests that a decision be taken on "whether the procedure of the

BIA, which obviously affects the DSG, falls within the competence of the DPO", so must in this regard

first be differentiated:

In point D.2 it has already been stated that the data protection authority is responsible for the main question.

If the complainant brings up the "proceedings of the BIA" and subsequently submits that the

Respondent denied him access to the "over 8000-page BIA file".

to state in this regard that it is not the purpose of Directive 95/46/EC (and as a result of a

Data protection complaint) is to secure access to administrative documents (cf. the judgment of

ECJ of 17 July 2014, C-141/12 and C-372/12, YS and MS, para. 46).□

From the data protection rights of data subjects - such as the right to□

Confidentiality - can therefore not be derived a subjective right to access files, since it is not□

The purpose of the rights of the data subject is to fulfill party rights in another procedure (cf. instead□

many the decision of the DSB of March 9, 2015, DSB-D122.299/0003-DSB/2015, in relation to this□

Right of providing information).□

The data protection authority is therefore not responsible for denying access to files□

to deny□

This application by the appellant was therefore also to be rejected in accordance with the verdict.□

D.5 On the competence of the data protection authority in subsidiary question 3□

If the complainant requests that a decision be made that "the log file decree of the BMF□

dated June 21, 2017, GZ BMF-320700/0004-I/1/2017, is illegal on the basis of the DSG because it also□

includes legal entities and partnerships that do not fall under the scope of protection of□

§ 1 DSG fall", it should be noted that the data protection authority is not entitled to the legality□

to review or correct a decree that is an internal administrative regulation (cf.□

§§ 30 and 31 DSG 2000).□

This application by the appellant was therefore also rejected in accordance with the verdict.□

However, it should be pointed out that Section 1 (1) first sentence DSG refers to “everyone” and therefore□

legal persons and groups of persons from the scope of protection (cf. also the decision□

of the data protection authority of September 13, 2018, GZ DSB-D216.713/0006-DSB/2018).□

D.6 On the substance of the main question□

a) General□

First of all, it should be pointed out that the facts of the case at hand have two components: First□

one is about the use of the log data by the respondent, one□

to investigate a justified suspicion of a gross breach of duty, on the other hand it is about□

the use of the log data for criminal investigation purposes, specifically for suspicion□

investigating the commission of criminal offenses within the meaning of Section 8 (4) DSG 2000.

It is also noted that the Bureau of Internal Affairs ("BIA") is merely an internal

organizational unit of the respondent and it is not an independent one

customer under data protection law.

b) Regarding personal reference and the AIS

If the complainant submits that in the AIS - even if only partially - none at all

personal data would be processed, it must be countered that the DSK is already in

With regard to the AIS, has made a decision using the DSG 2000 (cf. the

Decision of the DSK of December 16, 2005 loc.

If the complainant asks the data protection authority to request the respondent to

to describe in more detail what the AIS-DB2 application is in its entirety and in turn

states that certain parts of DB2 do not contain personal data and neither do they contain tax information

would contain relevant data, from the point of view of the data protection authority it is not recognizable that

to what extent this should be relevant in the present proceedings.

On the one hand, it is undisputed that the Respondent submitted an analysis for unjustified

Had data access carried out regarding a specific taxpayer and it was the

The results of this analysis are personal data, namely at what point in time or

to what extent the complainant relies on the data of that particular taxpayer

has accessed. If - in part - no personal data should be processed in the AIS,

on the other hand, the complainant would have no right of appeal in this regard, since

the fundamental right to secrecy in the protection of personal data is exhausted.

c) For justified suspicion of a gross breach of duty

From the provision according to § 14 paragraph 4 in conjunction with paragraph 5 DSG 2000 it follows that at least during

a three-year period of time log data may be used for this purpose, the legality

to control access to the database secured by access logging, and

although - in the absence of more detailed legal regulations - in any way that the client of the

Data application considered appropriate, with the limit being the principle of proportionality or the

Excess prohibition applies. Using log data to verify the legitimacy of access

can therefore vary in intensity and according to various methods, i.e. both through

Routine control of all access processes as well as event-related controls (as is the case)

or by controlling certain categories of queries (as here), by controlling the queries

certain employees or categories of employees or through random checks (cf.

the decision of the DSK of December 16, 2005 loc.

The former DSK has already stated that every client according to § 14 DSG 2000

is obliged to take appropriate measures to ensure that the data processed by him is not accessed

is illegally accessed. Access to tax data of citizens by officials of the

Financial administration for non-official purposes is an inadmissible use of data. the

Logging of access and evaluating control of the logs for the purpose of identification and

future prevention of inadmissible access is generally recognized according to the state of the art

Means for realizing data security in the form of general prevention against inadmissible

accesses. Section 14 DSG 2000 not only shows the obligation to log query data,

but also the obligation to use log data for checking the admissibility

of the data set (cf. the decision of the DSK of June 21, 2005,

GZ K121.014/0008-DSK/2005; see also the recommendation of the data protection authority of 23 May

2016, GZ DSB-D210.783/0004-DSB/2016).

The Respondent is therefore first to agree that according to § 14 para. 4 DSG 2000

permissibly carried out an analysis of the log data in order to, within the meaning of §§ 43 ff BDG 1979,

but in particular with regard to § 79g BDG 1979, Federal Law Gazette No. 333/1979 in the version of Federal Law Gazette I No.

to investigate a justified suspicion of a gross breach of official duty and thereby future ones

prevent unauthorized access.

d) To use the log data for criminal investigation purposes (suspicion of inspection

of crimes)

However, the Respondent overlooks the fact that the Complainant's complaint is based on

aims to ensure that the Respondent also uses the log data for criminal investigation purposes

have used and that such use of the log data in the present case not by

§§ 8 para. 4 DSG 2000 in conjunction with 14 para. 4 DSG 2000 is covered.

The use of the log data for the purpose of investigating a matter with judicial

Punishment of threatened behavior results initially from an introductory piece by the respondent

of October 3, 2017, signed by the team leader of the BIA (screenshot provided, page 4. of

Complainant's statement of 4 August 2018). The subject line of this entry piece

reads "Suspicion of § 310 StGB gg (for the time being u.T)" and not: "Suspicion of a gross

Breach of service" - or similar. The order, an analysis of unjustified data access

from the outset also aimed at the suspicion of inspection

to investigate a crime, but in particular with regard to § 310 StGB. Also a letter from Dr. Karl

R*** of 3 October 2017 (screenshot provided, page 5 of the complainant's observations

of August 4, 2018) expressly ordered "the allegations according to the introductory piece" (meant

therefore: to examine the introductory piece of October 3, 2017) and no longer differentiated between

an analysis of a possible breach of service and an analysis of criminal law

investigative purposes. This is supported by the fact that the complainant is apparently supported by the respondent

"with reference to criminal offenses" on October 10, 2018 - thus in close temporal connection with

the dispatch of the initial piece of October 3, 2017 - was questioned (page 9 of the statement

of the Respondent of August 4, 2018), which was not disputed by the Respondent

would.

The fact is also based on the memorandum of the StA Vienna dated November 2, 2017

GZ. *3 UT *2*2/17n (screenshot provided, page 7 of the complainant's statement dated

August 4, 2018), according to which the respondent informed the StA Vienna that "the group of perpetrators

can be narrowed down to four people based on internal surveys", including the

Complainant counts. Even if the respondent also has the log data for

determination of a gross breach of service, he has from this point in time at the latest

the data is also used to investigate suspected commission of a crime. About it

In addition, there is also a memo dated October 24, 2017 on the same GZ. of the StA Vienna available

(Submitted screenshot, page 7. of the complainant's statement of 4 August 2018), the

is not completely legible, but also indicated that ongoing reporting regarding the

internal investigations by the respondent to the StA Vienna.

The fact is also based on the internal e-mail traffic of the respondent (submitted

Screenshot, page 11. of the complainant's statement of 4 August 2018), according to which the

Respondents themselves noted in an email that “this ongoing scavenger hunt for

individual pieces of the puzzle" bring nothing and it seems necessary, "the pending at the StA Vienna

Procedure, ie to coordinate the do investigative steps with the ho-led".

Also in the BIA report, first paragraph (screenshot provided, page 12 of the statement by the

Complainant of August 4, 2018) the following is stated: "With regard to the substantiation of the

sufficient initial suspicion that the present case is a criminal act,

in particular the violation of tax or official secrecy (i.e. meaning: § 310 StGB), the

Facts brought to the attention of the WKStA by the BMF immediately”. The Respondent

thereby implicitly admits that the analysis of the log data from the outset (at least also)

Clarification of the suspicion of committing criminal offenses served.

The Respondent's statements that in the event of unauthorized access to

databases of the AIS also inevitably the suspicion of the existence of a breach of duty

would result (page 3 of the Respondent's statement of September 28, 2018), and that

the analysis of the query behavior carried out by the BIA at the request of the respondent

with regard to the legality of access to BMF databases “for purely business-related reasons

Queries” was made (page 5 of the Respondent’s statement of September 28, 2018),

can't change anything about it. The Respondent expressly supported himself from the beginning

to an "investigation into the suspicion of § 310 StGB", albeit initially against one

unknown perpetrators, at the latest after "the circle of perpetrators on the basis of internal surveys to four

Persons" was limited, also concerning the complainant.

Overall, there are clear indications that the Respondent has the log data

Regarding complainants (at least also) to clarify the suspicion of committing criminal offences

used. It can therefore not be assumed that the analysis of the log data is the

Complainant concerning only an investigation into a breach of official duty

acted.

It should first be noted that § 14 para. 4 DSG 2000 refers to two cases, in

which log data deviates from the purpose of the determination - i.e. the control of the admissibility of the

Use of the logged or documented database – the following may be used:

In particular, further use for the purpose of monitoring those affected is incompatible

data is contained in the logged database, or for the purpose of checking those persons

who accessed the logged database for a reason other than that of

Verification of their access authorization, unless it is used for the purpose of

Prevention or prosecution of a crime according to § 278a StGB (criminal organization) or

a crime punishable by imprisonment for a maximum of five years.

In this case, however, there is neither the first case according to § 278a StGB, nor is there a case of one

crime with a maximum sentence of imprisonment exceeding five years. This is how it turns out

the Respondent's introductory piece of October 3, 2017 in the subject line expressly the

"Suspicion of § 310 StGB gg (for the time being u.T)", whereby § 310 paragraph 1 StGB is a prison sentence of up to three

years. A suspicion of other offenses carrying a maximum sentence of imprisonment

exceeds five years, at no time was the Respondent

put forward.

If the respondent argues that he is to be reported to the WKStA in accordance with § 78 StPO

obliged, he overlooks the following: The respondent did not come only after the analysis had been carried out

of the log data to the conclusion that there was a notifiable suspicion of a criminal offense. Much more

From the Respondent's point of view, the suspicion of Section 310 of the Criminal Code existed from the start

and log data were then analyzed to investigate this suspicion in more detail. It's falling

however, in the area of responsibility of the StA according to the relevant provisions of §§ 101 ff StPO

to take investigative steps or to conduct a corresponding investigative procedure and has the StA in

§ 74 StPO also provides a corresponding basis for the processing of personal data.

In the present case, however, the respondent even has log data on the complainant

concerning used to eliminate the suspicion of committing a criminal offense after a

Corresponding proceedings were pending at the StA Vienna. As stated, this follows from the fact that

the Respondent twice "reported" to the StA Vienna and in the report of November 2nd

2017 of the respondent to the StA Vienna it is stated that "the group of perpetrators due to

internal surveys can be narrowed down to four people".

It should be noted that an analysis of log data with the purpose, not just the legality

of data access, but according to certain patterns in the behavior of the

Authorized access to seek conclusions about otherwise illegal behavior of those affected

(here: suspicion of § 310 StGB) enable the described in § 14 para. 4 DSG 2000

exceeds the legitimate control purpose. The text of § 14 para. 4 DSG 2000 provides - as already

set out – the limitation of the purpose of use of log data is unequivocally clear,

in particular also by the fact that it includes the few permissible extensions of the purpose of use

expressly and conclusively (cf. the decision of the DSK of December 16, 2005 loc. cit.).

In contrast to the DSK decision of June 21, 2005 mentioned by the respondent,

GZ K121.014/0008-DSK/2005, the present case was not just about the question of whether the

Use of log data to check the legitimacy of access was allowed to a

to investigate a justified suspicion of a gross breach of official duty and thereby future ones

to prevent unauthorized access (this was declared permissible anyway, cf. point D.6.c.).

Rather, in the present case, the question was whether the Respondent used this log data

misused and was allowed to use it to raise suspicions of committing criminal offences,

especially with regard to § 310 StGB.

D.7 Result

Due to the change in purpose of data processing described, there was a transmission within the meaning of Section 4

Z 12 DSG 2000 before.

§ 8 para. 4 DSG 2000 finally regulates when the use of "criminal data" does not counteract

breaches the confidentiality interests of a data subject that are worthy of protection (cf. VwSlg. 18.498 A/2012).

The Respondent could not find any facts justifying his procedure in the sense

of § 8 para. 4 DSG 2000.

By improperly using the log data to investigate suspected

Section 310 StGB was therefore ultimately - regardless of the fact that the determination of a

lack of access authorization consequences under employment law can be founded - in the

The complainant's right to secrecy of personal data concerning him

improperly intervened.

Against this background, the question raised by the complainant was needed

with regard to the admissibility of the storage period according to § 14 paragraph 5 DSG 2000 no longer received

will.

As a result, the decision had to be taken in accordance with the verdict.