GZ: DSB-D123.070/0005-DSB/2018 from 13.9.2018

[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 for reasons of pseudonymization

and/or changed. 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 Dr. Ida A***

(Appellant) of June 23, 2018 against 1) the Federal Ministry for Europe,

Integration and external affairs (first respondent) and 2) the Federal Chancellery

(Second respondent) for violation of the right to secrecy as follows:

- The appeal is dismissed.

Legal bases: §§ 1 paragraphs 1 and 2, 24 paragraphs 1 and 5 of the Data Protection Act (DSG),

Federal Law Gazette I No. 165/1999 as amended; Art. 4 Z 5, Art. 25 and 32 of the General Data Protection Regulation

(GDPR), OJ No. L 119 of 4 May 2016, p. 1.

REASON

A. Submissions of the parties and course of the proceedings

1. On June 23, 2018, the complainant brought two - almost identical in content -

Complaints against the first and temporary complainant and claimed in it a

Violation of the fundamental right to data protection due to failure to delete data or

pseudonymization. In summary, the complainant submitted that the

Respondent sensitive personal data of the complainant in electronic

form and would save without pseudonymization. Specifically, the data would

Information on the sex life and health of those concerned. The state has

obtained this data in 2007 during an unlawful undercover investigation.

In this regard, several procedures before the data protection authority or the
former Data Protection Commission has been made pending. Further data (with
well meant: the further storage of data) would be the result of
the following procedures, in particular to protect their rights. the
Respondents had their data in 2014 in connection with a
received an international complaint ("X against Austria, UN document
CEDAW/C/**3/D/1*/2014 dated July 11, 2016"), which also opposes the collection of data
and which have since been archived in electronic form in Vienna and Geneva.
The Respondent already had a request for data deletion on July 24, 2016
to the first respondent or a request for carding of the paper files to the
Second respondent asked, which would not have been complied with, however, since
the archiving of said data for the documentation of various domestic
Procedures provided for by law and also to document the said
international complaints procedure is necessary. The BVwG already has one
appropriate complaint against this failure to delete data, among others with the
Grounds dismissed that data erasure immediately after completion
of a procedure is not compatible with constitutional principles (reference to BVwG
from August 31, 2017, Zl. W214 2152086).
The complainant has now two years after completion of the said
Proceedings with e-mail dated May 25, 2018, the respondents to delete their
personal data is requested, the corresponding deletion requests are in the file
as a copy. She went on to say that the request for deletion was then also fulfilled for her
would be if pseudonymization were to be carried out. The omitted
Pseudonymisation is a violation of the fundamental right to data protection. It would be
disproportionate if data is kept in a non-pseudonymised form
would. The complainant fears that her identity in the following

Decades, every time the data is accessed, what is no longer with the

public interest can be justified. In particular, their data would be at

immediately public after a successful hacker attack on the server of the respondent

accessible. If data were retained to protect "Austrian

Legal claims” against the re-filing of a similar complaint by them

to defend at another tribunal, then the purpose of documentation will pass

the required pseudonymization is not restricted. According to the legal opinion of the Constitutional Court

must maintain a current and

concrete necessity are asserted (reference to VfGH of 12.12.2018,

Zl. E3249/2016). It could also be deduced from the GDPR that far-reaching

Data protection measures should be the norm for archiving. So normalize

Art. 5 para. 1 lit c GDPR the principle of data minimization and as an instrument for it

cite pseudonymization under Art. 25 (1) GDPR. The omission of this or

Comparable protective measures would be one with the fundamental right to data protection

irreconcilable careless handling of sensitive data.

2. With a statement dated June 25, 2018, the complainant submitted the

Response letter from the Respondent, which corresponds to the request for deletion

Complainant of May 25, 2018 each failed to comply.

3. With the deficiency rectification order of July 3, 2018, the data protection authority requested the

complainant to submit their complaint in accordance with the statutory provisions

specify and explain in concrete terms which rights the complainant is entitled to

deemed injured.

4. The complainant submitted in a letter dated July 7, 2018 that

Subject of the proceedings the question of the illegality of data storage without

pseudonymization is. The complainant was concerned that her name and

other information suitable for identification from the other data so

would be separated that from the remaining data alone no longer on their identity

can be closed. By the Respondents refusing to delete the data

and thereby massively intervene in the private life of the complainant,

they would be subject to the obligation to bear the risks arising from data storage

to minimize what the pseudonymization, or an equivalent technical

action counts.

5. The Respondent for the First Appeal led with a statement dated August 7, 2018

summarized from that the BVwG with the quoted by the complainant

Knowledge of August 31, 2017, Zl. W214 2152086-1, also led to the meeting,

that a public interest in documentation stands in the way of deletion. the

Arguments of the BVwG regarding this documentation interest would also

the new legal situation according to Art. 5 Para. 2 lit. e DSGVO in conjunction with § 2 Z 3 and § 5 des

Federal Archives Act and Z 9 of the Annex to § 2 Para. 1 of the Federal Archives Ordinance

as well as Section 25 of the Monument Protection Act remain applicable. Accordingly, it is about

Records of proceedings before the Constitutional Court, the Administrative Court

and before international institutions for archival material that is subject to the Monument Protection Act

be under protection. In the present case would not only be an international institution

dealt with (CEDAW), but also at the VwGH a - still pending - extraordinary

revision introduced. According to § 5 paragraph 3 of the Federal Archives Act, this document is for

To be handed over to the Austrian State Archives for archiving under lock and key. To

Acceptance of the written material would be the handing over federal departments and from the

Takeover of the Austrian State Archives Responsible iSv Art. 4 Z 7 DSGVO.

Regarding the examination of the possibility of pseudonymization of the

The files relating to the complainant were stated that the files, which data

contained the complainant, as sealed files would be kept, whereby the

strictest locking level "lock sensitive" is used. The files would be in

electronic file (ELAK) marked with this security level and with the

appropriate access rights. have access to the content of these files

only the officials specified by name in the file flow, persons with

Leading role in the prescribed higher-level organizational units and

Heads of the groups involved in the workflow and auditors. The majority of the

The files kept by ELAK would already have been filed in the present case, i.e. they would

are no longer being processed and only in exceptional cases by authorized persons

and viewed on a case-by-case basis. Access is only granted by a very

restricted group of employees who are subject to official secrecy

would be subject to, and only in connection with the present

Complaint or any future Complainant complaints. A

such interference with the fundamental right guaranteed under Art. 8 ECHR

Appellant is to be classified as proportionate. Limiting the risk

an unjustified processing of the data by means of the explained classification of the

Files as "sensitive lock" offer in view of the low probability of intervention-

and intensity thus a level of protection appropriate to the risk in accordance with Art. 32 Para. 1

GDPR. Pseudonymisation as an additional protective measure is carried out due to the

Legally prescribed and court-confirmed documentation interest by the

First respondent not considered.

6. The second respondent brought this up with a statement dated July 31, 2018

in summary, that there is no legal entitlement to pseudonymisation,

because in the sense of Art. 25 DSGVO a weighing of interests or a weighing up

various factors, such as the type and scope of processing,

risk potential, appropriateness of costs and state of the art

must be defined in order to define the measures that are the most appropriate

data security measure. A pseudonymization could in the concrete

Case, among other things, therefore not apply because the facts of the□

from a variety of unstructured data (opinions, reports,□

File notes and the like) or the entire extensive file remain legible□

must, which would no longer be guaranteed after pseudonymization. alone off□

This reason is the pseudonymization, apart from the enormous effort that□

would be required, no appropriate action. In particular, since by a□

Pseudonymization no increase in the level of protection compared to the current anyway□

would already take place at a very high level of protection and even with pseudonymization□

Resolutions would have to be kept under lock and key. Some factors leading to that□

would contribute to the current very high level of protection would be the existence of one□

strict authorization concept, the official secrecy of the employees, a□

End-to-end encryption (client-server) with strong encryption algorithm□

as well as the operation by the Bundesrechenzentrum GmbH as a processor, the□

have several certifications related to IT security.□

7. The DPA informed all parties by letter dated 9 August 2018 that□

that the complaint against the first respondent and the complaint against□

the second respondent on the basis of the same facts pursuant to Section 39 (2) AVG□

for a joint decision under the GZ: DSB-D123.070.□

8. The complainant then replied - according to the results of the parties□

of the preliminary investigation - in her statement of August 10, 2018□

summarized that they become the legal basis for pseudonymization□

Art. 5 para. 1 lit c support. It is a consideration iSv Art. 8 EMRK necessary, as in□

archiving of their data in the public interest can be designed in such a way□

that the associated encroachment on their fundamental right to data protection is the least□

successes. Pseudonymisation cannot be ignored in this consideration. the□

Although the complainant does not deny that due to the already taken□

Measures to secure data can achieve a high level of protection, however

the Respondents would be exposed targets for attacks on the computer systems of

Outside. In view of the intended long retention period of the data

However, it corresponds to life experience that in this long time it is still

“data leaks” could occur. Technological innovations that are already foreseeable

could make the current security measures obsolete in the next few years.

Regardless, the measures taken would not necessarily counteract

protect unreliable employees, even if these employees are subject to criminal law

be aware of the consequences. The data concerning them would be protected, however

would be the protection compared to the other electronic files at the

Respondents not particularly higher. Pseudonymization would also be one

simple measure where documents would still be legible. The complainant

I continue to consider myself a fundamental right by not using pseudonyms

violated secrecy.

B. Subject of Complaint

First of all, it should be stated that the complainant originally on May 25, 2018

a request for deletion to the respective respondent and within the scope of their

Submission of June 23, 2018 to the data protection authority - among various others

Rights (e.g. the right to restriction of processing in accordance with Art. 18 GDPR) -

a violation of the right to erasure pursuant to Art. 17 GDPR was also asserted

has. In further submissions - in particular in response to the

Defect rectification order from the data protection authority of July 7, 2018 - led the

Appellant, however, from the fact that the subject of the proceedings is now the question of

Unlawfulness of data storage without pseudonymization (cf. on the concept of

Pseudonymization Art. 4 Z 5 GDPR). To this end, the complainant has already brought

her submission of June 23, 2018, as well as in her statement of August 10, 2018

before that the "omission of pseudonymization" is "a violation of the fundamental right

Privacy".

Against this background, the unsuccessful deletion requests of May 25 were no longer valid

2018 against the respondents or a violation of the right to erasure

according to Art. 17 GDPR, but a violation of § 1 DSG.

Based on the submissions of the appellant, it follows that

The subject of the complaint is only the question of whether the respondents

Complainant violated the right to secrecy by

Pseudonymisation of the complainant's personal data in her

electronic filing systems (ELAK).

C. Findings of Facts

1. The Respondents store personal data of the Complainant

in the electronic filing system (ELAK).

Evidence assessment: The findings made are based on the insofar undisputed

Submission of the complainant of June 23, 2018 and on the undisputed

Statement of the first respondent of August 7, 2018 or the

Second respondent dated July 31, 2018.

2. So far there has been no compromise of the data processing systems of

Respondent, in which personal data of the complainant

were disclosed or lost.

Evidence assessment: The findings made are based on the arguments

of the complainant of June 23, 2018 and August 10, 2018, when the

Complainant limited to one that could potentially occur in the future

indicate damage, such as their reference to possible hacker attacks, "data leaks",

or foreseeable technological innovations affecting the current security measures

the Respondent could make obsolete in the next few years. In the present

proceedings, there are also no indications of damage already suffered by the

complainant or from the disclosure of her data that has already taken place

unauthorized third parties.

D. In legal terms it follows that:

1. Violation of § 1 Para. 1 DSG (fundamental right to secrecy)

The complainant does not have any until the conclusion of the present proceedings

specific act demonstrated by which they are in their fundamental right to secrecy

would have been injured. Rather, it was limited to, because of a

"omitted pseudonymization" of their data in ELAK not (yet) manifested

Events such as potential hacker attacks, "data leaks", or foreseeable technological events

Bring innovations into the meeting, in the context of which the complainant

disclosure of their data could harm them in the future.

The data protection authority can violate the fundamental right to secrecy

However, only considered ex post determine why the complaint regarding

injuries that may occur in the future for this reason alone

was to be dismissed.

2. To enforce specific data security measures

Regarding a violation of the fundamental right to secrecy by a

"Failure to use pseudonymization" means that there is no right under the GDPR

it can be deduced that a data subject takes specific data security measures

iSv Art. 32 DSGVO could demand from a person responsible. Neither can

a data subject – as requested by the complainant – specific

Demand data minimization measures within the meaning of Article 5 (1) (c) GDPR.

In principle, it is possible that a data subject, due to insufficient

Data security measures of a person responsible in the fundamental right to secrecy

is violated (e.g. because this results in disclosure to unauthorized third parties), in this case

however, firstly the injury would have to have already taken place (cf. point 1) and secondly

Even in this case, the data subject would not have the right to choose a specific

Data security measure adult.

As can be seen from Art. 32 GDPR, the obligation to ensure the security of

Processing of personal data the person responsible or the

Processor, whereby this security – taking into account the provisions in paragraph 1 of this

Provision mentioned elements - can be guaranteed in several ways.

Also from the point of view of a systematic interpretation of the GDPR cannot

be concluded that the legislature of a data subject is a subjective

wanted to grant the right to comply with certain data security measures:

Thus, the rights of data subjects are expressly stated in Chapter III; the

Pseudonymization is found as a measure in Chapter IV, which is the objective

Obligations of controllers and processors regulates.

In this context, the former Data Protection Commission

noted that data security measures - to which the complainant

obviously refers - only create an obligation of the person responsible, not

but subjective legal claims of a data subject (cf. the decision of the DSK

from August 2, 2005, GZ: K121.038/0006-DSK/2005). The Federal Administrative Court

confirmed this view and, with reference to the case law of the DSK, stated that the

Assertion of specific data protection measures of a decree

agreement is not accessible (cf. the findings of the Federal Administrative Court of July 11, 2017,

Zl. W214 2117640-1 and from April 20, 2017, Zl. W214 2007810-1).

The data protection authority can only fulfill this obligation on the part of the person responsible

investigating an ex officio investigation procedure (Art. 55 Para. 1 in conjunction with Art. 57

Para. 1 lit a and h GDPR) and the person responsible, if necessary, to comply with the

instruct regulation (Art. 58 para. 2 lit d DSGVO). In the present case, however

there are no indications that justify a corresponding official examination procedure

would.

3. Result

As a result, there is neither an (already occurred) violation of the fundamental right

Secrecy before, nor can - as explained - a specific

Data security measure (specifically: pseudonymization) as part of a

Complaints procedure can be asserted.

Against this background, the decision had to be made according to the verdict.