GZ: DSB-D213.692/0001-DSB/2018 from 16.11.2018

[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 in the official examination procedure against the allergy

Tagesklinik D*** GmbH (responsible person) for violations of obligations under the

GDPR as follows:

1. The person responsible has against the obligation to order a

violation of the data protection officer.

2. The person responsible obliges data subjects with the form

"Declaration of consent to data processing - data protection law" (available

at http://www.allergie-tagesklinik***.at/wp-content/uploads/2018/08/ALTK***-

DSGVO-Information sheet-with-consent-20180502_2*5*.pdf) to a

unlawful consent by

a) the declaration of consent records facts that do not require consent

are subject, but give the impression that consent is required for this

is to be granted, and

b) cannot be inferred from the declaration of consent with sufficient clarity

is, for which data processing the consent is the legal basis

is.

3. The person responsible has violated the information obligations by im

"Information sheet on data protection" or on their website at

http://www.allergie-tagesklinik***.at/datenschutz/

a) does not clearly distinguish whether the information pursuant to Art. 13 or pursuant to

Art. 14 GDPR;

b) the name and contact details of a non-appointed

indicates the data protection officer;

c) incompletely citing the legal bases for the processing;

d) in relation to Art. 6 Para. 1 lit. f GDPR does not state in which the

legitimate interests pursued by the person responsible,

based;

e) does not state that consent can be revoked at any time

can be without affecting the legality of the due

Consent is affected by the processing that has taken place up to the point of revocation.

4. The person responsible has against the obligation to examine the necessity of a

Conducting data protection impact assessments

processing activities

a) Patient files (address, billing and registration data)

b) Settlement (settlement with social security)

c) request for findings/transmission of findings (transmission and disclosure),

d) Testing of samples (testing and sending of samples [blood,

secretion etc.]),

e) Management of prescriptions (storing which prescriptions patients

require),

f) Pharmacy (operation, administration, billing and organization of

medicine chest),

all described in more detail under II.B. in the register of processing activities

responsible, by wrongly assuming that

that in any case no data protection impact assessments are to be carried out.□

5. The responsible person is assigned within a period of eight weeks□

other execution□

a) to appoint a data protection officer within the meaning of Art. 37 ff GDPR□

and to report to the data protection authority;□

b) the form "Declaration of consent to data processing - data protection□

Law" and the "Information sheet on data protection" or the information□

the website http://www.allergie-tagesklinik***.at/datenschutz/ under□

Consideration of points 2 and 3 of this notice legally compliant□

design; and□

c) to check for the data processing specified in point 4,□

whether a data protection impact assessment is to be carried out and the□

to report this to the data protection authority.□

Legal basis: Section 22 (1) of the Data Protection Act (DSG), Federal Law Gazette I No. 165/1999 as amended;□

Art. 6, Art. 7 (4), Art. 9, Art. 12, Art. 13, Art. 14, Art. 35, Art. 37, Art. 57 (1) lit. h,□

Article 58 paragraph 1 letter b and paragraph 2 letter d General Data Protection Regulation (GDPR), ABl.□

No. L119 of 05/04/2016, p.1; Regulation of the Data Protection Authority on the exceptions□

from the data protection impact assessment (DSFA-AV), Federal Law Gazette II No. 108/2018; regulation□

the data protection authority about processing operations for which a data protection□

Impact assessment is to be carried out (DSFA-V), Federal Law Gazette II No. 278/2018.□

REASON□

A. Procedure□

1. The data protection authority has the (mandatory) submissions of those responsible from□

June 18 and June 22, 2018 pursuant to Art. 33 GDPR (security breaches) as of□

Reason taken to initiate an ex officio investigation procedure, since in the reports of□

Only one "data protection coordinator" is named for breaches of data security□

would. The data protection authority then asked to comment on this and demanded□

in particular,□

□□

to submit the list of processing activities;□

□□

the data protection declarations to be given to patients□

to forward;□

□□

to announce whether and under what circumstances data not□

be identified directly from the data subject;□

□□

to state the reasons why no data protection officer has been appointed□

would;□

□□

the data protection measures carried out by the person responsible□

Submit Impact Assessments (DPIA) hereafter, or the reasons□

to announce why DPIA from the point of view of those responsible□

was (were) allowed to omit;□

□□

to state the reasons why no reference to cookies is made□

should or an opt-out could not be provided;□

□□

if no DPIA was to be carried out, to announce which ones□

Data security measures exist and which ones□

data minimization measures have been or are being taken;□

□□

if this does not result from the directory, the storage period□

to announce the data and to indicate whether storage in□

cloud services or on servers in the EEA or third countries;□

□ to disclose processors and transfer recipients;□

□□

those pursuant to Section 30 (3) DSG and those pursuant to Section 9□

Administrative Penal Act 1991 (VStG) to announce the appointed person.□

2. With a submission dated August 13, 2018, the person responsible stated:□

"Dear Ms. V***,□

Dear Mag. G***,□

With reference to your letter of July 16, 2018, I may comment as follows:□

a) Ad directory processing activities: in the appendix□

b) Ad Patient Privacy Policy: attached□

c) Ad circumstances: data are always determined directly by the data subject□

or always determined in the presence of the person (if the patient does not speak German□

speaks and has an interpreter with him or is too young and has an interpreter□

legal guardian is present)□

d) Ad data protection officer: we have the information (e.g. from the Medical Association□

and WKO) before May 25, 2018 understood that doctors due to their core activity□

do not require a mandatory data protection officer, but take one voluntarily□

be able. Meanwhile we read on https://www.wko.at/service/unternehmensfuehrung-□

financing-foerderungen/eu-dsgvo-datenschutzbeauftragter-faq.html#11 und□

http://www.aekwien.at/datenschutzgrundverordnung that we because of our□

Number of employees probably have to take one. What is the current recommendation here?□

of the DSB? Do we have to have one? If so, we clearly will□

change immediately. Please give us your feedback.□

e) Ad DPIA: no written data protection impact assessment was carried out, as this□

according to http://www.aekwien.at/datenschutzgrundverordnung for the medical□

Patient administration would not be necessary (the data processing concerned corresponds to□

the excepted data processing according to §1 DSFA-AV, DSFA-A12).□

Nevertheless, there is an "IT guideline" created for the allergy day clinic as well□

"Risk assessment", which also names the specific case (transmission of findings).□

f) Ad cookies: We have a reference to cookies on our imprint page□

at http://www.allergie-tagesklinik***.at/impressum/ or a reference text to□

Data protection on our homepage under "Notes for patients". But now it was□

additionally set a cookie notice banner on the start page, as of today.□

g) Ad data security measures: in the appendix□

h) Ad storage period: see processing directory in the appendix□

i) Ad processor: in the appendix□

j) Ad appointed person: The managing director has Dr. Flora L*** inside.□

To open the attachments, please click here as well as first name, last name and e-mail□

Enter address.□

If you have any questions, I can also be reached at 06**/*9*8*7*6.□

Warm wishes□

Walter Ä***□

---------- ----------□

Mag. Walter Josef Ä***□

privacy□

Allergy day clinic D***□

P***-Gasse 13*, A-**** D***□

T: +43 (***) *44*4*23 - 5*□

F: +43 (***) *44*4*23 - 3*□

M: +43 (6**) *7**22*01

Email: w.ae***@allergie-tagesklinik***.at

Web: www.allergie-tagesklinik***.at

Regional Court R***, FN *4*7*2*j

---------- ----------

The exchange of messages with the Allergy Day Clinic D*** via e-mail is non-binding. Legal Statements

require the written form. The information in this e-mail is confidential and intended exclusively for the addressee. The

Allergy Day Clinic D*** reserves all rights to the message and attached files. If you don't

intended addressee (and one of his/her employees or his/her authorized recipient) of this e-mail or their

Should be representative, any form of acknowledgment, publication, duplication or transmission of the content

inadmissible. If you have received this email in error, please notify us immediately and delete it

the email is irretrievable. Automatic receipt and read confirmations do not count as confirmation of receipt of yours

News.

B. Subject of the proceedings

The subject of the data protection review is whether or to what extent the obligations of

DSGVO are complied with by the person responsible. The scale of the exam refers

refers to the data protection violations suspected by the authority and to the

Facts that have emerged from the review.

C. Findings of Facts

1. The person responsible is a GmbH based in D***. Your business purpose is

Diagnosis and therapy of allergic diseases, especially in children and

Familys.

At the time of the decision, she employed three management staff, seventeen

Doctors, twelve office and laboratory workers and two nutritionists. be there

regularly and comprehensively special categories of data according to Art. 9 DSGVO

(health data) processed.

2. The person responsible uses the form "Declaration of consent to

Data processing - data protection law", which can be found at http://www.allergie-

tagesklinik***.at/wp-content/uploads/2018/08/ALTK***-DSGVO-Informationsblatt-mit-

Consent-20180502_2*5*.pdf can be accessed and downloaded and

has the following content (format not reproduced 1:1):

Declaration of consent to data processing - data protection

law

The Allergy Day Clinic D*** GmbH (hereinafter Allergy Day Clinic D***) is for

Obliged to secrecy, has personal data that is known to her in her work

are to be treated confidentially, to maintain data protection and third parties only such

Pass on information that is necessary for processing. The unencrypted one

Sending of personal data (see information sheet on data protection on the

Pages 2 and 3) is not permitted under the European General Data Protection Regulation because the

Protection and integrity of the data cannot be guaranteed.

For this reason, Allergy Day Clinic D*** requires express written consent

of all patients in order to process personal data in the future and

to be sent and received unencrypted (dispatch of findings by e-mail, by telephone

report, etc.).

Therefore, please give the following express written consent in block letters

fill in and sign. Each person – including children – must have their own

consent to be filled out.

Completed between the Allergy Day Clinic D*** on the one hand, and on the other hand:

FIRST NAME Patient

LAST NAME Patient

DATE OF BIRTH (day, month, year) Telephone

EMAIL ADDRESS Patient Gender

× I expressly agree that personal data (esp.□

Information about my condition when accepting the consultation or treatment that□

History of an illness, the diagnosis, the course of the illness, my findings□

as well as information about the type and scope of the advisory, diagnostic or□

therapeutic services including the use of medicinal specialties)□

processed, stored and in unencrypted form to and from□

be sent accordingly to relevant third parties. The approval of the□

unencrypted transmission can be revoked at any time with effect for the future.□

Furthermore, I irrevocably agree that the Allergy Day Clinic D*** may use others at any time□

Companies and/or persons to carry out the agreed service□

may use. This also applies to the processing including storage of□

personal data. I acknowledge that by submitting the□

Data (unauthorized) third parties can obtain knowledge of the information and this□

data can be changed. I understand that this is to disclose my□

health condition can result. I am aware that the Allergy Day Clinic D***□

assume no liability for the correct and complete transmission of the data□

can.□

3. The person responsible provides under http://www.allergie-tagesklinik***.at/datenschutz/□

The following information on data protection is available, which corresponds to that□

are also printed on pages 2 and 3 of the declaration of consent:□

“Privacy Information□

Allergy Day Clinic D*** GmbH (hereinafter Allergy□

Day Clinic D***) is an important concern. The Allergy Day Clinic D*** assures you□

Therefore, that your personal data respecting the principle of good faith□

belief and will only be processed for the purposes set out below. the□

Allergy Day Clinic D*** also confirms that suitable technical and□

organizational measures have been taken to protect your data and

To fulfill obligations under the European General Data Protection Regulation (GDPR). in the

Within the meaning of Art.13 ff GDPR, the Allergy Day Clinic D*** would also like to help you

the following information about the processing of your personal data and

about your rights and obligations in connection therewith.

Who is responsible for data processing and who can you contact

turn?

Allergy day clinic D*** GmbH

P*** alley 13*

****D***

Data protection officer: appointed

Contact details of the contact person:

Mag. Walter Josef Ä***

w.ae***@allergie-tagesklinik***.at

Which data is processed and from which sources does this data come?

The Allergy Day Clinic D*** processes the personal data that the allergy

Day Clinic D*** receives from you as part of the business relationship. In addition

Allergy Day Clinic D*** processes data that Allergy Day Clinic D*** receives from

Third parties (GKK, information providers, debtor registers, etc.) and from the public

accessible sources (company register, media, etc.) permissibly received.

Personal data includes your personal master data (name,

Address, contact details, date and place of birth, nationality, legal

representative, etc.), identification data (ID card data, etc.),

Authentication data, contract data (contractual/legal relationships, etc.),

Patient information (history of diseases,

Diagnoses, course of the disease, type and extent of the advisory, diagnostic or

therapeutic services including the use of medicinal specialties,□

Appointments, etc.), contract billing and payment data□

(social security, bank details, etc.), planning and control data,□

disclosed information (from third parties, e.g. from public directories),□

Evaluation Data, Communication Content, Communication Metadata, Resume Data,□

personal life data, information on previous employment,□

Information about religious or philosophical beliefs, health (enquiry□

of samples, etc.), sexual orientation, ethnic origin, etc., employee data as well□

Data required to fulfill legal and regulatory tasks.□

For what purposes and on what legal basis is the data used□

processed?□

Allergy Day Clinic D*** processes your personal data in accordance with□

the provisions of the GDPR and the Data Protection Adaptation Act 2018:□

□ to fulfill contractual obligations (Article 5 (1b) GDPR)□

Documentation obligation according to & 51 Medical Act as well as the recording of all□

Services including automatically created and archived□

Text documents in these matters, etc.□

□ to fulfill legal obligations (Article 6 (1c) GDPR)□

Personal data may be processed for the purpose of fulfilment□

different legal obligations (Doctors Act, etc.) or from tax and□

corporate law requirements may be required.□

□□

within the scope of your consent (Art 6 Para 1a GDPR)□

If you give the Allergy Day Clinic D*** consent to the processing of your□

have given personal data, processing takes place in accordance with the□

Declaration of consent for the purposes specified and to the extent agreed therein. One□

Consent given can be revoked at any time with effect for the future.

 to protect legitimate interests (Art 6 Para 1f GDPR).

Who receives your data?

Within the Allergy Day Clinic D***, those positions or

Employees your data, which they use to fulfill the contractual,

legal and regulatory obligations and legitimate interests.

In addition, commissioned by the Allergy Day Clinic D***

Processors (IT service providers, back office service providers, etc.) your data, if

they need the data to fulfill their respective service. All

Processors are contractually obliged to process your data

treated confidentially and processed only within the framework of the provision of services.

How long is your data stored?

The Allergy Day Clinic D*** processes your personal data insofar as

necessary, for the duration of the entire business relationship (from the initiation,

Processing until the termination of a contract) and beyond according to the

statutory storage and documentation obligations.

In addition, the statutory limitation periods for the storage period, which e.g

the General Civil Code in certain cases up to 30 years

may amount to be taken into account.

What data protection rights do you have?

The Allergy Day Clinic D*** points out that within the meaning of the GDPR

the right to information about your stored data at any time (Article 15 GDPR), as well as

under certain conditions, the right to erasure (Article 17 GDPR),

Restriction (Art 18 GDPR), correction (Art 16 GDPR), data minimization and

Data portability (Art 20 GDPR) and objection (Art 21 GDPR). To the

To exercise your rights, please contact the above

responsible. The Allergy Day Clinic D*** also points out that you

a right of appeal to the supervisory authority (Austrian data protection authority)

entitled to, should you believe that a data breach has occurred. for

The Allergy Day Clinic D*** is of course at your disposal for questions and information

available at any time.

Are you obliged to provide data?

As part of the business relationship, you must provide those personal data

provide the necessary for the establishment and implementation of the business relationship

are required and the Allergy Day Clinic D*** is required to collect them by law

is obliged.

Is there automated decision making including profiling?

Allergy day clinic D*** does not use any automated decision-making processes

Art 22 GDPR to bring about a decision on the justification and

Execution of the business relationship."

4. In the list of processing activities of those responsible, under

point II.B. a total of nine processing operations are listed:

 patient record,

 Payroll (both social insurance/private),

 Findings request/findings transmission,

 examination of samples,

 organization of consultations,

 Management of recipes,

 medicine cabinet,

 ELGA and

Information to own patients.

The person responsible has no data protection for any of these processing activities.

Impact assessment carried out.

Evidence Evidence: Evidence was recorded through the submissions of the

Responsible persons including attachments as well as on the basis of the official knowledge of the authority and

ex officio research on the website of those responsible.

D. In legal terms it follows that:

1. Regarding the competence of the authority:

Any supervisory authority is permitted to conduct investigations in the form of

carry out data protection checks (Article 57 (1) (h) GDPR).

According to § 18 Para. 1 DSG, the data protection authority is the national supervisory authority

Art. 51 DSGVO set up and entitled, at any time and without giving reasons

check those responsible. The data protection authority, based on the information provided by

responsible in (mandatory) reports of data breaches

Art. 33 GDPR had reason to believe that the person responsible comprehensively

processes special categories of data and has not appointed a data protection officer

has. The data protection authority therefore initiated the decision on July 16, 2018

official test procedure.

2. Regarding point 1 (mandatory appointment of a data protection officer):

In any case, those responsible appoint a data protection officer if the

Core activity of the person responsible or the processor in the extensive

Processing of special categories of data according to Art. 9 GDPR exists (Art. 37

Paragraph 1 lit. c GDPR).

The Guidelines on the Data Protection Officer of the Art. 29 Working Party on Data Protection

(WP 243 rev.01, available e.g. at

https://www.dsb.gv.at/europaischer_datenschutzausschuss_edsa) do

2.1.3, page 9, in footnote 14, commenting on this in terms of an extensive

Data processing “the processing of personal data […] not as extensive

[should] apply where the processing involves personal data of patients or […]

concerned and by an individual doctor, other health professional

[…] he follows".

For more information on what is meant by "extensive data processing".

can be understood can be found in the guidelines for data protection impact assessment (DPIA)

and answering the question whether processing within the meaning of Regulation 2016/679

"likely to involve a high risk", WP 248 Rev.01 (available at

https://www.dsb.gv.at/documents/22758/112500/Leitlinien+zur+Datenschutz-

Impact assessment-wp248-rev-01_de.pdf/2246301e-ffbb-4a03-bf23-797fee89174e), on

Page 11:

Accordingly, the following criteria must be taken into account:

a) Number of those affected, either as a specific number or as a proportion of

corresponding population group;

b) processed amount of data or bandwidth of the different processed

data items;

c) Duration or permanence of data processing;

d) geographic extent of data processing.

In view of that

a) the core activity of those responsible in the diagnosis and treatment of

Allergies - i.e. in the processing of health data according to Art. 9 Para. 1

GDPR – lies,

b) they have twelve office or laboratory staff, seventeen doctors and two nutritionists

busy and

c) store health data by law for at least 10 years

are (§ 51 ÄrzteG)

should therefore have come to the conclusion that – under

Consideration of the mentioned criteria - certainly an extensive processing

special categories of data according to Art. 9 DSGVO and therefore

a data protection officer should have been appointed.

Consequently, this breach of duty was to be determined in accordance with the verdict.

3. Regarding point 2 (inadmissible consent):

3.1. If the data processing is based on the consent of a data subject,

to take particular account of whether the fulfillment of a contract by the

Consent to processing of personal data that is necessary for

the fulfillment of the contract is not required (Article 7 (4) GDPR).

The person responsible leads to this in your form "Declaration of consent to

Data processing – Data Protection Act" from:

"[...] The unencrypted transmission of personal data (see

Information sheet on data protection on pages 2 and 3) is in accordance with

European General Data Protection Regulation not allowed because of the protection and

the integrity of the data cannot be guaranteed.

Therefore, the Allergy Day Clinic D*** needs an explicit and

written consent of all patients

to process personal data in the future and to do so unencrypted

send and receive (dispatch of findings by e-mail, telephone

Findings information, etc.)"

Under the part to be filled out by the person concerned (with name, date of birth and other

contact details) can be found, framed and with a pre-ticked box

provided the following text passage:

"I expressly agree that personal data

(especially information about my condition when I took over the consultation or

treatment, history of disease, diagnosis, den□

Course of the disease, my findings and information about the type and extent□

of advisory, diagnostic or therapeutic services□

including the use of medicinal products) is processed and stored□

and in unencrypted form to and from the accordingly□

relevant third parties. The approval of the□

unencrypted transmission can be used at any time with effect for the future□

be revoked. I further agree irrevocably that the allergy□

Day Clinic D*** at any time other companies and/or persons□

carrying out the agreed service. this concerns□

also the processing including storage of personal data. I□

I acknowledge that the transmission of the data (unauthorized)□

Third parties can obtain knowledge of the information and this data□

can be changed. I understand that this is to disclose my□

health condition can result. I am aware that the allergy□

Day clinic D *** no liability for the correct and complete□

transmission of the data."□

3.2. The consent demanded from the data subjects turns out to be inadmissible□

out.□

3.2.1. First of all, the consent cannot be inferred with the necessary clarity for□

which data processing the consent represents the legal basis. In the□

The information provided according to Art. 13 GDPR is the legal basis□

Consent is mentioned, but there are also other legal bases, such as the□

Fulfillment of legal obligations or the protection of legitimate interests.□

In this respect, it is unclear for which specific data processing the consent is given□

legal basis is.□

The declaration of consent therefore proves to be illegal in this respect (cf

also the decision of the data protection authority of July 31, 2018, GZ DSB-D213.642/0002-

DSB/2018; not published yet).

3.2.2. The person responsible binds the consent to data processing to a

Consent to the unencrypted transmission of data because it means the GDPR

stipulate a - not even indirectly derivable from the relevant regulations -

Obligation to transmit data in encrypted form.

However, we cannot accept any obligation to encrypt the transmission

a declaration of consent from data subjects. The question,

whether a transmission takes place in encrypted or unencrypted form is namely

one of the data security measures according to Art. 32 GDPR and thus solely from the

to judge those responsible. A consent within the meaning of Art. 6 Para. 1 lit.

Art. 9 Para. 2 lit. a GDPR is not permissible because the consent is not given here

serves to create a legal basis for data processing, but to

of - if necessary - data security measures to the detriment of

to be able to deviate from those affected.

For this reason, too, the requested consent proves to be inadmissible.

3.2.3. The declaration of consent also states that the data subject

"irrevocably" agrees "that the allergy day clinic D*** at any time other

Companies and/or persons to carry out the agreed service

may use. This also applies to the processing including storage of

personal data."

This passage can only be understood to mean that the use of

Contract processors are approved, for which the relevant regulations in Art. 28

Find GDPR. The decision as to whether a processor is used is up to you

also solely the person responsible, who also has the duty to carefully select and

to conclude a contract with a specific content with the processor.

Consequently, the use of processors is subject to the consent of data subjects

not accessible, which is why a relevant consent is not legally effective

can be granted. The consent therefore proves to be valid in this respect as well

unlawful.

Finally, it should be pointed out that an "irrevocable" consent in any case

of the GDPR, which therefore cannot be demanded (cf. Art. 7 Para. 3

GDPR) and any consent in this regard would also not be binding

(Art. 7 para. 2 GDPR).

3.2.4. The declaration of consent also contains the passage according to which those affected

Acknowledge "that through the transmission of the data (unauthorized) third parties become aware

about which information can be obtained and this data can be modified. It is ... with me

aware that this may lead to the disclosure of my state of health. It is ... with me

aware that the Allergy Day Clinic D*** accepts no liability for the correct and

complete transmission of the data."

Again, aspects of data security according to Art. 32 GDPR

addressed, of which by means of consent to the detriment of those affected not

can be deviated from. Rather, it is the duty of a person responsible adequate

to take measures to ensure that there is no violation of the

protection of personal data and consequently the requirements of the GDPR

are complied with (Art. 24 GDPR).

Consequently, this part of the declaration of consent also proves to be unlawful.

4. Regarding point 3 (violation of the information obligations):

4.1. In the information provided, no structural distinction is made as to whether it is in accordance with Art. 13

or Art. 14 GDPR is granted. However, this distinction is important in that

as information is also to be provided under Art. 14 GDPR, Art. 13 GDPR is not

covers. According to Art. 14 Para. 1 lit. d, the information is to be given which

categories of personal data are processed; same is – different from in

Art. 13 - to also provide information about the origin of the data (Art. 14 para. 2 lit. f

GDPR).

According to the case law of the ECJ (judgment of October 1, 2015, C-201/14, still on

Legal situation according to Directive 95/46/EC, whereby this decision also applies to Art. 13

and 14 GDPR relevance) comes the information obligations an essential

importance, because the scope of the right to information in any case precludes the exercise of

to enable the right to information.

Apart from that, from the point of view of those affected, it is necessary for them to provide an explanation

can see clearly and unequivocally which data is collected directly from them

and which data may be used from other sources (see

see Art. 12 Para. 1 GDPR), which, however, involves different information obligations

tie

By not clearly distinguishing between the information requirements in the information requirements

Art. 13 and Art. 14 GDPR are distinguished, the person responsible has against them

obligations as well as Art. 12 Para. 1 GDPR.

4.2. As noted, the controller would have appointed a data protection officer

have to. In the information provided, Mag. Walter Josef Ä*** as

Named data protection officer, although he was not appointed as such. With that

gives the false impression that those responsible have a

Data protection officer who has all the guarantees of Art. 38 GDPR,

has ordered.

As a result, the person responsible has breached its obligation under Article 13 (1) (b) and Article 14

Para. 1 lit. b in conjunction with Art. 37 et seq. GDPR.

4.3. In the data protection declaration, only “Art. 5 para. 1b"

(probably meaning: Art. 6 Para. 1 lit. b) and Art. 6 Para. 1 lit. a, lit. c and lit. f GDPR.

Since the person responsible is indisputably special categories of personal data

processed according to Art. 9 GDPR (namely health data), the

Legal basis for the processing of this data exclusively according to Art. 9 Para. 2

GDPR.

It is therefore the task of those responsible to check whether, given their field of activity

Art. 6 GDPR is relevant as the legal basis for data processing.

Because the person responsible has failed in its data protection declaration to

relevant legal bases for the processing of special categories

to provide personal data, contrary to its obligation under Article 13 (1) lit. c

and Article 14 (1) (c) GDPR.

4.4. According to Art. 13 Para. 1 lit. d and Art. 14 Para. 2 lit. b GDPR, a person responsible,

if the data processing is based on Art. 6 Para. 1 lit. f GDPR ("Processing to protect

legitimate interests of the person responsible or a third party"), the legitimate

List interests pursued by the person responsible or the third party.

If the person responsible does not comply with this obligation in their data protection declaration,

has violated the cited provisions of the GDPR.

It should be noted that this legal basis is exclusively for the processing of

Data that does not fall under Art. 9 GDPR can be used.

4.5. In the data protection declaration, consent is used as a legal basis for the

Data processing mentioned, but without – as required by Art. 13 Para. 2 lit. c or Art. 14

Paragraph 2 lit. d DSGVO required - to point out that a right to at any time

Withdrawal of consent exists without affecting the legality of the

Consent is affected by the processing that has taken place up to the point of revocation.

The person responsible therefore violated the cited provisions.

5. Regarding point 4 (violation of the obligation to check whether a data protection

impact assessment is required):

The person responsible explains that the data processing, which is carried out in its

Processing directory under II.B. “Patient Management” trades, not one

"written" data protection impact assessment (DPIA), since

the exceptional circumstances of § 1 in conjunction with DSFA-A12 apply according to the annex to the DPFA-AV.

In this regard, it must be stated that the person responsible can already be seen from the explanatory notes

(available on the website of the data protection authority) should have established that the

Patient Management - Limited to the subject of managing the records that

usually also occur in customer administration - only then not to a DPIA

undergo if it is administered by a single physician.

For the processing activities

 Patient files (address, billing and registration data)

 Settlement (settlement with social security)

 Request for findings/transmission of findings (transmission and disclosure),

 Examination of samples (examination and dispatch of samples [blood,

secretion etc.]),

 Management of prescriptions (storing which prescriptions patients

require),

 Pharmacy (operation, administration, billing and organization of

medicine chest),

all health data known to those responsible is managed,

disclosed and transmitted. Thus, from the wording of Art. 35 Para. 2

lit. b DSGVO clearly shows that in these cases the examination of the necessity of a

DPIA would have been required.

According to § 2 Para. 3 Z 1 DSFA-V, the extensive processing is subject

personal data according to Art. 9 GDPR in any case to a DPIA if

in addition, at least one further criterion according to paragraph 3 is met (for "extensive

Processing" see again the guidelines on data protection cited above

impact assessment).

It should be noted that the DPFA-AV and the DPFA-V do not

contain concluding enumerations, but only processing operations

list, which in any case are subject to one or no DPIA. Is a

The processing operation is not covered by one of the two regulations

Those responsible have the obligation to check in each individual case whether a DPIA is required or not

not. The already cited guidelines on data protection

impact assessment are used.

It is therefore the responsibility of those responsible, based on the above

To check whether the data processing mentioned here is subject to a DPIA

are subjected to or not.

However, since the person responsible assumed incorrectly that

in any case, if it did not have to carry out a DPIA, it has, contrary to its obligation under Art. 35

breach GDPR.

6. Regarding the performance mandate (paragraph 5):

The performance mandate is based on Art. 58 Para. 2 lit. d GDPR. A time limit of eight

weeks seems appropriate to meet the performance mandate.