

GZ: DSB-D213.864/0003-DSB/2019 of December 16, 2019□

[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 against the municipality in an official examination procedure□

Z\*\*\*, \*\*\*1 \*\*\*Z, \*\*\*straße 7, as the operator of the seaside resort Z\*\*\* as follows:□

1. The official examination procedure was justified and it is found that the□

Processing of personal data (biometric data) using□

Palm vein scanner for the purpose of access control to the seaside resort by the□

Municipality Z\*\*\* unlawfully.□

2. The Municipality of Z\*\*\* will be informed of the further processing of this data by means of□

Palm vein scanners prohibited with immediate effect.□

3. The community Z\*\*\* is charged within a period of 4 weeks the previous□

personal data processed for access control purposes□

(biometric data) to delete.□

Legal basis: Art. 4 nos. 1, 2, 7, 11 and 14, Art. 5, Art. 6 Para. 1 lit. a, Art. 7, Art. 9□

Paragraphs 1 and 2, Article 57 Paragraph 1 letter a and letter h, Article 58 Paragraph 1 letter b and Paragraph 2 letter d, letter f  
lit. g of Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR), OJ.□

No. L 199 of 05/04/2016, p. 1.□

REASON□

A. Submissions and Proceedings□

1. The data protection authority directed after anonymous advertisements and media reports about the□

alleged use of a palm vein scanner in the seaside resort of Z\*\*\*

Test procedure (“data protection check”) against the municipality of Z\*\*\* as the operator of the

Seaside resort Z\*\*\*.

2. By letter dated August 7th, 2019, the data protection authority requested the municipality of Z\*\*\*

to comment on the following points or the designated documents and

Lists to submit:

The municipality of Z\*\*\* was asked to provide a list of

processing activities within the meaning of Art. 30 GDPR.

Municipality Z\*\*\* was requested to state whether with regard to the initially

mentioned data processing a data protection impact assessment iSv Art. 35

GDPR has been carried out and if not, why it was not carried out.

If so, the corresponding data protection impact assessment had to be submitted.

Municipality Z\*\*\* was asked to state which specific ones

Legal basis for such processing of personal data -

in particular the processing of special categories of personal data iSv

Art. 9 GDPR – is supported.

If such processing of personal data is based on consent

iSv Art. 4 Z 11 DSGVO is supported, the municipality Z\*\*\* was requested to provide more details

carry out, in what way and under what circumstances such

consent is obtained. In addition, it was applied

data protection authority a corresponding excerpt of a declaration of consent

to submit.

If such processing of personal data is based on consent

iSv Art. 4 Z 11 DSGVO is supported, the municipality Z\*\*\* was also asked

to explain to what extent the mandatory use of a palm vein scanner for

season ticket holder is compatible with the ban on coupling.□

□ The community Z\*\*\* was finally asked to explain which ones□

Appropriate technical and organizational measures have been taken to ensure that□

meets the requirements of the GDPR and the rights of the data subjects□

are protected (Art. 25 GDPR) and in particular to explain how the□

Security of processing (Article 32 GDPR) is guaranteed.□

4. By Opinion dated October 15, 2019, received October 18, 2019,□

the municipality of Z\*\*\* presented a bundle of documents. Below are□

including a list of processing activities, an excerpt of a□

Declaration of consent, an information sheet on the palm vein scanner, a tabular□

Overview of technical and organizational measures and two□

Processor Agreements. Furthermore, the municipality of Z\*\*\* made the following statement:□

By letter from the data protection authority dated August 7th, 2019. (received cm 03.09.2019)□

the community Z \*\*\* was informed that an ex officio investigation procedure against them as□

operator of the seaside resort was initiated.□

With the same letter, the municipality of Z\*\*\* was given the opportunity to□

to comment on the points mentioned in writing.□

The municipality Z\*\*\* reimburses the following within an open period□

opinion□

and executes it as follows:□

To 1.:□

A copy of the processing directory in accordance with Art. 30 GDPR of the municipality of Z\*\*\*□

will be sent in the attachment (enclosure I).□

To 2.:□

The biometric data is anonymized and is used by a one-way function□

processed and encrypted using so-called templates. It's not possible to get out of here□

Conclusions of personal data, such as name, age, gender, □

state of health or the like. In addition, these are encrypted □

Templates separated from actual personal data of the data subject □

stored in such a secure manner that the data structures do not allow any conclusions to be drawn about the □

actual owner can be drawn. □

Because the processing does not pose a high risk to the rights and freedoms □

natural persons, there was no need for one □

Carry out data protection impact assessment according to Art. 35 GDPR. □

To 3.: □

The data subjects have the processing of said personal data □

Godparents expressly consented for a specified purpose. □

The processing purpose is clear because only one person has access to the seaside resort □

and it is not possible to pass on this entry. □

The seaside resort is managed as a private business by the municipality of Z\*\*\*. For the □

Entry fees are fixed for access to the seaside resort. □

In order to ensure access control and to rule out misuse, the □

Installation of a simple access system installed. □

To 4.: □

The processing of personal data is only carried out when purchasing a □

Season ticket carried out personally in the seaside resort of the municipality of Z\*\*\*. □

In this case, the consent of the persons concerned is unequivocal, since they are □

consent to the processing of the data concerned. □

The declaration of consent form is included in the attachment (Annex 2). □

To 5.: □

Any visitor to the seaside resort who does not consent to the processing of the □

personal data the possibility of purchasing a day pass. □

The reason for processing personal data is to ☐

To prevent misuse of season tickets by passing them on. ☐

To 6: ☐

A copy of the catalog of measures (technical organizational measures) of ☐

Municipality Z\*\*\* is sent in the enclosure (Enclosure 3). ☐

In addition to the statement on points 1 to 6, the municipality of Z\*\*\* ☐

provided the following information: ☐

- Contract for order processing X\*\*\* GmbH (Annex 4). ☐

- Contract for order processing by Y\*\*\* GmbH (Annex 5) ☐

- Information regarding palm vein scanner company A\*\*\* (Enclosure 6) ☐

- Contract for data protection officer (Appendix 7). ☐

Finally, it is stated that over two thousand registrations have been made. ☐

Information according to Art. 15 GDPR was requested by five people and by the ☐

Municipality Z\*\*\* answered in time. ☐

Side dishes: ☐

processing directory ☐

declaration of consent ☐

catalog of measures ☐

Processor Agreement x ☐

Processor Agreement y ☐

Information palm vein scan ☐

Contract for data protection officer ☐

B. Test item ☐

It must be checked whether the processing of biometric data carried out by means of ☐

Palm vein scanner by the municipality of Z\*\*\* is carried out lawfully and thus the DSGVO ☐

is equivalent to. ☐

### C. Findings of Facts

The municipality Z\*\*\* is the operator of the seaside resort Z\*\*\*. For access control purposes the seaside resort for season ticket holders became a palm vein scanner in May 2019. Installed. The investment costs were 50,000 euros. This is done via the adjustment of the vein pattern of the palms a biometric identity check. To the effect that the palm vein sensor uses infrared light to record the vein image, which is being absorbed by the red blood cells in the veins. This will change the vein structure, which is made visible to an infrared camera and thus forms the basis of the biometric pattern.

To purchase a season ticket, it is a requirement that the vein pattern of both

hands be recorded at the checkout and from now on every time you enter the

Seebad to use the palm vein scanner. An alternative access option is for

Season ticket holders no longer provided. Access without palm vein scan is as

Bathing guest only possible by purchasing a day ticket.

The price for a day ticket for adults was 4.50 euros in 2019. for one

Season tickets for adults were charged at 50 euros.

Furthermore, you are only entitled to open the access barriers with a season ticket in order to

as a tenant with access rights to a boat mooring to those in the seaside resort

to drive to boat berths. Opening the access barriers using a

Day ticket is not possible.

Before the vein pattern when purchasing a season ticket for the first time at the checkout

is recorded, bathers must sign the following declaration of consent:

Consent to the collection, processing and storage of biometric data

in terms of the General Data Protection Regulation (EU)

2016/679

The municipality of Z\*\*\* (hereinafter referred to as "operator") is set to

Biometric technology for the purpose of verifying/identifying data subjects□

F\*\*\*Secure™ in various forms.□

These are: Access to the seaside resort.□

In the following, the personal consent of the person concerned is requested:□

Hereby I declare,□

First name surname:□

Address:□

Year of birth:□

my agreement that my biometric information - specifically my specific□

Vein pattern of the right and left palms for the purpose of□

Verification/identification to the operator's IT and access systems equipped in this way□

centrally recorded, processed and stored. Any further use as well as the□

The operator is expressly prohibited from passing on this data.□

The biometric data is anonymized and is used by a one-way function□

processed and encrypted using so-called templates. It's not possible to get out of here□

conclusions about personal data such as name, age, gender,□

state of health or the like. In addition, these□

encrypted templates separated from actual personal data of the□

Affected stored securely, so that due to the data structures no□

conclusions about the actual owner can be drawn.□

I am aware that I can revoke this consent at any time. The revocation has in□

Text form to the operator of the system.□

Place and date□

signature□

Evidence assessment: The statements made are based on the opinion of the□

Municipality Z\*\*\* of October 15, 2019, ha. received on October 18, 2019, and the□

Attachments submitted with it. Also on the various media reports (U\* article□  
from 22.07.2019 [https://www.u\\*.at/oesterreich/handvenenscanner-seebad-z\\*\\*\\*-5\\*739\\*\\*4;](https://www.u*.at/oesterreich/handvenenscanner-seebad-z***-5*739**4;)□  
P\* article from 17.07.2019 [https://p\\*.at/chronik/seebad-wer-saisonkarte-will-muss-](https://p*.at/chronik/seebad-wer-saisonkarte-will-muss-)□  
[register palm veins/\\*2746\\*391](https://www.q*.at/story/*68439**4/handvenenscan/seebad-sorgt-fuer-aufregung); Q\* article from 07/18/2019□  
[https://www.q\\*.at/story/\\*68439\\*\\*4/handvenenscan/seebad-sorgt-fuer-aufregung](https://www.q*.at/story/*68439**4/handvenenscan/seebad-sorgt-fuer-aufregung); \*TV□  
Sender \*\* from 19.07.2019 [https://\\*ort.at/stories/\\*\\*4981\\*/](https://*ort.at/stories/**4981*/); Report of "The Greens &□  
Independent Z\*\*\*\*" \*- Editorial from May 15, 2019 [https://.www.leben-z\\*\\*.at/wp-](https://.www.leben-z**.at/wp-)□  
[content/uploads/sites/1\\*/201\\*/0\\*/ZumThema\\_Handvenenscanner\\_Seebad\\_29846\\*\\*8.pdf](https://.www.leben-z**.at/wp-content/uploads/sites/1*/201*/0*/ZumThema_Handvenenscanner_Seebad_29846**8.pdf);□  
all last queried by the data protection authority on December 12, 2019). The Findings□  
to the entrance fees of the seaside resort Z\*\*\* result from the information on the□  
Community website, [https://www.z\\*\\*\\*at/feizeit/seebad](https://www.z***at/feizeit/seebad) (requested by the□  
Data Protection Authority on 12.12.2019).□

D. In legal terms it follows that:□

D.1. To the official test procedure□

The data protection authority initiated on the basis of Article 58 (1) (b) GDPR□  
ex officio review procedure ("data protection review") against the municipality of Z\*\*\* (in□  
Consequence: operator) who operates the seaside resort Z\*\*\*.□

D.2. On the distribution of roles under data protection law□

The operator is responsible for the biometric access control she carries out using□  
Palm vein scanner according to their own statements (point 19 of the submitted□  
Processing directory) as the person responsible for data protection pursuant to Art. 4 Z 7□  
to qualify for GDPR. Municipality Z\*\*\* also appears on the form shown above□  
for the declaration of consent, giving outsiders the impression that□  
that the municipality Z\*\*\* is responsible. In the opinion of the Municipality of Z\*\*\*□  
is stated on p. 2 that the seaside resort as a private enterprise□  
community is led; more information and evidence that this□



Operation is also to be qualified as the person responsible within the meaning of the GDPR, but are in the process

didn't come out.

The data protection authority therefore comes to the conclusion that the municipality of Z\*\*\*

Responsible according to Art. 4 Z 7 DSGVO for the processing of data by means of

palm vein scanner is.

### D.3. Processing of biometric data

According to Art. 4 Z 14 DSGVO are "biometric data" with special technical

Procedures obtained personal data on the physical, physiological

or behavioral characteristics of a natural person that are unique

Enable or confirm identification of that natural person, such as facial images

or dactyloscopic data.

According to Art. 4 Z 2 GDPR, "processing" means anyone with or without help

process carried out by automated processes or any such series of processes in

connection with personal data such as collecting, capturing, the

Organizing, ordering, storing, adapting or changing

Reading, querying, use, disclosure by transmission,

distribution or any other form of provision, matching or

association, restriction, deletion or destruction.

Images of palm vein patterns are - as noted - with a special

technical process (using infrared light). palm vein pattern

are among the physiological characteristics of a person, can be a natural

clearly assign a person and thus enable the clear identification of a person

natural person. Palm vein pattern as biometric data within the meaning of Art. 4 Z 14 GDPR

are therefore undoubtedly also personal data within the meaning of Art. 4 Z 1 DSGVO. For the

Use of the palm vein scanner for access control purposes

Hand vein samples recorded by data subjects, iSv Art. 4 Z 2 GDPR

processed.□

In principle, the processing of biometric data applies in accordance with Art. 9 Para. 1 GDPR□

to uniquely identify a natural person as processing special□

Categories of Personal Data ("Sensitive Data"). The processing of this data□

is prohibited unless the processing is based on one of the items listed exhaustively in paragraph 2□

Intervention facts can be supported. An exception to this is according to Art. 9 Para. 2□

lit a. GDPR if the data subject is involved in the processing of the said□

personal data for one or more specified purposes expressly□

has consented.□

D.4. Principles for the processing of personal data□

Article 5 GDPR reads:□

Principles for the processing of personal data□

(1) Personal data must□

a) lawfully, fairly and in a manner that is fair to the data subject□

be processed in a comprehensible manner ("lawfulness, processing in good faith□

faith, transparency");□

b)□

collected for specified, explicit and legitimate purposes and not in any□

further processed in a way that is incompatible with those purposes; one□

Further processing for archiving purposes in the public interest, for□

scientific or historical research purposes or for statistical purposes□

not considered incompatible with the original purposes in accordance with Article 89(1).□

("earmarking");□

c) adequate and relevant to the purpose and necessary for the purposes of the processing□

be limited to what is necessary ("data minimization");□

d) accurate and, where necessary, up to date; it is all□

to take reasonable measures to ensure that personal data with regard to

the purposes of their processing are incorrect, be erased or rectified immediately

("Accuracy");

e)

stored in a form that allows identification of data subjects only

for as long as is necessary for the purposes for which they are processed;

personal data may be stored longer if the personal

Data subject to the implementation of appropriate technical and organizational

Measures taken by this regulation to protect the rights and freedoms of

data subject are required, exclusively for purposes of public interest

Archival purposes or for scientific and historical research purposes or for

statistical purposes are processed in accordance with Article 89 paragraph 1 ("storage limitation");

f)

processed in a way that ensures adequate security of the

personal data, including protection against unauthorized or

unlawful processing and against accidental loss, accidental

Destruction or accidental damage by appropriate technical and

organizational measures ("integrity and confidentiality");

(2) The person responsible is responsible for compliance with paragraph 1 and must

Be able to demonstrate compliance ("accountability").

The ECJ states in its case law that the processing of personal

Data relate to at least one fact according to Art. 7 of Directive 95/46/EC

(now: Art. 6 GDPR) and in Art. 6 of this guideline (now:

Art. 5 GDPR) must comply with the principles set out (judgment of December 11

2019, C-708/18, margin no. 36).

These principles also include the principle of data minimization according to Art. 5

Paragraph 1 lit. c GDPR.□

#### D.5. General information on the principle of data minimization□

The principle of data minimization is the reduction of□

Processing of personal data to the essential. The data minimization□

ensures that the processing is qualitative for the specified processing purpose□

and is quantitatively limited.□

Data minimization means that data processing is appropriate and appropriate for the purpose□

be substantial and limited to what is necessary for the purposes of the processing□

got to. Adequacy is the proportionality test□

narrower sense. The relevance denotes the suitability within the meaning of the□

constitutional doctrine of proportionality, i.e. whether a□

data processing is conducive to achieving the purpose at all. With the restriction□

to the extent necessary, it is finally made clear once again that the data is not□

may go beyond the purposes. This requirement is regularly□

adequacy and relevance consumed [cf. instead of many□

Hötzendorfer/Tschohl/Kastelitz in Knyrim, DatKomm Art 5 GDPR Rz 34 ff (as of□

1.10.2018, rdb.at)].□

#### D.6. General information on data protection consent and the prohibition on coupling□

According to its own statements, the operator supports the processing of personal data□

Data of affected persons for the purpose of access control in Seebad Z\*\*\* only on the□

Legal basis of the consent according to Art. 9 Para. 2 lit. a GDPR.□

According to Art. 4 Z 11 GDPR, "consent" of the data subject means any□

voluntarily for the specific case, in an informed manner and unequivocally□

given declaration of intent in the form of a declaration or another clear one□

affirmative action by which the person concerned indicates that they are with the□

processing of the personal data concerning you.□

In accordance with Art. 7 GDPR and taking into account Art. 4 Z 11 and recital 43

GDPR, consent must be given voluntarily and may not be linked to the fulfillment of a

contract, although this consent to the performance of this contract is not

is required. Consent is involuntary if, in the event of non-submission of the

consent, a disadvantage is to be expected (cf. the decision of the data protection authority

from April 16, 2019, GZ DSB-D213.679/0003-DSB/2018).

The former Art. 29 Data Protection Working Party has dealt with the concept of the

"Consent" employed and an analysis of the term made. She has

also dealt with the disadvantages that prevent voluntariness and is

came to the conclusion that such a disadvantage exists when

Risk of deception, intimidation, coercion or significant adverse consequences

consists. The controller must demonstrate that it is possible to obtain consent

refuse or revoke without suffering any disadvantages. A responsible person must

for example, demonstrate that refusing or withdrawing consent is not

leads to costs for the data subject and consequently to a clear disadvantage.

Furthermore, the controller should prove that the data subject is a real or

had a free choice whether to consent or not (cf. Art. 29 Data Protection Working Party, guidelines in

Reference to consent pursuant to Regulation 2016/679, WP 259, rev. 01 p. 12; cf. also

recital 42 GDPR; see also the decision of the data protection authority of

30 November 2018, GZ DSB-D122.931/0003-DSB/2018).

The element "free" implies that the individuals concerned have a real choice and the

have control In general, the GDPR requires that consent is not

is valid when the data subject has no real choice to consent

feels pressured or suffers negative consequences if she does not comply.

When consent is a non-negotiable part of terms and conditions, it will

assumed that the consent was not given voluntarily. Art. 7 para. 4 of the GDPR

points out, among other things, that a situation in which the consent with the acceptance of contract terms is "bundled" or the performance of a contract or the provision of a service with a request for consent to a processing of personal data necessary for the fulfillment of the contract are not required, is considered to be highly undesirable. Will consent given in such a situation is deemed not to have been given voluntarily (cf. recital 43 GDPR).

When the controller is performing a contract with a request for consent linked, a data subject who gives the person responsible their does not wish to make personal data available for processing, consequently runs the risk of being denied the services she has asked for (cf. again the notification of April 16, 2019).

When coupling the consent to a processing of non-contractual personal data with the conclusion of a contract is fundamentally of this to assume that the granting of consent is not voluntary, if not in Individual case special circumstances for a voluntary data protection

Speak consent (see the judgment of the Supreme Court of August 31, 2018, GZ 6 Ob 140/18h mwN).

According to the case law of the data protection authority, it must also be taken into account that a voluntary consent can be given if a certain processing operation also to the recognizable advantage of the person concerned (cf. instead of many the Notice of March 8, 2006, GZ K178.209/0006-DSK/2006; cf. also Kotschy in Brodil (ed.), Data protection in labor law [2010] 3).

D.7. In the matter

lawfulness of data processing

Since specific categories of personal data are processed,

the lawfulness of the processing is based exclusively on Art. 9 Para. 2

GDPR.

A - legally compliant - consent is the legal basis according to Article 9 Paragraph 2 lit

GDPR under consideration.

In this context, the question arises as to whether the form "Consent to

the collection, processing and storage of biometric data within the meaning of

General Data Protection Regulation (EU) 2016/679" consent to the processing

personal data of the data subjects standardized in the GDPR

meets requirements.

In this specific case, season ticket holders - as has been established - are entitled to use the

Palm vein scanners required. Purchasing a season ticket requires that a

Declaration of consent is signed, otherwise only the purchase of a day pass

possible. There is an alternative access option (without using the palm vein scanner).

it does not for season ticket holders. If a data subject does not give such consent

from, the consequence and the clear disadvantage is that no season ticket for

to be able to purchase the seaside resort. Those affected have real choice and control

therefore not people.

With reference to the general statements on the ban on coupling (cf. D.6.), it is

obvious that the consent under examination is not "voluntary". the

Possibility to purchase a day pass without using the palm vein scanner

does not constitute a lawful alternative option because the data subject will no doubt be affected by it

considerable additional costs would arise, as already argued by the

Shows those responsible, especially in the case of season ticket holders, the objective

wanting to use a biometric verification system to avoid misuse. Apart from that

of which is the use of the boat berth only with a season ticket - and not with

a day ticket – possible.

In this context, it is also necessary to check which processing operations are carried out for the

fulfillment of the contract (provision of a service) are required at all. The

The ban on coupling only includes consent that is not necessary for the purpose of the contract

required are. The "necessity" is to be measured against the purpose of the contract. core purpose

the purchase of a season ticket is the seasonal use of the seaside resort and the

associated infrastructure.

From the point of view of the data protection authority, the consent to the data processing has been given

a palm vein scanner is not required to use the infrastructure. Is required

only that there is access control to the seaside resort to prevent unauthorized persons from entering

prevent use.

As a result, it can be stated that the ban on coupling violated and consent to

the data processing under examination is inadmissible.

In the absence of permissible consent of the persons concerned in the processing of the biometric

(and thus special category of) data and in the absence of applicability others

Exceptions within the meaning of Art. 9 Para. 2 GDPR, there is a lack of one under review

Legal basis for lawfulness of processing.

For this reason alone, the data processing in question proves to be

unlawful and consequently non-compliant with the GDPR.

Proportionality / Data Minimization

Even if one relies on legitimate consent (or another legal basis)

out, the data processing in question would still be disproportionate and

consequently does not correspond to the principle of Article 5 (1) (c) GDPR.

Personal data may only be processed if the purpose of the

Processing cannot be reasonably achieved by other, milder means

can (cf. recital 39 GDPR and the already cited judgment of the ECJ of

December 11, 2019, margin no. 47 f).



The former Article 29 Data Protection Working Party also issued a statement on the

Risks of biometric technologies pointed out and the

proportionality test highlighted (cf. Article 29 Working Party,

Opinion 3/2012, WP193):

“When using biometric data, the question of proportionality arises

of the data processed in the individual categories against the background of the

for the purpose of the respective processing. Because biometric data is only used

if they are appropriate and relevant and not excessive

The scope must be covered, the necessity and proportionality of the

processing are strictly checked. In addition, it must be checked whether the

intended purpose with greater respect for privacy

could be achieved.

When analyzing the proportionality of a proposed biometric

Systems is to check in advance whether the system is required to the determined

to fulfill the purpose d. H. whether this system for the fulfillment of this purpose

actually essential or merely the most convenient or least expensive solution

represents. A second factor is whether the system is designed to perform

Purpose is probably efficient. In this context, the specific

Characteristics of the proposed biometric technology to be taken into account. A

The third aspect is to weigh up whether the expected impairment of

Privacy is in proportion to the expected benefit. If this benefit

is relatively low and, for example, only in terms of increased convenience or in

a small cost saving is the invasion of privacy

not considered proportionate. The fourth aspect for evaluating the

The adequacy of a biometric system consists in examining whether the

desired result could not also be achieved with means which the

privacy would be less compromised.”□

The purpose of the data processing in question is access control□

Seebad Z\*\*\*.□

The operator herself states that the use of the palm vein scanner also□

serve to prevent the season tickets from being passed on.□

However, the expected benefit is disproportionate to the biometric test carried out□

Data processing:□

Biometric data is inherently personal, unique and not□

amendable and therefore by its very nature with regard to fundamental rights and□

fundamental freedoms particularly sensitive. They deserve special protection because in□

There are significant risks associated with their processing (cf. also□

recital 51 GDPR). The question of proportionality is in view of the of the□

The purpose pursued by the operator must therefore be checked strictly.□

The processing that is the subject of the procedure would only be permissible if the purpose of the□

Processing cannot reasonably be achieved by other means.□

However, that is not the case in the present case.□

Couldn't be a milder alternative to access control with a palm vein scanner□

transferable season tickets are issued with a photo of the ticket holder that□

either controlled and reconciled upon entry by staff (such as this□

is also common in the Viennese baths, cf.□

<https://www.wien.gv.at/freizeit/baeder/zugangspreise/monatskarten.html>, retrieved on□

December 6, 2019) or which are randomly checked in the seaside resort (as with□

a ticket inspection on public transport). Such an approach□

would also be looking at the investment costs of 50,000 euros and ongoing□

Maintenance costs of the palm vein scanner reasonable.□

In addition to the principle of lawfulness of processing is therefore also the principle□

violated data minimization.□

The data protection authority also does not overlook the fact that the operator comprehensive□

technical and organizational measures have been taken, however, the aspect of□

Security of processing for the proportionality test iSd□

data minimization principle itself irrelevant. It is only necessary to check whether it□

There are milder means of achieving an end that involve less severe intervention for those affected□

mean people. Since there are - as explained - such milder means, in the□

specific case violated the principle of data minimization and is also from this□

reason to assume the inadmissibility of the subject data processing.□

The security of the processing would at best be within the framework of the principle of integrity□

and to check confidentiality (Art. 5 Para. 1 lit. f GDPR), according to which personal□

Data must be processed in a way that ensures adequate security□

personal data, including protection against unauthorized or□

unlawful processing and against accidental loss, accidental□

Destruction or accidental damage by appropriate technical and□

organizational measures. Furthermore, security measures iSv□

Safeguards to prevent or mitigate unreasonable consequences for□

Those affected who were implemented by the operator as part of a□

Weighing of interests within the meaning of Art. 6 Para. 1 lit. f GDPR must be taken into account (cf. on the□

Key factors to consider in a balancing of interests, Art. 29-□

Data Protection Working Party, Opinion 06/2014 on the concept of legitimate interest□

controller according to Article 7 of Directive 95/46/EC, WP 217,□

844/14/EN, p. 43). Such a balancing of interests occurs when examining whether□

there are milder means of achieving the purpose in accordance with the principle of data minimization,□

However not. The technical and organizational measures taken were important□

therefore not go into any further at this point.□

#### D.8. Result□

Since the data processing under examination lacks a permissible legal basis□

has already taken place unlawfully, but on the other hand also disproportionately (Art. 5 Para. 1 lit. c□

GDPR), the operator was to be given a corresponding service contract and the□

Prohibit data processing and delete the existing ones□

apply personal data.□

The performance mandate is based on Article 58 (2) lit. f and g GDPR.□

It was therefore to be decided accordingly.□