

[Anmerkung Bearbeiter: Namen und Firmen, Rechtsformen und Produktbezeichnungen, Adressen (inkl. URLs, IP- und E-Mail-Adressen), Aktenzahlen (und dergleichen), etc., sowie deren Initialen und Abkürzungen können aus Pseudonymisierungsgründen abgekürzt und/oder verändert sein. Offenkundige Rechtschreib-, Grammatik- und Satzzeichenfehler wurden korrigiert.]

B E S C H E I D

S P R U C H

Die Datenschutzbehörde entscheidet im amtswegigen Prüfverfahren gegen die Gemeinde Z***, ***1 ***Z, ***straße 7, als Betreiber des Seebades Z*** wie folgt:

1. Das amtswegige Prüfverfahren war berechtigt und es wird festgestellt, dass die Verarbeitung personenbezogener Daten (biometrische Daten) mittels Handvenenscanner zum Zweck der Zutrittskontrolle zum Seebad durch die Gemeinde Z*** unrechtmäßig erfolgt.
2. Der Gemeinde Z*** wird die weitere Verarbeitung dieser Daten mittels Handvenenscanner mit sofortiger Wirkung untersagt.
3. Der Gemeinde Z*** wird aufgetragen, binnen einer Frist von 4 Wochen die bisher für Zwecke der Zutrittskontrolle verarbeiteten personenbezogenen Daten (biometrische Daten) zu löschen.

Rechtsgrundlagen: Art. 4 Z 1, 2, 7, 11 und 14, Art. 5, Art. 6 Abs. 1 lit. a, Art. 7, Art. 9 Abs. 1 und 2, Art. 57 Abs. 1 lit. a und lit. h, Art. 58 Abs. 1 lit. b und Abs. 2 lit. d, lit. f und lit. g der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO), ABl. Nr. L 199 vom 4.5.2016, S. 1.

B E G R Ü N D U N G

A. Vorbringen und Verfahrensgang

1. Die Datenschutzbehörde leitete nach anonymen Anzeigen und Medienberichten über den behaupteten Einsatz eines Handvenenscanners im Seebad Z*** ein amtswegiges Prüfverfahren („Datenschutzüberprüfung“) gegen die Gemeinde Z*** als Betreiberin des Seebades Z*** ein.

2. Mit Schreiben vom 07. August 2019 forderte die Datenschutzbehörde die Gemeinde Z*** auf, zu folgenden Punkten Stellung zu nehmen bzw. die bezeichneten Dokumente und Verzeichnisse vorzulegen:

- Die Gemeinde Z*** wurde aufgefordert, ein Verzeichnis von Verarbeitungstätigkeiten iSv Art. 30 DSGVO vorzulegen.
 - Die Gemeinde Z*** wurde aufgefordert auszuführen, ob im Hinblick auf die eingangs erwähnte Datenverarbeitung eine Datenschutz-Folgenabschätzung iSv Art. 35 DSGVO durchgeführt wurde und falls nein, weshalb eine solche unterlassen wurde. Falls ja, war die entsprechende Datenschutz-Folgenabschätzung vorzulegen.
 - Die Gemeinde Z*** wurde aufgefordert darzulegen, auf welche konkrete Rechtsgrundlage eine derartige Verarbeitung personenbezogener Daten – insbesondere die Verarbeitung besonderer Kategorien personenbezogener Daten iSv Art. 9 DSGVO – gestützt wird.
 - Sofern eine derartige Verarbeitung personenbezogener Daten auf eine Einwilligung iSv Art. 4 Z 11 DSGVO gestützt wird, wurde die Gemeinde Z*** aufgefordert näher auszuführen, auf welche Weise und unter welchen Umständen eine solche Einwilligung eingeholt wird. Darüber hinaus wurde aufgetragen, der Datenschutzbehörde einen entsprechenden Auszug einer Einwilligungserklärung vorzulegen.
 - Sofern eine derartige Verarbeitung personenbezogener Daten auf eine Einwilligung iSv Art. 4 Z 11 DSGVO gestützt wird, wurde die Gemeinde Z*** auch aufgefordert auszuführen, inwiefern die verpflichtende Nutzung eines Handvenenscanners für Saisonkartenbesitzer mit dem Koppelungsverbot vereinbar ist.
 - Die Gemeinde Z*** wurde schließlich noch aufgefordert darzulegen, welche geeigneten technischen und organisatorischen Maßnahmen getroffen wurden, damit die Anforderungen der DSGVO erfüllt und die Rechte der betroffenen Personen geschützt werden (Art. 25 DSGVO) und insbesondere auch darzulegen, wie die Sicherheit der Verarbeitung (Art. 32 DSGVO) gewährleistet wird.
4. Mit Stellungnahme vom 15. Oktober 2019, ha. eingelangt am 18. Oktober 2019, legte die Gemeinde Z*** ein Konvolut an Dokumenten vor. Darunter befinden sich u.a. ein Verzeichnis der Verarbeitungstätigkeiten, ein Auszug einer Einwilligungserklärung, ein Infoblatt zum Handvenenscanner, eine tabellarische

Übersicht über technische und organisatorische Maßnahmen sowie zwei Auftragsverarbeiterverträge. Weiters nahm die Gemeinde Z*** wie folgt Stellung:

*Mit Schreiben der Datenschutzbehörde vom 07.08.2019. (eingelangt am 03.09.2019) wurde der Gemeinde Z*** mitgeteilt, dass ein amtswegiges Prüfverfahren gegen sie als Betreiberin des Seebades eingeleitet wurde.*

*Mit gleichem Schreiben wurde der Gemeinde Z*** die Möglichkeit eingeräumt, zu den angeführten Punkten schriftlich Stellung zu nehmen.*

*Innerhalb offener Frist erstattet die Gemeinde Z*** nachstehende*

Stellungnahme

und führt diese wie folgt aus:

Zu 1.:

*Eine Kopie des Verarbeitungsverzeichnisses gemäß Art. 30 DSGVO der Gemeinde Z*** wird in der Beilage übermittelt (Beilage I).*

Zu 2.:

Die biometrischen Daten werden anonymisiert und durch eine Einwegfunktion zu sogenannten Templates verarbeitet und verschlüsselt. Es ist nicht möglich, hieraus Rückschlüsse personenbezogener Daten, wie zB Name, Alter, Geschlecht, Gesundheitszustand oder ähnliches zu ziehen. Zusätzlich werden diese verschlüsselten Templates getrennt von tatsächlichen personenbezogenen Daten des Betroffenen so abgesichert gespeichert, dass aufgrund der Datenstrukturen kein Rückschluss auf den tatsächlichen Besitzer gezogen werden kann.

Da aufgrund der Verarbeitung weder ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht, war keine Notwendigkeit einer Datenschutzfolgeabschätzung nach Art. 35 DSGVO durchzuführen.

Zu 3.:

*Die betroffenen Personen haben der Verarbeitung der genannten personenbezogenen Daten für einen festgelegten Zweck ausdrücklich zugestimmt. Der Verarbeitungszweck ist dadurch eindeutig, dass nur eine Person Zutritt zum Seebad hat und eine Weitergabe dieses Eintrittes nicht möglich ist. Das Seebad wird als privatwirtschaftlicher Betrieb der Gemeinde Z*** geführt. Für den Zutritt in das Seebad sind Eintrittsgebühren festgelegt. Um eine Zutrittskontrolle zu gewährleisten und Missbrauch auszuschließen wurde die Installation eines einfachen Zutrittssystems installiert.*

Zu 4.:

*Die Verarbeitung personenbezogener Daten wird ausschließlich beim Bezug einer Saisonkarte persönlich im Seebad der Gemeinde Z*** durchgeführt.*

Die Einwilligung der betroffenen Personen erfolgt in diesem Fall eindeutig, da sie mit der Verarbeitung der betreffenden Daten einverstanden sind. Das Formular der Einverständniserklärung wird in der Beilage angeführt (Beilage 2).

Zu 5.:

Jeder Besucher im Seebad hat bei Nichteinwilligung der Verarbeitung der personenbezogenen Daten die Möglichkeit des Erwerbes einer Tageskarte. Der Grund für die Verarbeitung personenbezogener Daten besteht darin, einen Missbrauch der Saisonkarten durch Weitergabe dieser Karten zu verhindern.

Zu 6.:

*Eine Kopie des Maßnahmenkataloges (technisch organisatorische Maßnahmen) der Gemeinde Z*** wird in der Beilage übermittelt (Beilage 3).*

*Zusätzlich zur Stellungnahme zu den Punkten 1. bis 6. werden von der Gemeinde Z*** folgende Informationen bereitgestellt:*

- *Vertrag über eine Auftragsverarbeitung X*** GmbH (Beilage 4).*
- *Vertrag über eine Auftragsverarbeitung Y*** GmbH (Beilage 5).*
- *Informationen bezüglich Handvenenscanner Firma A*** (Beilage 6).*
- *Werkvertrag Datenschutzbeauftragter (Beilage 7).*

*Abschließend wird festgestellt, dass über zweitausend Erfassungen erfolgt sind. Von fünf Personen wurde eine Auskunft nach Art. 15 DSGVO begehrt und seitens der Gemeinde Z*** fristgerecht beantwortet.*

Beilagen:

Verarbeitungsverzeichnis

Einwilligungserklärung

Maßnahmenkatalog

Auftragsverarbeitervertrag x

Auftragsverarbeitervertrag y

Informationen Handvenenscan

Werkvertrag Datenschutzbeauftragter

B. Prüfgegenstand

Zu überprüfen ist, ob die durchgeführte Verarbeitung biometrischer Daten mittels Handvenenscanner durch die Gemeinde Z*** rechtmäßig erfolgt und somit der DSGVO entspricht.

C. Sachverhaltsfeststellungen

Die Gemeinde Z*** ist Betreiberin des Seebades Z***. Zum Zwecke der Zutrittskontrolle in das Seebad für Saisonkartenbesitzer wurde im Mai 2019 ein Handvenenscanner installiert. Die Investitionskosten lagen bei 50.000 Euro. Dabei erfolgt über den Abgleich des Venenmusters der Handinnenflächen eine biometrische Identitätsprüfung. Zur Aufnahme des Venenbildes arbeitet der Handvenensensor mit Infrarotlicht, welches von den roten Blutkörperchen in den Venen absorbiert wird. Dadurch wird die Venenstruktur für eine Infrarotkamera sichtbar gemacht und bildet so die Basis des biometrischen Musters.

Für den Erwerb einer Saisonkarte ist es Voraussetzung, das Venenmuster beider Handinnenflächen an der Kasse erfassen zu lassen und fortan bei jedem Zutritt zum Seebad den Handvenenscanner zu nutzen. Eine Alternative Zutrittsmöglichkeit ist für Saisonkartenbesitzer nicht mehr vorgesehen. Der Zutritt ohne Handvenenscan ist als Badegast nur noch mittels Erwerb einer Tageskarte möglich.

Der Preis für eine Tageskarte für Erwachsene betrug im Jahr 2019 4,50 Euro. Für eine Saisonkarte für Erwachsene wurden 50 Euro verrechnet.

Weiters ist man nur mittels Saisonkarte berechtigt die Zufahrtsschranken zu öffnen, um als zufahrtsberechtigter Mieter eines Bootsliegeplatzes zu den im Seebad befindlichen Bootsliegeplätzen zuzufahren. Ein Öffnen der Zufahrtsschranken unter Verwendung einer Tageskarte ist nicht möglich.

Bevor das Venenmuster im Zuge des Erwerbs einer Saisonkarte erstmals an der Kasse erfasst wird, müssen Badegäste folgende Einwilligungserklärung unterzeichnen:

***Einwilligung in die Erhebung, Verarbeitung und Speicherung von biometrischen Daten
im Sinne der Datenschutz Grundverordnung (EU)
2016/679***

*Die Gemeinde Z*** (im folgenden „Betreiber“ genannt) setzt zum
Zwecke der Verifikation/Identifikation von Betroffenen die biometrische Technologie
F***Secure™ in verschiedenen Ausprägungen ein.
Diese sind: Zutritt in das Seebad.*

Hierzu wird im Folgenden um die persönliche Zustimmung des Betroffenen gebeten:

Hiermit erkläre ich,

Vorname: Familienname:

Anschrift:

Geburtsjahr:

mein Einverständnis, dass meine biometrischen Informationen - konkret meine spezifischen Venenmuster der rechten und linken Handinnenflächen zum Zwecke der Verifikation/Identifikation an die derart ausgestatteten IT- und Zutrittssysteme des Betreibers zentral erfasst, verarbeitet und gespeichert werden. Jede weitere Nutzung sowie die Weitergabe dieser Daten ist dem Betreiber ausdrücklich untersagt.

Die biometrischen Daten werden anonymisiert und durch eine Einwegfunktion zu sogenannten Templates verarbeitet und verschlüsselt. Es ist nicht möglich, hieraus Rückschlüsse personenbezogene Daten wie z.B Name, Alter, Geschlecht, Gesundheitszustand oder ähnliches zu ziehen. Zusätzlich werden diese verschlüsselten Templates getrennt von tatsächlichen personenbezogenen Daten des Betroffenen abgesichert gespeichert, so dass aufgrund der Datenstrukturen kein Rückschluss auf den tatsächlichen Besitzer gezogen werden kann.

Mir ist bekannt, dass ich diese Einwilligung jederzeit widerrufen kann. Der Widerruf hat in Textform gegenüber dem Betreiber des Systems zu erfolgen.

Ort, Datum

Unterschrift

Beweiswürdigung: Die getroffenen Feststellungen beruhen auf der Stellungnahme der Gemeinde Z*** vom 15. Oktober 2019, ha. eingelangt am 18. Oktober 2019, sowie den damit übermittelten Beilagen. Weiters auf den verschiedenen Medienberichten (U*-Artikel vom 22.07.2019 https://www.u*.at/oesterreich/handvenenscanner-seebad-z***-5*739**4; P*-Artikel vom 17.07.2019 https://p*.at/chronik/seebad-wer-saisonkarte-will-muss-handvenen-registrieren/*2746*391; Q*-Artikel vom 18.07.2019 https://www.q*.at/story/*68439**4/handvenenscan/seebad-sorgt-fuer-aufregung; *TV-Sender ** vom 19.07.2019 https://*ort.at/stories/**4981*/; Bericht der „Die Grünen & Unabhängigen Z****“ - Redaktion vom 15. Mai 2019 https://.www.leben-z**.at/wp-content/uploads/sites/1*/201*/0*/ZumThema_Handvenenscanner_Seebad_29846**8.pdf; alle zuletzt abgefragt durch die Datenschutzbehörde am 12.12.2019). Die Feststellungen zu den Eintrittspreisen des Seebades Z*** ergeben sich aus den Angaben auf der Gemeinde-Webseite, https://www.z***at/feizeit/seebad (Abgefragt durch die Datenschutzbehörde am 12.12.2019).

D. In rechtlicher Hinsicht folgt daraus:

D.1. Zum amtswegigen Prüfverfahren

Die Datenschutzbehörde leitete auf Grundlage von Art. 58 Abs. 1 lit. b DSGVO ein amtswegiges Prüfverfahren („Datenschutzüberprüfung“) gegen die Gemeinde Z*** (in Folge: Betreiberin) ein, die das Seebad Z*** betreibt.

D.2. Zur datenschutzrechtlichen Rollenverteilung

Die Betreiberin ist für die von ihr durchgeführte biometrische Zutrittskontrolle mittels Handvenenscanner laut eigenen Angaben (Punkt 19 des vorgelegten Verarbeitungsverzeichnisses) als datenschutzrechtliche Verantwortliche gemäß Art. 4 Z 7 DSGVO zu qualifizieren. Auch scheint die Gemeinde Z*** am oben abgebildeten Formular für die Einwilligungserklärung auf, womit für Außenstehende der Eindruck vermittelt wird, dass die Gemeinde Z*** Verantwortliche ist. In der Stellungnahme der Gemeinde Z*** wird auf S. 2 zwar ausgeführt, dass das Seebad als privatwirtschaftlicher Betrieb der Gemeinde geführt wird; nähere Informationen und Anhaltspunkte dafür, dass dieser Betrieb auch als Verantwortlicher iSd DSGVO zu qualifizieren ist, sind im Verfahren aber nicht hervorgekommen.

Die Datenschutzbehörde kommt daher zum Schluss, dass die Gemeinde Z*** Verantwortliche gemäß Art. 4 Z 7 DSGVO für die Verarbeitung von Daten mittels Handvenenscanner ist.

D.3. Verarbeitung von biometrische Daten

Gemäß Art. 4 Z 14 DSGVO sind „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.

Gemäß Art. 4 Z 2 DSGVO versteht man unter „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Bilder von Handvenenmustern werden – wie festgestellt – mit einem speziellen technischen Verfahren (unter Nutzung von Infrarotlicht) gewonnen. Handvenenmuster zählen zu den physiologischen Merkmalen einer Person, lassen sich einer natürlichen Person eindeutig zuordnen und ermöglichen dadurch die eindeutige Identifizierung einer natürlichen Person. Handvenenmuster als biometrische Daten iSd Art. 4 Z 14 DSGVO sind daher zweifelsfrei auch personenbezogene Daten iSv Art. 4 Z 1 DSGVO. Für die Nutzung des Handvenenscanners zum Zwecke der Zutrittskontrolle werden die Handvenenmuster von betroffenen Personen erfasst, somit iSv Art. 4 Z 2 DSGVO verarbeitet.

Grundsätzlich gilt gemäß Art. 9 Abs. 1 DSGVO die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person als Verarbeitung besonderer Kategorien personenbezogener Daten („sensible Daten“). Die Verarbeitung dieser Daten ist untersagt, sofern die Verarbeitung nicht auf einen, in Abs. 2 taxativ aufgezählten Eingriffstatbestand gestützt werden kann. Eine Ausnahme hiervon liegt nach Art. 9 Abs. 2 lit a. DSGVO vor, wenn die betroffene Person in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt hat.

D.4. Grundsätze für die Verarbeitung personenbezogener Daten

Artikel 5 DSGVO lautet:

Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

- a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
 - b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
 - c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
 - d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
 - e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);
 - f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);
- (2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Der EuGH hält in seiner Rechtsprechung fest, dass die Verarbeitung personenbezogener Daten sich auf zumindest einen Tatbestand gemäß Art. 7 der Richtlinie 95/46/EG (nunmehr: Art. 6 DSGVO) stützen können und den in Art. 6 dieser Richtlinie (nunmehr: Art. 5 DSGVO) dargelegten Grundsätzen entsprechen muss (Urteil vom 11. Dezember 2019, C-708/18, Rz 36).

Zu diesen Grundsätzen zählt auch der Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO.

D.5. Allgemeines zum Grundsatz der Datenminimierung

Beim Grundsatz der Datenminimierung handelt es sich um die Reduktion der Verarbeitung personenbezogener Daten auf das Unverzichtbare. Die Datenminimierung stellt sicher, dass die Verarbeitung durch den festgelegten Verarbeitungszweck qualitativ und quantitativ begrenzt wird.

Die Datenminimierung besagt, dass eine Datenverarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss. Bei der Angemessenheit handelt es sich um die Verhältnismäßigkeitsprüfung im engeren Sinne. Die Erheblichkeit bezeichnet die Geeignetheit im Sinne der grundrechtlichen Verhältnismäßigkeitsdogmatik, also ob eine durchgeführte Datenverarbeitung überhaupt zur Zweckerreichung förderlich ist. Mit der Beschränkung auf das notwendige Maß wird schließlich noch einmal klargestellt, dass die Daten nicht über die Zwecke hinausgehen dürften. Diese Anforderung wird regelmäßig von der Zweckangemessenheit und der Erheblichkeit konsumiert [vgl. anstelle vieler *Hötzendorfer/Tschohl/Kastelitz in Knyrim, DatKomm Art 5 DSGVO Rz 34 ff (Stand 1.10.2018, rdb.at)*].

D.6. Allgemeines zur datenschutzrechtlichen Einwilligung und zum Koppelungsverbot

Laut eigenen Angaben stützt die Betreiberin die Verarbeitung der personenbezogenen Daten betroffener Personen zum Zweck der Zutrittskontrolle im Seebad Z*** nur auf die Rechtsgrundlage der Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO.

Gemäß Art. 4 Z 11 DSGVO versteht man unter „Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Gemäß Art. 7 DSGVO sowie unter Berücksichtigung von Art. 4 Z 11 und ErwGr. 43 DSGVO muss eine Einwilligung freiwillig erfolgen und darf nicht an die Erfüllung eines Vertrages gekoppelt sein, obwohl diese Einwilligung zur Erfüllung dieses Vertrags nicht erforderlich ist. Unfreiwillig ist eine Einwilligung dann, wenn bei Nichtabgabe der Einwilligung ein Nachteil zu erwarten ist (vgl. dazu den Bescheid der Datenschutzbehörde vom 16. April 2019, GZ DSB-D213.679/0003-DSB/2018).

Die ehemalige Art. 29-Datenschutzgruppe hat sich in ihren Leitlinien mit dem Begriff der „Einwilligung“ beschäftigt und eine Analyse des Begriffes vorgenommen. Dabei hat sie sich auch mit der die Freiwilligkeit verhindernden Nachteilen auseinandergesetzt und ist zu dem Ergebnis gekommen, dass ein solcher Nachteil dann gegeben ist, wenn das Risiko einer Täuschung, Einschüchterung, Nötigung oder beträchtlicher negativer Folgen besteht. Der Verantwortliche muss nachweisen, dass es möglich ist, die Einwilligung zu verweigern oder zu widerrufen, ohne Nachteile zu erleiden. Ein Verantwortlicher muss beispielsweise nachweisen, dass das Verweigern oder Widerrufen der Einwilligung nicht

zu Kosten für die betroffene Person führt und folglich zu einem eindeutigen Nachteil. Ferner sollte der Verantwortliche nachweisen, dass die betroffene Person eine echte oder freie Wahl hatte, ob sie einwilligt oder nicht (vgl. Art. 29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259, rev. 01 S. 12; vgl. auch ErwGr. 42 DSGVO; vgl. weiters den Bescheid der Datenschutzbehörde vom 30. November 2018, GZ DSB-D122.931/0003-DSB/2018).

Das Element „frei“ impliziert, dass die betroffenen Personen eine echte Wahl und die Kontrolle haben. Im Allgemeinen schreibt die DSGVO vor, dass eine Einwilligung nicht gültig ist, wenn die betroffene Person keine wirkliche Wahl hat, sich zur Einwilligung gedrängt fühlt oder negative Auswirkungen erdulden muss, wenn sie nicht einwilligt. Wenn die Einwilligung ein nicht verhandelbarer Teil von Geschäftsbedingungen ist, wird angenommen, dass die Einwilligung nicht freiwillig erteilt wurde. Art. 7 Abs. 4 der DSGVO weist unter anderem darauf hin, dass eine Situation, in der die Einwilligung mit der Annahme von Vertragsbedingungen „gebündelt“ wird oder die Erfüllung eines Vertrags oder die Erbringung einer Dienstleistung mit dem Ersuchen um Einwilligung in eine Verarbeitung von personenbezogenen Daten „verknüpft“ wird, die für die Erfüllung des Vertrags nicht erforderlich sind, als in höchstem Maße unerwünscht angesehen wird. Wird die Einwilligung in einer solchen Situation erteilt, gilt sie als nicht freiwillig erteilt (vgl. ErwGr. 43 DSGVO).

Wenn der Verantwortliche die Erfüllung eines Vertrags mit dem Ersuchen um Einwilligung verknüpft, geht eine betroffene Person, die dem Verantwortlichen ihre personenbezogenen Daten nicht für die Verarbeitung zur Verfügung stellen möchte, folglich das Risiko ein, dass ihr Leistungen verwehrt werden, um die sie ersucht hat (vgl. dazu nochmals den Bescheid vom 16. April 2019).

Bei der Koppelung der Einwilligung zu einer Verarbeitung vertragsunabhängiger personenbezogener Daten mit einem Vertragsschluss ist grundsätzlich davon auszugehen, dass die Erteilung der Einwilligung nicht freiwillig erfolgt, wenn nicht im Einzelfall besondere Umstände für eine Freiwilligkeit der datenschutzrechtlichen Einwilligung sprechen (siehe dazu das Urteil des OGH vom 31. August 2018, GZ 6 Ob 140/18h mwN).

Nach der Judikatur der Datenschutzbehörde ist weiters zu berücksichtigen, dass eine freiwillige Einwilligung dann vorliegen kann, wenn ein bestimmter Verarbeitungsvorgang auch zum erkennbaren Vorteil der betroffenen Person gereicht (vgl. anstelle vieler den Bescheid vom 8. März 2006, GZ K178.209/0006-DSK/2006; vgl. dazu auch *Kotschy* in *Brodil* (Hrsg), Datenschutz im Arbeitsrecht [2010] 3).

D.7. In der Sache

Rechtmäßigkeit der Datenverarbeitung

Da gegenständlich besondere Kategorien personenbezogener Daten verarbeitet werden, richtet sich die Rechtmäßigkeit der Verarbeitung ausschließlich nach Art. 9 Abs. 2 DSGVO.

Eine – rechtskonforme – Einwilligung kommt als Rechtsgrundlage nach Art. 9 Abs. 2 lit. a DSGVO in Betracht.

In diesem Zusammenhang stellt sich die Frage, ob die mittels Formular „*Einwilligung in die Erhebung, Verarbeitung und Speicherung von biometrischen Daten im Sinne der Datenschutz Grundverordnung (EU) 2016/679*“ erhobene Einwilligung in die Verarbeitung personenbezogener Daten der betroffenen Personen den in der DSGVO normierten Anforderungen entspricht.

Im konkreten Fall sind Saisonkartenbesitzer – wie festgestellt – zur Nutzung des Handvenenscanners verpflichtet. Der Erwerb einer Saisonkarte setzt voraus, dass eine Einwilligungserklärung unterzeichnet wird, andernfalls ist nur der Erwerb einer Tageskarte möglich. Eine Alternative Zutrittsmöglichkeit (ohne Nutzung des Handvenenscanners) gibt es für Saisonkartenbesitzer nicht. Gibt eine betroffene Person keine solche Einwilligung ab, so bestehen die Konsequenz und der eindeutige Nachteil darin, keine Saisonkarte für das Seebad erwerben zu können. Eine echte Wahl und Kontrolle haben betroffene Personen daher nicht.

Mit Verweis auf die allgemeinen Ausführungen zum Koppelungsverbot (vgl. D.6.) ist es offensichtlich, dass die prüfgegenständliche Einwilligung nicht „freiwillig“ erfolgt. Die Möglichkeit eine Tageskarte ohne Einsatz des Handvenenscanners zu erwerben, stellt keine rechtmäßige Alternativoption dar, weil der betroffenen Person dadurch zweifellos erhebliche Mehrkosten entstehen würden, wie bereits die Argumentation der Verantwortlichen zeigt, gerade bei Saisonkartenbeziehern das gegenständliche biometrische Prüfsystem einsetzen zu wollen, um Missbrauch zu vermeiden. Abgesehen davon ist die Benützung des Bootsliegendeplatzes nur mit einer Saisonkarte – und nicht mit einer Tageskarte – möglich.

In diesem Zusammenhang ist auch zu prüfen, welche Verarbeitungen für die Vertragserfüllung (Erbringung einer Dienstleistung) überhaupt erforderlich sind. Das Koppelungsverbot umfasst nämlich nur Einwilligungen, die für den Vertragszweck nicht erforderlich sind. Die „Erforderlichkeit“ ist dabei am Vertragszweck zu messen. Kernzweck

des Erwerbs einer Saisonkarte ist die saisonale Nutzung des Seebades und der dazugehörenden Infrastruktur.

Aus Sicht der Datenschutzbehörde ist die Einwilligung in die Datenverarbeitung durch einen Handvenenscanner zur Nutzung der Infrastruktur nicht erforderlich. Erforderlich ist nur, dass eine Zutrittskontrolle zum Seebad besteht, um unberechtigte Personen von einer Nutzung abzuhalten.

Im Ergebnis ist daher festzuhalten, dass Koppelungsverbot verletzt und die Einwilligung in die prüfgegenständliche Datenverarbeitung unzulässig ist.

Mangels zulässiger Einwilligung der Betroffenen in die Verarbeitung der biometrischen (und somit besonderen Kategorie von) Daten und mangels Anwendbarkeit anderer Ausnahmen iSv Art. 9 Abs. 2 DSGVO fehlt es prüfgegenständlich an einer Rechtsgrundlage für die Rechtmäßigkeit der Verarbeitung.

Die gegenständliche Datenverarbeitung erweist sich daher schon aus diesem Grund als unrechtmäßig und folglich als nicht der DSGVO entsprechend.

Verhältnismäßigkeit / Datenminimierung

Selbst wenn man von einer zulässigen Einwilligung (oder einer anderen Rechtsgrundlage) ausginge, wäre die gegenständliche Datenverarbeitung dennoch unverhältnismäßig und entspricht folglich nicht dem Grundsatz nach Art. 5 Abs. 1 lit. c DSGVO.

Es dürfen personenbezogene Daten nur dann verarbeitet werden, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere, gelindere Mittel erreicht werden kann (vgl. ErwGr. 39 DSGVO sowie das bereits zitierte Urteil des EuGH vom 11. Dezember 2019, Rz 47 f).

Auch die ehemalige Artikel-29-Datenschutzgruppe hat in einer Stellungnahme auf die Risiken von biometrischen Technologien hingewiesen und die Verhältnismäßigkeitsprüfung hervorgehoben (vgl. Artikel-29-Datenschutzgruppe, Stellungnahme 3/2012, WP193):

„Bei der Nutzung biometrischer Daten stellt sich die Frage der Verhältnismäßigkeit der in den einzelnen Kategorien verarbeiteten Daten vor dem Hintergrund des Zwecks der jeweiligen Verarbeitung. Da biometrische Daten nur dann verwendet werden können, wenn sie angemessen und relevant sind und nicht in übermäßigem Umfang erfasst werden, müssen die Notwendigkeit und die Verhältnismäßigkeit der Verarbeitung streng geprüft werden. Außerdem muss geprüft werden, ob der beabsichtigte Zweck nicht auch unter stärkerer Respektierung der Privatsphäre erreicht werden könnte.

Bei der Analyse der Verhältnismäßigkeit eines vorgeschlagenen biometrischen Systems ist vorab zu prüfen, ob das System erforderlich ist, um den ermittelten Zweck zu erfüllen, d. h., ob dieses System für die Erfüllung dieses Zwecks tatsächlich wesentlich ist oder bloß die bequemste oder kostengünstigste Lösung darstellt. Ein zweiter Faktor ist, ob das System zur Erfüllung des vorgesehenen Zwecks wahrscheinlich effizient ist. In diesem Zusammenhang sind die spezifischen Merkmale der vorgesehenen biometrischen Technologie zu berücksichtigen. Ein dritter Aspekt besteht in der Abwägung, ob die zu erwartende Beeinträchtigung der Privatsphäre im Verhältnis zum erwarteten Nutzen steht. Wenn dieser Nutzen verhältnismäßig gering ist und beispielsweise nur in erhöhter Bequemlichkeit oder in einer geringen Kosteneinsparung besteht, ist die Beeinträchtigung der Privatsphäre nicht als verhältnismäßig zu bewerten. Der vierte Aspekt für die Bewertung der Angemessenheit eines biometrischen Systems besteht in der Prüfung, ob das gewünschte Ergebnis nicht auch mit Mitteln erreicht werden könnte, welche die Privatsphäre weniger beeinträchtigen würden.“

Der Zweck der gegenständlichen Datenverarbeitung liegt in der Zutrittskontrolle zum Seebad Z***.

Die Betreiberin gibt selbst an, dass der Einsatz des Handvenenscanners weiters dazu diene, eine Weitergabe der Saisonkarten zu unterbinden.

Der erwartete Nutzen steht jedoch in keinem Verhältnis zur durchgeführten biometrischen Datenverarbeitung:

Biometrische Daten sind von Natur aus höchstpersönlich, einzigartig und nicht abänderbar und daher ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel. Sie verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken bestehen (vgl. dazu auch ErwGr. 51 DSGVO). Die Frage der Verhältnismäßigkeit ist mit Blick auf den von der Betreiberin verfolgten Zweck daher streng zu prüfen.

Die verfahrensgegenständliche Verarbeitung wäre nur dann zulässig, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch anderen Mittel erreicht werden kann.

Das ist gegenständlich jedoch nicht der Fall.

Als gelindere Alternative zur Zugangskontrolle mit Handvenenscanner könnten nicht übertragbare Saisonkarten mit einem Foto des Karteninhabers ausgegeben werden, die entweder beim Zugang von Bediensteten kontrolliert und abgeglichen werden (so wie dies auch bei den Wiener Bädern üblich ist, vgl.

<https://www.wien.gv.at/freizeit/baeder/eintrittspreise/monatskarten.html>, abgerufen am 06. Dezember 2019) oder die stichprobenartig im Seebad überprüft werden (so wie bei einer Fahrkartenkontrolle in öffentlichen Verkehrsmitteln). Eine solche Vorgehensweise

wäre auch mit Blick auf die Investitionskosten von 50.000 Euro und laufenden Wartungskosten des Handvenenscanners zumutbar.

Neben dem Grundsatz der Rechtmäßigkeit der Verarbeitung ist daher auch der Grundsatz der Datenminimierung verletzt.

Die Datenschutzbehörde übersieht auch nicht, dass von der Betreiberin umfassende technische und organisatorische Maßnahmen getroffen wurden, jedoch ist der Aspekt der Sicherheit der Verarbeitung für die Verhältnismäßigkeitsprüfung iSd Datenminimierungsgrundsatzes selbst unerheblich. Es ist lediglich zu prüfen, ob es gelindere Mittel zur Zweckerreichung gibt, die einen weniger starken Eingriff für betroffene Personen bedeuten. Da es – wie dargelegt – solche gelinderen Mittel gibt, ist im konkreten Fall der Grundsatz der Datenminimierung verletzt und ist auch aus diesem Grund von der Unzulässigkeit der prüfgegenständlichen Datenverarbeitung auszugehen. Die Sicherheit der Verarbeitung wäre allenfalls im Rahmen des Grundsatzes der Integrität und Vertraulichkeit zu überprüfen (Art. 5 Abs. 1 lit. f DSGVO), wonach personenbezogene Daten in einer Weise verarbeitet werden müssen, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen. Weiters könnten Sicherheitsmaßnahmen iSv Schutzmaßnahmen zur Verhinderung bzw. Abmilderung unangemessener Folgen für Betroffene, die durch die Betreiberin implementiert wurden, im Rahmen einer Interessenabwägung iSd Art. 6 Abs. 1 lit. f DSGVO berücksichtigt werden (vgl. zu den Schlüsselfaktoren, die bei einer Interessenabwägung zu berücksichtigen sind, Art. 29-Datenschutzgruppe, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, 844/14/EN, S. 43). Zu einer solchen Interessenabwägung kommt es bei der Prüfung, ob es gelindere Mittel zur Zweckerreichung iSd Grundsatzes der Datenminimierung gibt, jedoch nicht. Auf die getroffenen technischen und organisatorischen Maßnahmen war an dieser Stelle daher auch nicht weiter einzugehen.

D.8. Ergebnis

Da die prüfgegenständliche Datenverarbeitung mangels zulässiger Rechtsgrundlage bereits unrechtmäßig erfolgt, andererseits aber auch unverhältnismäßig (Art. 5 Abs. 1 lit. c DSGVO) ist, war der Betreiberin ein entsprechender Leistungsauftrag zu erteilen und die Datenverarbeitung zu untersagen sowie die Löschung der vorhandenen personenbezogenen Daten aufzutragen.

Der Leistungsauftrag gründet sich auf Art. 58 Abs. 2 lit. f und g DSGVO.

Es war daher spruchgemäß zu entscheiden.