**Ergänzung zu Ihrer Datenschutzerklärung – biometrisches Zugangssystem**

Diese Informationen dienen als Hinweis für eine mögliche Ergänzung der allgemeinen Datenschutzerklärung Ihres Fitnessstudios gemäß Art. 13 DSGVO beim Einsatz des Zugangssystems von der Facetronic UG. Verantwortlich für die Datenverarbeitung ist gemäß Art. 4 Nr. 7 DSGVO das jeweilige Fitnessstudio, bei dem das Mitglied einen Vertrag abgeschlossen hat. Da der Einsatz der Software individuell erfolgt, kann die Facetronic UG keine konkreten Vorgaben machen, sondern nur Hinweise geben. Bitte beachten Sie auch den Arbeitnehmerdatenschutz.

## I. Allgemeine Hinweise

- Identifikationsmethoden

  Das Facetronic-System bietet verschiedenen technische Zugangsmöglichkeiten für den Studiozugang an:

| Methode | Technische Umsetzung | Verarbeitete Datenkategorien | Rechtsgrundlage | Biometrischer Abgleich? |
|---|---|---|---|---|
| **RFID-Medium (Karte/Chip)** | Vorhalten des Mediums an den Leser. Übertragung einer ID-Nummer. | Allgemeine Identifikationsnummer (UID), Zeitstempel. | Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung) | **Nein** |
| **QR-Code** | Optisches Scannen eines digitalen Sicherheitsschlüssels (Token). | Verschlüsselter Zeichencode, Zeitstempel. | Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung) | **Nein** |
| **Gesichtserkennung** | Identifikation ausschließlich durch automatischen Abgleich der Gesichtszüge. | Biometrische Parameter (mathematischer Zahlencode), Zeitstempel. | Art. 9 Abs. 2 lit. a i.V.m. Art. 6 Abs. 1 lit. a DSGVO (Einwilligung) | **Ja** |
| **Kombinations-Option (Karte/ QR-Code + Gesichtserkennung)** | Vorhalten der Karte/ optisches Scannen eines Tokens **plus** automatisierte Identitätsprüfung durch die Kamera. | UID/ verschlüsselter Zahlencode, Zeitstempel **und** biometrische Parameter (Zahlencode). | Art. 9 Abs. 2 lit. a i.V.m. Art. 6 Abs. 1 lit. a DSGVO (Einwilligung) | **Ja** |

- Bei der Identifikationsmethode „Gesichtserkennung“ nutzt das System zur Identitätsprüfung biometrische Algorithmen zur Merkmalsextraktion und zum Musterabgleich.
- **Abgrenzung von Videoüberwachung und Biometrie:** Der Einsatz des biometrischen Scanners erfolgt ausschließlich zum Zweck der Identitätsverifikation und Zutrittskontrolle. Dieser Zweck ist rechtlich strikt von einer allgemeinen Videoüberwachung (CCTV) zur Wahrung des Hausrechts oder zum Eigentumsschutz zu trennen.
    - **Zweckbindung:** Eine Rechtsgrundlage für eine Videoüberwachung legitimiert nicht die biometrische Verarbeitung von Daten. Es ist eine separate Einwilligung gemäß Art. 6 Abs. 1 lit. a i.V.m. Art. 9 Abs. 2 lit. a DSGVO erforderlich.
    - **Betriebsmodus „Dauerhaft“:** Die Aktivierung der Option ‚Dauerhaft‘ darf aus datenschutzrechtlichen Gründen innerhalb der EU und EWR-Staaten nicht erfolgen. Es

drohen hohe Bußgelder. Bei einem Einsatz außerhalb dieser Staaten muss der Einsatz jeweils mit der nationalen Datenschutzbehörde abgestimmt werden.
    - **Schutz Unbeteiligter:** Der Scanner ist so zu positionieren, dass Passanten, Besucher ohne Einwilligung oder Personen in öffentlich zugänglichen Bereichen nicht vom Erfassungsradius erfasst werden. Eine biometrische ‚Vorab-Erfassung' unbeteiligter Dritter ist unzulässig.
    - **Hinweis auf Scanner:** Sie müssen auf den Einsatz des Scanners im Rahmen des biometriechen Gesichts-Scans mittels Aushangs deutlich am IDA-Gerät hinweisen. Einen Mustervorschlag für einen solchen Aushang finden Sie unter **Anlage 1**.
- **Gewährleistung der Freiwilligkeit:** Das System sieht eine echte Freiwilligkeit der Nutzung durch Ihre Mitglieder vor. Jedes Mitglied hat die Option, eine Zugangsmöglichkeit ohne Nutzung von Bild- bzw. biometrischen Daten zu wählen (z. B. via RFID-Chip oder QR-Code).
    - **Mitarbeiterzugang:** Auf diesem Weg müssen auch Mitarbeitende die Möglichkeit eines nicht vom System biometrisch erfassten Zugangs haben.

## II. Datenschutzerklärung

Für einen datenschutzkonformen Einsatz des Systems, müssen Sie als verantwortlicher Studiobetreiber im Sinne von Art. 4 Nr. 7 DSGVO Ihre Mitglieder über den Einsatz des biometrischen Zugangssystem mittels einer Datenschutzerklärung informieren. Bitte beachten Sie hierbei, dass die Datenschutzerklärung explizit auch für den biometriechen Systemeinsatz erfolgen muss. Die Datenschutzerklärung Ihres Studios muss daher durch die Datenschutzerklärung zum biometriechen Systemeinsatz ergänzt werden.

Im Folgenden geben wir Ihnen die notwendigen Informationen hinsichtlich der Ergänzung ihrer bestehenden Datenschutzerklärung um den Einsatz des biometriechen Zugangssystems.

**[Unverbindlicher Formulierungsvorschlag für die Ergänzung Ihrer Datenschutzerklärung hinsichtlich der Datenverarbeitung durch den Einsatz des biometrische Zugangssystems]**

**[…]**

**Datenschutzhinweise zum eingesetzten biometrischen Zugangssystem in unserem Studio**

Wir nutzen in unserem Studio ein biometrisches Zugangssystem.

**1.) Technische Zugangsmöglichkeiten/ Prozessbeschreibung**

**a.) Übersicht Zugangsmöglichkeiten zum Studio**

| Methode | Funktionsweise | Datennutzung | Rechtsgrundlage | Biometrie |
|---|---|---|---|---|
| **Klassisch: Karte / Chip** | Identifikation durch Vorhalten Ihres RFID-Mediums am Lesegerät. | Übermittlung einer anonymen ID-Nummer und des Zeitstempels. | Vertragserfüllung (Art. 6 DSGVO) | Nein |
| **Digital:**<br>**QR-Code** | Optisches Einlesen eines Sicherheitsschlüssels (Token). | Erfassung eines verschlüsselten digitalen Codes und des Zeitstempels. | Vertragserfüllung (Art. 6 DSGVO) | Nein |

| | | | | |
|---|---|---|---|---|
| **Komfort:**<br><br>**Gesichtserkennung** | Identifikation durch Abgleich mit einem verschlüsselten mathematischen Datensatz (Template). | Nutzung eines abstrakten Zahlencodes ohne dauerhafte Bildspeicherung. | Freiwillige Einwilligung (Art. 9 & 6 DSGVO) | Ja |
| **Sicherheit Plus: Zwei-Faktor-Authentifizierung (2FA)** | Verknüpfung von Karte oder QR-Code mit einer zusätzlichen Identitätsprüfung per Template-Abgleich zur Verifizierung der Nutzer-ID | Abgleich der Medien-ID mit dem verschlüsselten mathematischen Datensatz. | Freiwillige Einwilligung (Art. 9 & 6 DSGVO) | Ja |

**Erläuterungen zu Ihrem Schutz und Ihrer Wahlfreiheit**

- Abstrakte Datensicherheit: Bei den biometrisch gestützten Verfahren generiert das System aus Gesichtsmerkmalen ein mathematisches Modell (Template). Eine Rekonstruktion Ihres Lichtbildes aus diesem abstrakte Zahlencode ist technisch nicht möglich.

  Zur Veranschaulichung: Sie können sich diesen Vorgang wie ein mehrgängiges Menü vorstellen, das in einem Mixer fein püriert wurde. Zwar sind die chemischen Grundbestandteile theoretisch noch vorhanden, aber das ursprüngliche, optische Erscheinungsbild des Menüs lässt sich aus der Mixtur niemals wiederherstellen. Genauso verhält es sich mit Ihrem Template: Es ist eine digitale „Zutatenliste“, aus der kein Gesicht mehr entstehen kann.

- Die erhobenen Bilddaten sowie die daraus generierten biometrischen Templates werden ausschließlich zur Identitätsverifikation im Rahmen der Zutrittskontrolle verwendet. Eine Nutzung der Daten zur Weiterentwicklung, Optimierung oder zum Training von Algorithmen der künstlichen Intelligenz (KI) ist ausdrücklich ausgeschlossen.

- Wahrung der Privatsphäre: Das während des Zutrittsvorgangs kurzzeitig erfasste Bildmaterial wird ausschließlich im Arbeitsspeicher für den Sekundenbruchteil des Abgleichs verarbeitet und unmittelbar nach der Identifikation gelöscht.

- Freiwilligkeit als Prinzip: Die Nutzung biometrisch gestützten Verfahren ist absolut freiwillig. Ihnen stehen mit der Karte oder dem QR-Code jederzeit gleichwertige Identifikationswege zur Verfügung, die gänzlich ohne diese Technologie auskommen.

- Schutz vor Identitätsmissbrauch: Die Kombi-Option (Zwei-Faktor-Authentifizierung) schützt Sie effektiv vor den Folgen eines Kartenverlusts, da Ihr Zugang nicht durch unbefugte Dritte genutzt werden kann.

**b.) Jeweilige Prozessbeschreibung**

**(1) Identifikation über physische oder digitale Medien (RFID / QR-Code):**

Das System liest die anonyme ID-Nummer der Karte des Nutzers, den digitalen Code (Token) oder den QR-Code aus und gleicht diesen mit dem Mitgliedsstatus ab. In dieser Einstellung findet keine biometrische Analyse statt.

**(2) Gesichtserkennung (Biometrische Identitätsprüfung):**

Sofern die biometrische Option durch das Mitglied gewählt wurde, erfolgt die Verarbeitung in zwei Phasen – Onboarding und Authentifizierung:

**Registrierung (Onboarding):** Ihr biometrisches Profil (Referenz-Template) wird wahlweise direkt am Facetronic IDA-Gerät im Studio oder durch einen Foto-Upload in Ihrem Mitgliederprofil erstellt. Eine KI-basierte Software analysiert dabei die biometrischen Merkmale Ihres Gesichts und wandelt diese in einen anonymisierten, mathematischen Zahlenwert (Hash) um. Das System prüft mittels KI-basierter „Liveness Detection" (Lebenderkennung), ob eine echte Person vor der Kamera steht, um Missbrauch durch Fotos zu verhindern. Der mathematische Zahlenwert (Hash) wird lokal auf dem Lesegerät und verschlüsselt in der Magicline-Cloud gespeichert, um das Check-in an allen Terminals zu ermöglichen. Eine Rekonstruktion Ihres Bildes aus dem Zahlenwert ist nicht möglich. Ihr Originalfoto wird nach der Erstellung des Zahlenwertes für den biometrischen Abgleich nicht mehr benötigt. Sofern Sie ein Profilbild hochgeladen haben, speichern wir dieses lediglich zur optischen Identifikation in Ihrem Mitgliedskonto; für den technischen Check-in wird ausschließlich anonymisierte Zahlenwert (Hash) genutzt.

**Biometrische Identifikation:** Beim Check-in erfasst das Facetronic IDA-Gerät Ihr Gesicht in Echtzeit und wandelt es mittels KI-Technologie in einen temporären Zahlenwert (Hash) um. Die im IDA-Gerät integrierte Edge-KI gleicht den temporären Hash mit Ihrem im Onboarding hinterlegten Referenz-Template ab (1:N - Abgleich). Zur Betrugsprävention prüft das System mittels KI-basierter Lebenderkennung (Liveness Detection), ob eine echte Person vor der Kamera steht. Nach erfolgreicher Identifizierung meldet das IDA-Gerät Ihre Mitglieds-ID an die Magicline-Software. Diese prüft in Echtzeit Ihren Vertragsstatus und sendet bei vorliegender Berechtigung den Befehl zur Türöffnung an das IDA-Gerät zurück. Eine Rekonstruktion Ihres Gesichts aus den mathematischen Zahlenwerten (Hash) ist nicht möglich. Die KI lernt nicht aus Ihren Daten und erstellt keine Verhaltensprofile.

Die Nutzung des biometriechen Verfahrens ist freiwillig und erfolgt nur auf Basis Ihrer ausdrücklichen Einwilligung (Art. 9 Abs. 2 lit. a, Art. 6 Abs. 1 lit. a DSGVO), die Sie jederzeit widerrufen können.

**(3) biometrischen Verifikation (2-Faktor-Abgleich):**

Das System ermöglicht die Verknüpfung eines Identifikationsmediums (gemäß Ziff. 1) mit einer zusätzlichen biometrischen Prüfung (gemäß Ziff. 2), um eine missbräuchliche Nutzung von Karten oder QR-Codes durch unbefugte Dritte auszuschließen.

Sie erfassen Ihr RFID-Medium (Chip) oder Ihren QR-Code am Facetronic IDA-Gerät. Erst dann wird die Kamera für einen Sekundenbruchteil aktiviert. Das Gerät wandelt Ihr Gesichts-Bild mittels KI-basierter Technologie (Edge-KI) in einen temporären Zahlenwert (temporären Hash) um. Anschließend vergleicht die Edge-KI des IDA-Geräts diesen temporären Hash mit dem anonymisierten Referenz-Template Ihres Profils (1:1 Abgleich). Eine integrierte KI-basierte Lebenderkennung verhindert dabei Betrugsversuche durch Fotos. Der temporäre Wert wird nach dem Vergleich sofort wieder verworfen. Nach erfolgreicher Identifizierung meldet das IDA-Gerät Ihre Mitglieds-ID an die Magicline-Software. Diese prüft in Echtzeit Ihren Vertragsstatus und sendet bei vorliegender Berechtigung den Befehl zur Türöffnung an das IDA-Gerät zurück. Eine Rekonstruktion Ihres Gesichts aus den mathematischen Zahlenwerten (Hash) ist nicht möglich. Die KI lernt nicht aus Ihren Daten und erstellt keine Verhaltensprofile.

Die Nutzung des biometriechen Verfahrens ist freiwillig und erfolgt nur auf Basis Ihrer ausdrücklichen Einwilligung (Art. 9 Abs. 2 lit. a, Art. 6 Abs. 1 lit. a DSGVO), die Sie jederzeit widerrufen können.

## 2.) Zwecke und Rechtsgrundlage der Datenverarbeitung

Die Verarbeitung Ihrer Daten erfolgt zum Zweck der Zutrittskontrolle und der Sicherstellung der vertraglich vereinbarten Studionutzung. Die Rechtsgrundlagen hierfür sind:

- **Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung):** Für die Verarbeitung allgemeiner personenbezogener Daten (z. B. Name, Mitgliedsnummer, Zeitpunkt des Zutritts), die zur Durchführung des Mitgliedschaftsvertrages und zur Identifikation Ihrer Person erforderlich sind.
- **Art. 9 Abs. 2 lit. a i.V.m. Art. 6 Abs. 1 lit. a DSGVO (Einwilligung):** Für die Verarbeitung besonderer Kategorien personenbezogener Daten, insbesondere biometrischer Merkmale (z. B. Gesichtsbilder und daraus abgeleitete Identifikationsparameter). Diese Verarbeitung erfolgt ausschließlich auf Grundlage Ihrer ausdrücklichen Einwilligung.

- **Hinweis zur biometrischen Verifikation (2-Faktor-Abgleich):** Sofern Sie die optionale Verknüpfung von Karte/QR-Code mit Gesichtserkennung nutzen, erfolgt die Verarbeitung im Wege eines Zwei-Faktor-Abgleichs (Verifikation). Hierbei werden zwei Rechtsgrundlagen kombiniert:

  **Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung):** Für das Auslesen des physischen Mediums (RFID/QR), um Ihren Datensatz im System aufzurufen.

  **Art. 9 Abs. 2 lit. a i.V.m. Art. 6 Abs. 1 lit. a DSGVO (Einwilligung):** Für den anschließenden automatisierten Abgleich Ihres Live-Gesichtsbildes mit dem zum Medium hinterlegten biometrischen Template.

  Dieser Abgleich dient ausschließlich der Vermeidung von Kartenmissbrauch (Unterbindung von Chip-Sharing) und stellt sicher, dass nur das rechtmäßige Mitglied Zutritt erhält. Ein Abgleich gegen die gesamte Mitgliederdatenbank (Identifikation) findet in diesem Modus nicht statt.

  Details zur Freiwilligkeit und Ihrem Widerrufsrecht finden Sie unter 9.).

## 3.) Kategorien der verarbeiteten Daten und Verarbeitungszwecke

| Datenkategorie | Verarbeitete Daten | Zweck der Verarbeitung |
|---|---|---|
| **Allgemeine Stammdaten** | Vorname, Nachname, Mitgliedsnummer. | Identifikation Ihrer Person und Verwaltung Ihres Mitgliedsvertrages. |
| **Zutrittsprotokolle** | Zeitpunkt, Ort (Studio-ID) und Status (Erfolg/Fehler) des Zutritts. | Dokumentation der Studionutzung sowie statistische Auswertung der Studioauslastung zur bedarfsgerechten Optimierung unseres Serviceangebots (z. B. Personalplanung, Öffnungszeiten). |
| **Identifikations-Medien** | Chip-ID Ihrer RFID-Karte (UID) oder QR-Code-Token. | Technische Erkennung Ihres Zugangsmediums am Terminal zur Prüfung der Zugangsberechtigung. |
| **Biometrische Daten gemäß Art. 9 DSGVO (nur bei ausdrücklicher Einwilligung)** | | |
| **Biometrische Referenzdaten** | Ihr Referenzfoto und das daraus erstellte mathematische Modell (**Template**). | Eindeutige Identitätsprüfung für den Zugang ohne Identifikationsmedien (Chip/ RFID/ QR-Code) sowie zur Identitätssicherung bei Nutzung von Kombi-Option. |

| | | |
|---|---|---|
| **Temporäre Bilddaten** | Kurzzeitige Videoaufnahmen/Bilder während des Scanvorgangs am Terminal. | Durchführung des Abgleichs mit Ihrem hinterlegten Template in Echtzeit zur Türöffnung. |
| **Sicherheits- & Echtheitsdaten** | Technische Merkmale zur Echtheitsprüfung (Liveness Detection). | Missbrauchsschutz**:** Sicherstellung, dass eine reale Person (kein Foto/Video) vor dem Scanner steht (Anti-Spoofing). |

**4.) Datenempfänger und Auftragsverarbeitungsvertrag**

Zur Bereitstellung des Systems nutzt das Studio die Facetronic U.G., Im Zukunftspark 4, 74076 Heilbronn als Auftragsverarbeiter. Hierfür wurde mit Facetronic ein Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO geschlossen. Hierbei handelt es sich um einen datenschutzrechtlich vorgeschriebenen Vertrag, der eine datenschutzkonforme Verarbeitung Ihrer Daten gewährleistet. Facetronic setzt zur technischen Abwicklung und sicheren Speicherung (Hosting) die Infrastruktur von Amazon Web Services (AWS) ein. Die Verarbeitung erfolgt ausschließlich im Rechenzentrum Frankfurt am Main. Durch vertragliche Vereinbarungen und technische Verschlüsselung ist sichergestellt, dass die Dienstleister die Daten nur streng weisungsgebunden verarbeiten und kein unbefugter Zugriff auf biometrische Merkmale erfolgt.

**[hier müssen Sie als Studiobetreiber noch weitere Datenempfänger benennen, etwa den Betreiber Ihres Studio-Management-Systems (z.B. Magicline)]**

**5.) Speicherdauer**

Wir speichern Ihre personenbezogenen Daten nur so lange, wie es für die Erreichung der hier genannten Zwecke (Zutritt oder Vertragsverwaltung) erforderlich ist oder wie es die gesetzlichen Aufbewahrungsfristen vorsehen:

- **Klassische Identifikationsmedien (RFID-Karte / Chip / QR-Code):**
  Die auf den physischen oder digitalen Medien hinterlegten Identifikationsnummern (UID/Token) bleiben für die Dauer Ihrer aktiven Mitgliedschaft im System gespeichert. Mit Beendigung des Vertrages oder bei Rückgabe des Mediums wird die Verknüpfung zu Ihrer Person aufgehoben bzw. gelöscht.
- **Identifikationsdaten aus dem Onboarding (Referenz-Template):** Wenn Sie sich für den kartenlosen Zugang registrieren, wird kurzzeitig ein Foto aufgenommen. Unsere Software wandelt dieses Bild sofort in ein biometrisches Template (einen anonymen mathematischen Zahlencode) um. Diese Umwandlung erfolgt irreversible, d.h., dass aus dem Template im Nachhinein kein Bild mehr erzeugt werden kann.
  - Das zur Template-Erzeugung genutzte Lichtbild wird nach Abschluss des Rechenvorgangs unverzüglich gelöscht, sofern Sie nicht gesondert in die Nutzung als Profilbild in der Mitgliederverwaltung eingewilligt haben (je nach Studio). In den Facetronic IDA-Geräten wird ausschließlich das anonymisierte Template gespeichert.
  - Dieses Template wird gelöscht, sobald Sie Ihre Einwilligung widerrufen oder Ihre Mitgliedschaft endet.
- **Verarbeitungsdaten während des Zutrittsvorgangs:**
  - **Regulärer Zutritt (Übereinstimmung):** Das während des Zutrittsversuchs erfasste Lichtbild wird unmittelbar nach der Extraktion der biometrischen Merkmale (Hash-Erzeugung) noch vor dem eigentlichen Abgleich gelöscht. Der aus diesem Bild erstellte temporäre Hash (unabhängig davon, ob der Zutritt gewährt oder abgelehnt wurde) wird nach Abschluss des Identifikationsvorgangs ebenfalls unverzüglich gelöscht.

- **Identifikationsfehler (Keine Übereinstimmung):** Kann eine Person nicht eindeutig identifiziert werden (z. B. bei unbefugten Zutrittsversuchen durch Dritte), werden das Bild, der Zeitstempel und die ID für eine Dauer von maximal 10 Tagen gespeichert. Dies dient der nachträglichen Prüfung technischer Fehler sowie der Aufklärung unberechtigter Zutrittsversuche.
- **Dokumentierter Missbrauch**: Besteht nach einer manuellen Überprüfung der begründete Verdacht eines vorsätzlichen Missbrauchs (z. B. systematische Kartenweitergabe), werden die betreffenden Bilddaten zur Beweissicherung und zur Verfolgung von Rechtsansprüchen gemäß Art. 6 Abs. 1 lit. f DSGVO bis zum endgültigen Abschluss der rechtlichen Prüfung gespeichert.

- **Allgemeine Vertrags- und Protokolldaten:**
  - Protokolldaten über den Zeitpunkt des Zutritts (ohne Bildbezug) werden in der Regel nach 3 bis 6 Monaten automatisiert anonymisiert oder gelöscht.
  - Allgemeine Stammdaten und Vertragsunterlagen werden nach Beendigung der Mitgliedschaft für die Dauer der gesetzlichen Aufbewahrungspflichten gespeichert. Diese ergeben sich insbesondere aus dem Handels- und Steuerrecht (z. B. § 257 HGB, § 147 AO) und betragen je nach Art der Unterlagen zwischen 6 und 10 Jahren. Nach Ablauf dieser Fristen werden die Daten vollständig gelöscht.

## 6.) Automatisierte Entscheidungsfindung

Die Entscheidung über den Studiozutritt erfolgt automatisiert durch einen Systemabgleich:

**Identifikationsmedium (RFID/QR):** Ein softwarebasierter Logik-Abgleich prüft die Medien-ID gegen den Vertragsstatus in Magicline (ID vorhanden? Vertrag aktiv?).

**Biometrisch (1:N)**: Zweistufige Prüfung. Die **Edge-KI** identifiziert die Person mittels Liveness Detection (Spoofing-Abwehr) und Abgleich gegen hinterlegten Referenz-Hashes. Nach Identifizierung folgt die Statusprüfung durch Magicline.

**2-Faktor-Authentifizierung (1:1):** Kombiniertes Verfahren. Das Medium (RFID/QR) triggert die Kamera; die KI verifiziert das Live-Gesicht gezielt gegen den zur ID hinterlegten Hash (**1:1-Abgleich**). Dies dient der Identitätsprüfung und dem Ausschluss von Kartenmissbrauch.

**Hinweis**: Sie haben das Recht, die Entscheidung durch eine Person überprüfen zu lassen, Ihren eigenen Standpunkt darzulegen und die automatisierte Entscheidungsfindung anzufechten. Bitte wenden Sie sich hierfür an info@rb-verwaltung.com.

Die Automatisierung des Check-ins ist gemäß Art. 22 Abs. 2 lit. a DSGVO für den Abschluss oder die Erfüllung des Vertrages erforderlich, um einen reibungslosen Studiobetrieb (auch in personalfreien Zeiten) zu gewährleisten.

## 7.) Zweckbindung

Die erhobenen biometrischen oder technischen Identifikationsdaten werden ausschließlich zum Zwecke der Zutrittskontrolle und Identitätsverifikation verarbeitet. Eine anderweitige Nutzung oder Weitergabe an unbefugte Dritte ist ausgeschlossen; davon ausgenommen ist die technisch notwendige Übermittlung an unsere weisungsgebundenen IT-Dienstleister im Rahmen der Auftragsverarbeitung. Gegebenenfalls stattfindende statistische Auswertungen zur Auslastung der

Räumlichkeiten erfolgen ausschließlich in anonymisierter Form, ohne dass ein Rückschluss auf einzelne Personen möglich ist.

**8.) Freiwilligkeit und Widerruf**

- Die Teilnahme an der biometrischen Zugangskontrolle und die damit verbundene Bereitstellung von personenbezogenen Daten und biometrischen Daten ist freiwillig.
- Zur Wahrung der Freiwilligkeit stehen Ihnen auch alternative Zugangsmöglichkeiten zur Verfügung.
- Sie können Ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. In diesem Fall erfolgt der Zugang ausschließlich über die klassische Identifikationsmedien (RFID-Karte / Chip / QR-Code). Sie können die Möglichkeit des Kartenlosen Zugangs dann nicht mehr nutzen.

**9.) Ihre Rechte als betroffene Person**

Sie haben jederzeit folgende Rechte nach der Datenschutz-Grundverordnung:

- Auskunft nach Art. 15 DSGVO über die zu Ihrer Person gespeicherten Daten,
- Berichtigung unrichtiger oder unvollständiger Daten nach Art. 16 DSGVO,
- Löschung Ihrer Daten nach Art. 17 DSGVO, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen,
- Einschränkung der Verarbeitung nach Art. 18 DSGVO,
- Datenübertragbarkeit nach Art. 20 DSGVO,
- Widerspruch gegen die Verarbeitung nach Art. 21 DSGVO,
- Widerruf der Einwilligung nach Art. 7 Abs. 3 DSGVO: Sie haben das Recht, Ihre erteilte Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen, ohne dass die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung berührt wird.
- Beschwerde bei einer Datenschutzaufsichtsbehörde, insbesondere in dem Mitgliedstaat Ihres gewöhnlichen Aufenthaltsorts, Ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes (Art. 77 DSGVO).

**[Ende des unverbindlichen Formulierungsvorschlags für die Ergänzung Ihrer Datenschutzerklärung hinsichtlich der Datenverarbeitung durch den Einsatz des biometrische Zugangssystems]**

## III. Einwilligungserklärung

Es ist zwingende eine Einwilligungserklärung Ihrer Kunden hinsichtlich der Verarbeitung von biometrischen Daten einzuholen (in zweifacher Ausfertigung – eine für Sie und eine für Ihren Kunden).
Einen unverbindlichen Formulierungsvorschlag finden Sie als Studiobetreiber unter **Anlage 2.**

## IV. Nutzung der Nachrichtenfunktion des Lesers

Wenn Sie die Nachrichtenfunktion des Lesers nutzen wollen, muss dieser so montiert sein, dass Dritte das Display nicht einsehen können, während der Kunde die Nachrichten erhält und über den Scanner kommuniziert.

Bitte weisen Sie Ihre Kunden in diesem Fall auch darauf hin, dass sie darauf achten sollen, dass keine unbefugte Person die Nachrichten liest.

## V. Datenschutz-Folgeabschätzung

Bitte beachten Sie, dass gemäß Art. 35 Abs. 1 DSGVO immer dann eine Datenschutzfolgeabschätzung (DSFA) vom Verantwortlichen i.S.v. Art. 4 Nr. 7 DSGVO (Sie als Studiobetreiber) durchzuführen ist, wenn eine Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Beim Einsatz eines biometrischen Zugangssystems für ein Studio ist eine solche DSFA aus den folgenden Gründen erforderlich:

- Umfangreiche Verarbeitung besonderer Kategorien von Daten nach Art. 35 Abs. 3 lit. b DSGVO.
- Die Datenschutzaufsichtsbehörden führen gemäß Art. 35 Abs. 4 DSGVO Listen mit Verarbeitungsvorgängen, für welche die Durchführung eines DSFA erforderlich ist, sogenannte „Blacklist“. Demnach ist bei der Verarbeitung von biometriechen Daten zur Identifizierung eine DSFA durchzuführen, wenn die Verarbeitung großflächig erfolgt, was bei mehreren Studiomitgliedern der Fall ist.
- Nach den Leitlinien des Europäischen Datenschutzausschusses – WP 248, welchem sich die Datenschutzkonferenz (DSK) angeschlossen hat, nimmt die Wahrscheinlichkeit zu, dass eine Verarbeitung von Daten ein hohes Risiko für die Rechte und Freiheiten von Betroffenen hat und somit eine DSFA durchzuführen ist, wenn zwei oder mehr Risikokriterien erfüllt (z.B. Verarbeitung sensibler Daten + große Betroffenenzahl (mehrere Hundert Mitglieder)/ Systematische Überwachung (Protokollierung von Zutritten/ Fehlversuchen).

Die DSFA muss mindestens die nachfolgend dargestellten Inhalte abdecken. Zusätzlich sollten die Ergebnisse nachvollziehbar dokumentiert und die umgesetzten bzw. geplanten Maßnahmen (inkl. Verantwortlichkeiten und Terminen) festgehalten werden.

### 1. Systematische Beschreibung der geplanten Verarbeitung und Zwecke

- Zwecke der Zutrittskontrolle (z.B. Zugangsberechtigung prüfen, Missbrauch verhindern).
- Beschreibung der Verarbeitungsschritte (Enrollment/Registrierung, Matching, Zutrittsentscheidung, Logging).
- Datenkategorien (Templates/Rohdaten, Identitätsdaten, Zutritts- und Fehlversuchs-Logs, Admin-/Support-Logs).
- Beteiligte Rollen (Verantwortlicher/Auftragsverarbeiter), Empfänger und Unterauftragsverarbeiter.
- Datenflüsse und Speicherorte (Terminal/Edge/Server/Cloud), Schnittstellen (Mitgliederverwaltung etc.).
- Aufbewahrungs- und Löschfristen (inkl. Backup-/Synchronisationskonzept).

### 2. Bewertung von Notwendigkeit und Verhältnismäßigkeit

- Eignung und Erforderlichkeit: Warum ist Biometrie für den Zweck nötig?
- Prüfung milderer Mittel: Karte/QR/PIN/Smartphone; Dokumentation der Abwägung.
- Gestaltung einer gleichwertigen Alternative ohne Nachteile (sofern Biometrie freiwillig/auf Einwilligung basiert).

- Datenminimierung: Speicherung von Templates statt Rohdaten; Umfang und Dauer von Logs.
- Transparenz und Betroffenenrechte: Information der Mitglieder, Prozesse für Auskunft, Löschung, Widerruf/De-Enrollment.

**3. Bewertung der Risiken für Rechte und Freiheiten der Betroffenen**

- Sicherheitsrisiken: unbefugter Zugriff, Datenabfluss von Templates/Logs, Insider-Risiken.
- Fehlzuordnungen (False Accept/False Reject): unberechtigter Zutritt oder unberechtigte Zutrittsverweigerung.
- Zweckausweitung (function creep): Nutzung von Zutrittsdaten zur Leistungs-/Verhaltenskontrolle oder Profilbildung.
- Diskriminierungs- und Barrierefreiheitsrisiken (z.B. bestimmte Gruppen/Behinderungen).
- Risikoerhöhung durch zentrale Speicherung, große Betroffenenzahl oder umfangreiche Protokollierung.

**4. Geplante Maßnahmen zur Bewältigung der Risiken (Garantien, Sicherheitsvorkehrungen, Verfahren)**

- Technische und organisatorische Maßnahmen (TOMs): Verschlüsselung, Zugriffskontrolle (Rollen/MFA), Protokollierung, Härtung, Update-/Patch-Prozess, Monitoring.
- Architekturmaßnahmen: Trennung von Identitätsdaten und Templates, möglichst dezentrale/Edge-Speicherung, Mandantentrennung.
- Lösch- und Aufbewahrungsumsetzung: automatisierte Löschung, Backups/Replicas, Nachweisbarkeit.
- Support- und Administrationsprozesse: Freigabeprozesse, Protokollierung, minimale Rechte, zeitlich begrenzter Zugriff.
- Fallback/Notfall: alternativer Zutritt, Verfahren bei Störungen, Incident-Response inkl. Meldewegen.
- Wirksamkeitskontrolle: Tests/Reviews (z.B. Berechtigungstests, Löschtests), regelmäßige Aktualisierung der DSFA bei Änderungen.

Das Ergebnis der DSFA ist in einer Dokumentation festzuhalten, die zumindest folgenden Inhalt haben muss:

- DSFA-Bericht mit den Mindestinhalten (Kap. 4.1–4.4) und einer zusammenfassenden Risikobeurteilung.
- Maßnahmenplan (TOMs/organisatorische Maßnahmen) inkl. Verantwortlichkeiten, Fristen, Status.
- Entscheidungsvorlage zur Schwellwertanalyse (DSFA ja/nein) inkl. Begründung.
- Nachweise/Anhänge: Systemdokumentation, TOM-Anlage, Löschkonzept, Unterauftragsverarbeiterliste, Test-/Auditnachweise (soweit vorhanden).

## VI. Kurze Checkliste: Compliance-Anforderungen für den rechtssicheren Einsatz des biometrischen Zugangssystem von Facetronic in Ihrem Studio

### 1. Einwilligungsmanagement (Freiwilligkeit und Rechtsgrundlage)

Die Verarbeitung biometrischer Daten erfordert eine ausdrückliche Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO i.V.m. Art. 9 Abs. 2 lit. a DSGVO.

**Maßnahme**: Sie müssen von jedem Ihrer Kunden eine schriftliche oder rechtssichere digitale Einwilligungserklärung hinsichtlich der Verarbeitung von personenbezogenen Daten nach Art. 6 Abs. 1 lit. a DSGVO i.V.m. Art. 9 Abs. 2 lit. a DSGVO einholen.

**Zu beachten**: Sie müssen zwingend eine gleichwertige Alternative (z.B. RFID-Medium, PIN-Code) ohne Zusatzkosten anbieten, um die Bedingungen der Freiwilligkeit der Einwilligung nach Art. 7 DSGVO zu wahren.

### 2. Rechenschaftspflicht und Dokumentation

Gemäß Art. 4 Nr. 7 DSGVO müssen Sie als verantwortlicher Studiobetreiber die Konformität Ihrer Systeme, welche Daten Ihrer Kunden verarbeiten, jederzeit nachweisen können, Art. 5 Abs. 2 DSGVO.

**Maßnahmen**:

Sie müssen die Zugangskontrolle als eigenständigen Prozess in Ihrem Verarbeitungsverzeichnis aufnehmen.

Sie müssen eine Datenschutzfolgenabschätzung gemäß Art- 35 DSGVO durchführen.

### 3. Transparenz und Informationspflichten

Ihre Kunden als Betroffene im Sinne der DSGVO müssen zum Zeitpunkt der Datenerhebung über alle Details informiert werden, Art. 13 DSGVO.

**Maßnahme**: Stellen Sie spezifische Datenschutzhinweise zur biometrischen Zutrittskontrolle bereit. Diese müssen alle Pflichtangaben (u. a. Zweck, Speicherdauer, Betroffenenrechte und Empfänger der Daten) enthalten.

**Bereitstellung**: Die Informationen müssen dem Mitglied **vor der Unterzeichnung** des Vertrages bzw. vor dem Onboarding zur Kenntnis gegeben werden (z. B. als fester Bestandteil der Vertragsunterlagen oder durch gut sichtbaren Aushang am Point of Collection).

### 4. Auftragsverarbeitung

Sie müssen für die technische Bereitstellung durch den Dienstleister (Facetronic) einen Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO mit dem Dienstleister schließen.

**Maßnahme:** Schließen Sie einen Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO ab. Stellen Sie hierbei sicher, dass die EU-Standardvertragsklauseln (SCCs) als Anlage integriert sind, um potenzielle Datentransfers in Drittländer rechtssicher abzudecken.

### 5. Personalschulungen

Sie müssen nach Art. 4 der KI-Verordnung (KI-VO) Ihre Mitarbeiter im Umgang mit sensiblen biometrischen Systemen durch Schulungen sensibilisieren.

**Maßnahme:** Unterweisen Sie Ihr Team in der Funktionsweise der Vektorisierung: das Gesicht des Nutzers wird nicht als Foto gespeichert, sondern in einen abstrakten, nicht umkehrbaren Zahlencode umgewandelt, aus welchem nachträglich kein Bild rekonstruiert werden kann. In der täglichen Beratung ist daher zu betonen, dass Sie lediglich mit einem mathematischen „Fingerabdruck“ arbeiten und der kurzzeitige Videostream ausschließlich der Identitätssicherheit (Lebenderkennung) dient und sofort wieder gelöscht wird.

**Ziel**: Kompetente Auskunftsfähigkeit gegenüber Mitgliedern und Sicherstellung, dass keine unbefugten Fotoaufnahmen der Monitore oder Terminals angefertigt werden.

**Information nach Art. 13 DSGVO zur biometrischen Gesichtserkennung**

Fitomat Römhild setzen ein biometrisches Gesichtserkennungssystem zur Zugangskontrolle ein. Hierbei erfasst die Kamera biometrische Merkmale zur Erstellung eines Templates Ihres Gesichtsbildes, zum Abgleich mit dem hinterlegten Referenztemplate.

| | |
|---|---|
| **Name und Kontaktdaten des Verantwortlichen** | RB-Verwaltungs GmbH<br>Heurichstr. 5, 98630 Römhild; info@rb-verwaltung.com |
| **Kontaktdaten des Datenschutzbeauftragten** | RB-Verwaltungs GmbH<br>Heurichstr. 5, 98630 Römhild; info@rb-verwaltung.com |
| **Zwecke und Rechtsgrundlagen der Datenverarbeitung** | **Verarbeitungszweck**: Berechtigungsprüfung für Zutritt zum Studio.<br>**Rechtsgrundlage**: Die Einwilligung des Mitglieds gemäß Art. 9 Abs. 2 li. a DSGVO i.V.m. Art. 6 Abs. 1 lit. a DSGVO. |
| **Freiwilligkeit** | Die Nutzung ist freiwillig. |
| **Verfahren** | - Biometrische Verifikation<br>Ich möchte mein Zugangsmedium (Chip/QR) zusätzlich absichern. Beim Vorhalten des Mediums prüft die Kamera, ob mein Gesicht zum hinterlegten Profil passt (1:1 Abgleich). Dies dient dem Schutz vor Kartenmissbrauch (Chip-Sharing).<br>- Biometrische Identifikation<br>Ich möchte das Studio ohne Chip oder Karte betreten. Die Kamera erkennt mich automatisch beim Auslösen des Terminals durch Abgleich meines Live-Bildes mit der Datenbank (1:N Ab-gleich). |
| **Datenempfänger** | - **Facetronic UG** (haftungsbeschränkt), Im Zukunftspark 4, 74076 Heilbronn.<br>info@facetronic.de<br>Wir haben mit Facetronic einen Vertrag zur Auftragsverarbeitung gem. Art 28 DSGVO geschlossen.<br><br>- **Magic-line GmbH**, Raboisen 6, 20095 Hamburg.<br>welcome@magicline.de<br>Wir haben mit Magicline einen Vertrag zur Auftragsverarbeitung gem. Art 28 DSGVO geschlossen.<br><br>**Sicherheit**: Es erfolgt keine Weitergabe an unbefugte Dritte oder eine Nutzung zu Marketingzwecken. |
| **Speicherdauer** | Die Daten werden gelöscht, wenn der Zweck der Verarbeitung entfällt, sofern keine gesetzlichen Speicherfristen entgegenstehen. |
| **Betroffenenrechte** | Sie haben als betroffene Person das Recht von Fitomat Römhild Auskunft über die Verarbeitung personenbezogener Daten (Art. 15 DSGVO), die Berichtigung unrichtiger Daten (Art. 16 DSGVO), die Löschung der Daten (Art. 17 DSGVO) und die Einschränkung der Verarbeitung (Art. 18 DSGVO) zu verlangen, sofern die rechtlichen Voraussetzungen dafür vorliegen. Sie können verlangen, die bereitgestellten personenbezogenen Daten gemäß Art. 20 DSGVO zu erhalten oder zu übermitteln. Sie können nach Art. 21 DSGVO Widerspruch einlegen. Die Einwilligung in die Verarbeitung Ihrer Daten können Sie jederzeit widerrufen. Unbeschadet anderer Rechtsbehelfe können Sie sich beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit, Postfach 10 29 32, 70025 Stuttgart oder poststelle@lfdi.bwl.de, beschweren. |

Weitere Informationen entnehmen Sie bitte unserer Datenschutzerklärung:

unter www.rb-verwaltung.com

**Einwilligungserklärung in die biometrische Datenverarbeitung**

Die Einwilligung über die Verarbeitung meiner personenbezogenen Daten und der biometrischen Datenverarbeitung ist freiwillig, jederzeit beschränkbar und kann gegenüber Fitomat Römhild für die Zukunft widerrufen werden. Die Rechtmäßigkeit der Verarbeitung bis zum Widerruf wird dadurch nicht berührt.

Der Zutritt erfolgt über einen automatisierten Abgleich der biometrischen Merkmale des Nutzers. Die Entscheidung über die Türöffnung erfolgt vollautomatisch durch den Systemabgleich. Eine positive Identifizierung führt zur sofortigen Türöffnung. Im Falle einer Nichtübereinstimmung wird der Zutritt automatisch verweigert und die versuchte unbefugte Nutzung zu Sicherheitszwecken protokolliert.

Die Nutzung der biometrischen Gesichtserkennung ist freiwillig. Sollten Sie diese nicht nutzen wollen oder Ihre Einwilligung widerrufen, stellen wir Ihnen klassische Identifikationsmedien (RFID-Karte / Chip / QR-Code) zur Verfügung.

Die Informationen zur Datenerhebung gem. Art. 13 Datenschutzgrundverordnung (DSGVO) können Sie dem Aushang beim Zutritt des Studios entnehmen.