

*MUSTER Fitnessbetriebe*

Datenverarbeitungsverzeichnis

nach Art 30 Abs 1 Datenschutz-Grundverordnung (DSGVO)

[Verantwortlicher]

**Inhalt:**

Stammdaten

Verarbeitungsverfahren:

(Unzutreffendes löschen, Fehlendes ergänzen.)

1. Verkauf
2. Betrieb (CRM)
3. (Teil-)Automatisierte Trainingssteuerung 1)
4. Rechnungswesen
5. Personalwesen
6. Korrespondenz
7. Videoüberwachung
8. …………

Änderungsverlauf

Stammfassung vom ………… . Unterschrift:

1. Änderung vom …………. Unterschrift:

2. Änderung vom …………. Unterschrift:

*Dieses Dokument bezieht sich auf die ab 25.5.2018 in Österreich wirksame Rechtslage. Es wurde in Zusammenarbeit der Bundessparte Tourismus und Freizeitwirtschaft, des Fachverbands der Fitnessbetriebe und der Rechtsanwaltskanzlei MSP Law als unverbindliches Muster erstellt. Da Unternehmen sehr unterschiedlich arbeiten, muss dieses Dokument an die Gegebenheiten des Unternehmens angepasst werden. Es wird empfohlen, für diese Anpassung einen Rechtsberater beizuziehen. Eine Haftung der Urheber dieses Musters ist ausgeschlossen.*

Stammdaten

1. **Verantwortlicher Verarbeiter**

Fitnessstudio GmbH &Co KG, FB-Nummer

[Adresse]

[Telefon]

[Name des Geschäftsführers]

(zuständig für Datenschutz gemäß Geschäftsordnung vom [……….]): […….]

1. **Datenschutzkoordinator [untersteht dem Geschäftsführer]**

[Vorname Nachname]

[Funktion im Unternehmen]

[TelNr.]

[E-Mail]

1. **Weisungsfreier Datenschutzbeauftragter [soweit erforderlich]**

[Vorname Nachname]

[Funktion im Unternehmen]

[TelNr.]

[E-Mail]

1. **Datenschutz-Folgenabschätzung**

Eine Datenschutz-Folgenabschätzung wurde

o erstellt am ……………….1)

o nicht erstellt, weil die Verarbeitungen kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folgen haben. Insbesondere werden **nicht** eingesetzt:

- neue Technologien mit hohem Risikopotenzial, wie zB teilautomatisierte Trainingssteuerung;

- automatisiertes Profiling als Grundlage für Entscheidungsprozesse;

- umfangreiche Verarbeitung sensibler Daten (Art 9 Abs 1 DSGVO);

- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (Videoüberwachung).

(Zutreffendes ankreuzen oder ergänzen)

1. Wenn teil-automatisierte Trainingssteuerung eingesetzt wird, ist zwingend eine Datenschutz-Folgenabschätzung durchzuführen.
2. Verkauf
3. Verfahren

Bezeichnung: Beratung von Interessenten, Verkauf und Abrechnung von Leistungen des Fitnessstudios

Fachabteilung: Vertrieb

Kontakt: [Name des Abteilungsleiters]

1. Zweckbestimmung

Akquisition von Kunden, Beratung von Interessenten, Abschluss und Abrechnung von Verträgen.

1. Details zur Datenverarbeitung
   1. Betroffene Personen  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |
| --- | --- | --- |
|  | Personengruppe | Anmerkung |
| 01 | Interessenten | keine Kinder unter 16 Jahren |
| 02 | Kunden | keine Kinder unter 16 Jahren |
| 03 | Vertrauensperson | zur Information bei Notfällen |

* 1. Datenverwendung & Weitergabe  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

Verwendung intern

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
| 01 | Rechnungswesen | Gesetz |
| 02 | Marketing | Einwilligung |
|  |  |  |

Weitergabe extern

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
| 03 | Steuerberatung, Rechtsanwälte | Abwägung 1) |
| 04 | Gerichte, Behörden | Gesetz |
| 05 | Externe Beratungsunternehmen | Einwilligung (soweit nicht anonymisiert) |
|  |  | Vertrag |

1. Interesse des Verarbeiters an steuerlicher, rechtlicher und sonstiger Beratung überwiegt das Geheimhaltungsinteresse des Betroffenen, wenn die Empfänger zur Verschwiegenheit gegenüber Dritten gesetzlich oder vertraglich verpflichtet sind.

Weitergabe Drittstaaten

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
|  |  |  |

* 1. Auftragsverarbeiter

Firma [genauer Firmenname]

Adresse [Postanschrift]

Kontaktperson [Name, E-Mail, TelNr.]

Vertragsnummer

(Mehrere Auftragsverarbeiter gesondert anführen)

1. Datenkategorien
   1. Kunden  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | Lösch-frist | Empfänger – siehe 3.2. | Anmerkung |
| 01 | Name | Person | 5J | 01-05 |  |
| 02 | Geburtsdatum | Person | 5J | 01-05 |  |
| 03 | Geschlecht | Person | 5J | 02,04,05 |  |
| 04 | Sprache, Nationalität | Person | 5J | 02,04,05 |  |
| 05 | Postadresse | Person | 5J | 01-05 |  |
| 06 | Kontaktdaten inkl. TelNr | Person | 5J | 02,04,05 |  |
| 07 | Vertrauensperson | Person | 5J | 04 |  |
| 08 | Trainingsplan | Person | 5J | 02,04,05 |  |
| 09 | Preise, Konditionen | intern | 5J | 01-05 |  |
| 10 | Zahlungsart | Person | 5J | 01,03,04 |  |
| 11 | Bankverbindung, Kreditkarten | Person | 5J | 01,03,04 |  |
| 12 | KFZ Kennzeichen, PKW-Modell | Person | 5J | 04 |  |
| 13 | persönliche Bedürfnisse, Sonderwünsche | Person | 5J | 02,04,05 | sensibel, Zugriffsbeschrän-kung sofort nach Kündigung |
| 14 | Allergien & Unverträglichkeiten | Person | 5J | 02,04,05 | sensibel, Zugriffsbeschrän-kung sofort nach Kündigung |
| 15 | Anamnesedaten zu Fitness und Gesundheit | Person | 5J | 04,05 | sensibel, Zugriffsbeschrän-kung sofort nach Kündigung |
| 16 | Körpermaße | Person | 5J | 04,05 |  |
| 17 | Kunden-Feedback | Person | 5J | 02,04,05 |  |
|  |  |  |  |  |  |

* 1. Interessenten  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | Lösch-frist | Empfänger – siehe 3.2. | Anmerkung |
| 01 | Name | Person | 1J | 02,04,05 |  |
| 02 | Geburtsdatum | Person | 1J | 02,04,05 |  |
| 03 | Geschlecht | Person | 1J | 02,04,05 |  |
| 04 | Sprache, Nationalität | Person | 1J | 02,04,05 |  |
| 05 | Postadresse | Person | 1J | 02,04,05 |  |
| 06 | Kontaktdaten inkl. TelNr | Person | 1J | 02,04,05 |  |
| 13 | persönliche Bedürfnisse, Sonderwünsche | Person | 3M | 02,05 | sensibel, Zugriffsbeschrän-kung sofort nach Kündigung |
| 14 | Allergien & Unverträglichkeiten | Person | 3M | 04 | sensibel, Zugriffsbeschrän-kung sofort nach Kündigung |
| 15 | Anamnesedaten zu Fitness und Gesundheit | Person | 3M | 04 | sensibel, Zugriffsbeschrän-kung sofort nach Kündigung |
| 16 | Körpermaße | Person | 3M | 04 |  |
|  |  |  |  |  |  |

* 1. Vertrauenspersonen 1)  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | Lösch-frist | Empfänger  siehe 3.2. | Anmerkung | |
| 01 | Name | Person |  | 04 |  |
| 02 | Naheverhältnis | Person |  | 04 |  |
| 03 | Postadresse | Person |  | 04 |  |
| 04 | Kontaktdaten inkl. TelNr. | Person |  | 04 |  |
|  |  |  |  |  |  |

1. Die Vertrauensperson wird im Notfall (Unfall, Erkrankung) benachrichtig.
2. Technisch-organisatorische Maßnahmen (TOMs)
   1. Applikationen  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Applikation | Auftrags-verarbeiter | Maßnahmen |
| 01 | Mitgliederverwaltung |  | siehe Richtlinie für die Vergabe von User-Berechtigungen |
| 02 | Abrechnungs-Software |  | siehe Richtlinie für die Vergabe von User-Berechtigungen |
| 03 | Web-Portal |  | Schutzmaßnahmen gegen Hacker laut IT-Handhandbuch vom [….] |
|  |  |  |  |
|  |  |  |  |

* 1. Datenschutz durch Technologiegestaltung („privacy by design“) ist gewährleistet durch:
* Restriktive Zugriffsberechtigungen
* Datenschutzfreundliche Applikationen (siehe User-Handbuch der Applikationen)
* Verschlüsselung und Pseudonymisierung von Kreditkartendaten
* Sonstiges: Zugriff auf sensible Daten nur für besonders geschulte Mitarbeiter, die die Daten für ihre Tätigkeit (zB Personal Trainer) benötigen.

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Datenschutz durch datenminimierende Voreinstellungen („privacy by default“) ist gewährleistet durch:
* Grundeinstellungen in der Buchungssoftware
* Grundeinstellungen im Web-Portal
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Datensicherheit (Vertraulichkeit, Verfügbarkeit, Integrität)

Elektronische Verarbeitungen

* Verschlüsselung sämtlicher Datenträger auf denen personenbezogene Daten gespeichert werden;
* Verschlüsselung bei Übermittlungen an Auftragsverarbeiter oder Behörden;
* Mehrstufige Systemsicherungen (B2D2T). Sämtliche Sicherungsdaten sind ebenfalls verschlüsselt und die Aufbewahrung der Archivbänder erfolgt georedundant,
* Hohe Sicherungsmechanismen im Bereich der Netzwerktechnologie. Physisch getrenntes WLAN für Kunden.
* Regelmäßige Überprüfung der Maßnahmen durch den Datenschutzverantwortlichen und den Auftragsverarbeiter.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

Analoge Verarbeitungen

* Strukturierte Sammlungen von personenbezogenen Daten werden nicht für jedermann zugänglich aufbewahrt: in versperrbaren Schränken bzw. Räumen zu denen nur berechtigte Mitarbeiter Zugang haben.
* Sensible Daten in Papierakten werden nur versperrt und in Räumen mit Zugangskontrollen aufbewahrt.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Methoden zur Datenlöschung

Elektronische Verarbeitungen

* Die eingesetzten Applikationen (allenfalls ergänzt durch spezielle Software-Tools wie zB Tealium) gewährleisten, dass sämtliche elektronisch erfasste Datenkategorien mit entsprechenden Tags versehen werden. Dadurch wird die automatische Löschung bzw. Anonymisierung einzelner Datenkategorien, nach Wegfall der Rechtsgrundlage zur Verarbeitung, ermöglicht.
* Im Falle einer Löschung nach Betroffenenbegehren wird diese protokolliert und in die operativen Backups nachgezogen.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen)

Analoge Verarbeitungen

* Strukturierte Sammlungen von personenbezogenen Daten werden nach der angegebenen Aufbewahrungsfrist vernichtet.
* Sonstige: Sensible Daten werden 3 Monate nach Ende der Vertragsbeziehung in ein gesichertes Archiv mit Zutrittskontrollen transferiert.

(Zutreffendes ankreuzen oder ergänzen.)

1. Profiling

* Nein
* Ja, und zwar:

(Zutreffendes ankreuzen oder ergänzen.)

1. Entscheidungsautomatisierung

* Nein
* Ja, und zwar:

(Zutreffendes ankreuzen oder ergänzen.)

1. Betroffenenrechte
   1. Information Betroffener

* Standardformat: PDF
* Sonstiges

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Art der Information des Betroffenen?
* E-Mail, wenn Anfrage per E-Mail, sonst per Post
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

1. Betrieb
2. Verfahren

Bezeichnung: Betrieb des Fitness-Centers

Fachabteilung: Betrieb

Kontakt: [Name des Abteilungsleiters]

1. Zweckbestimmung

Betrieb des Fitness-Centers, Terminvereinbarungen, Gruppentrainings, Buchung von Zusatzleistungen, Beratung des Kunden

1. Details zur Datenverarbeitung
   1. Betroffene Personen  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |
| --- | --- | --- |
|  | Personengruppe | Anmerkung |
| 01 | Kunden |  |
|  |  |  |

* 1. Datenverwendung & Weitergabe  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

Verwendung intern

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
| 01 | Rechnungswesen | Gesetz |
| 02 | Marketing | Einwilligung, Abwägung |
|  |  |  |
|  |  |  |

Weitergabe extern

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
| 03 | Externe Trainer | Vertrag |
| 04 | Steuerberatung, Rechtsanwälte | Abwägung 1) |
| 05 | Gerichte, Behörden | Gesetz |
| 06 | Externe Beratungsunternehmen | Einwilligung (soweit nicht anonymisiert) |
|  |  |  |

1. Interesse des Verarbeiters an steuerlicher, rechtlicher und sonstiger Beratung überwiegt das Geheimhaltungsinteresse des Betroffenen, wenn die Empfänger zur Verschwiegenheit gegenüber Dritten gesetzlich oder vertraglich verpflichtet sind.

Weitergabe Drittstaaten

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
|  |  |  |

* 1. Auftragsverarbeiter

Firma [genauer Firmenname]

Adresse [Postanschrift]

Kontaktperson [Name, E-Mail, TelNr.]

Vertragsnummer

(Mehrere Auftragsverarbeiter gesondert anführen.)

1. Datenkategorien
   1. Kunde  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | Lösch-frist | Empfänger – siehe 3.2. | Anmerkung |
| 01 | Trainingszeiten | intern | 1J | 02,03,05,06 |  |
| 02 | Trainingsmethoden | intern | 1J | 02,03,05,06 |  |
| 03 | Zusatzleistungen | Person | 1J | 02,03,05,06 |  |
| 04 | Gruppentrainings | Person | 1J | 02,03,05,06 |  |
| 05 | Gastro-Konsumation | Person | 1J | 02,04-06 |  |
| 06 | Merchandising | Person | 1J | 02,04-06 |  |
| 07 |  |  |  |  |  |
| 08 |  |  |  |  |  |
|  |  |  |  |  |  |

1. Technisch-organisatorische Maßnahmen (TOMs)
   1. Applikationen  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Applikation | Auftrags-verarbeiter | Maßnahmen |
| 01 | Mitgliederverwaltung |  | siehe Richtlinie für die Vergabe von User-Berechtigungen |
| 02 | Terminverwaltung |  | siehe Richtlinie für die Vergabe von User-Berechtigungen |
|  |  |  |  |
|  |  |  |  |

* 1. Datenschutz durch Technologiegestaltung („privacy by design“) ist gewährleistet durch:
* Restriktive Zugriffsberechtigungen
* Datenschutzfreundliche Applikationen (siehe User-Handbuch der Applikationen)
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Datenschutz durch datenminimierende Voreinstellungen („privacy by default“) ist gewährleistet durch:
* Grundeinstellungen in der Terminverwaltungs-Software
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Datensicherheit (Vertraulichkeit, Verfügbarkeit, Integrität)

Elektronische Verarbeitungen

* Verschlüsselung sämtlicher Datenträger auf denen personenbezogene Daten gespeichert werden;
* Verschlüsselung bei Übermittlungen an Auftragsverarbeiter oder Behörden;
* Mehrstufige Systemsicherungen (B2D2T). Sämtliche Sicherungsdaten sind ebenfalls verschlüsselt und die Aufbewahrung der Archivbänder erfolgt georedundant,
* Hohe Sicherungsmechanismen im Bereich der Netzwerktechnologie. Physisch getrenntes WLAN für Kunden.
* Regelmäßige Überprüfung der Maßnahmen durch den Datenschutzverantwortlichen und den Auftragsverarbeiter.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

Analoge Verarbeitungen

* Außer den Trainingsplänen existieren keine Papierunterlagen.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Methoden zur Datenlöschung

Elektronische Verarbeitungen

* Die eingesetzten Applikationen (allenfalls ergänzt durch spezielle Software-Tools wie zB Tealium) gewährleisten, dass sämtliche elektronisch erfasste Datenkategorien mit entsprechenden Tags versehen werden. Dadurch wird die automatische Löschung bzw. Anonymisierung einzelner Datenkategorien, nach Wegfall der Rechtsgrundlage zur Verarbeitung, ermöglicht.
* Im Falle einer Löschung nach Betroffenenbegehren wird diese protokolliert und in die operativen Backups nachgezogen.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen)

Analoge Verarbeitungen

* Ausgedruckte Trainingspläne werden nach Ablauf der Trainingsperiode vernichtet.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

1. Profiling

* Nein
* Ja, und zwar:

(Zutreffendes ankreuzen oder ergänzen.)

1. Entscheidungsautomatisierung

* Nein
* Ja, und zwar:

(Zutreffendes ankreuzen oder ergänzen.)

1. Betroffenenrechte
   1. Information Betroffener

* Standardformat: PDF
* Sonstiges

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Art der Information des Betroffenen?
* E-Mail, wenn Anfrage per E-Mail, sonst per Post
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

1. Automatisierte Trainingssteuerung

1. Verfahren

Bezeichnung: Einsatz computergesteuerter Trainingsgeräte

Fachabteilung: Betrieb

Kontakt: [Name des Abteilungsleiters]

1. Zweckbestimmung

Einsatz moderner, computergesteuerter Trainingsgeräte zur Optimierung von Trainings unter Berücksichtigung der individuellen Voraussetzungen und Entwicklung des Kunden.

1. Details zur Datenverarbeitung
   1. Betroffene Personen  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |
| --- | --- | --- |
|  | Personengruppe | Anmerkung |
| 01 | Kunden | keine Kinder unter 16 Jahren |

* 1. Datenverwendung & Weitergabe  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

Verwendung intern

Nein.

Weitergabe extern

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
| 01 | Externe Trainer | Einwilligung |

Weitergabe Drittstaaten

Nein.

* 1. Auftragsverarbeiter

Firma [Hersteller der Trainingsgeräte zB Milon Care GmbH]

Adresse [Postanschrift]

Kontaktperson [Name, E-Mail, TelNr.]

Vertragsnummer

(Mehrere Auftragsverarbeiter gesondert anführen)

1. Datenkategorien
   1. Kunden  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | Lösch-frist | Empfänger – siehe 3.2. | Anmerkung |
|  | Trainingstermine und -dauer | intern | 3M | 01 |  |
|  | Trainingsleistung (kW, Strecke, Frequenz etc) | intern | 3M | 01 | sensibel |
|  | Vitalwerte (Blutdruck, Atemfrequenz etc) | intern | 3M | 01 | sensibel |
|  | automatisierte Trainingspläne | intern | 3M | 01 |  |
|  | Leistungsstatistik | intern | 3M | 01 | sensibel |
|  |  |  |  |  |  |

1. Technisch-organisatorische Maßnahmen (TOMs)
   1. Applikationen  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Applikation | Auftrags-verarbeiter | Maßnahmen |
| 01 | Trainingssoftware | zB Milon Care | Zugriff nur für den persönlichen Trainer des Kunden |
|  |  |  |  |

* 1. Datenschutz durch Technologiegestaltung („privacy by design“) ist gewährleistet durch:
* Verschlüsselung und Pseudonymisierung von Trainingsdaten
* Zugriff auf sensible Daten nur für besonders geschulte Mitarbeiter, die die Daten für ihre Tätigkeit (zB Personal Trainer) benötigen.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Datenschutz durch datenminimierende Voreinstellungen („privacy by default“) ist gewährleistet durch:
* Der Kunde entscheidet, welche Daten ermittelt und gespeichert werden.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Datensicherheit (Vertraulichkeit, Verfügbarkeit, Integrität)

Elektronische Verarbeitungen

* Verschlüsselung sämtlicher Datenträger auf denen personenbezogene Daten gespeichert werden;
* Verschlüsselung bei Übermittlungen an Auftragsverarbeiter oder Behörden;
* Mehrstufige Systemsicherungen (B2D2T). Sämtliche Sicherungsdaten sind ebenfalls verschlüsselt und die Aufbewahrung der Archivbänder erfolgt georedundant,
* Hohe Sicherungsmechanismen im Bereich der Netzwerktechnologie. Physisch getrenntes WLAN für Kunden.
* Sichtschutz von Monitoren, damit Dritte nicht mitlesen können.
* Regelmäßige Überprüfung der Maßnahmen durch den Datenschutzverantwortlichen und den Auftragsverarbeiter.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

Analoge Verarbeitungen

* Kein Ausdruck von Trainingsdaten.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Methoden zur Datenlöschung

Elektronische Verarbeitungen

* Automatische Löschung 3 Monate nach Beendigung des Vertragsverhältnisses, wenn keine Einwilligung für eine längere Speicherung vorliegt.
* Im Falle einer Löschung nach Betroffenenbegehren wird diese protokolliert und in die operativen Backups nachgezogen.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen)

Analoge Verarbeitungen

* Keine.

(Zutreffendes ankreuzen oder ergänzen.)

1. Profiling

* Ja, für Zwecke der Trainingsoptimierung.
* sonstiges

(Zutreffendes ankreuzen oder ergänzen.)

1. Entscheidungsautomatisierung

* Nein
* Ja, und zwar:

(Zutreffendes ankreuzen oder ergänzen.)

1. Betroffenenrechte
   1. Information Betroffener

* Standardformat: PDF
* Sonstiges

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Art der Information des Betroffenen?
* E-Mail, wenn Anfrage per E-Mail, sonst per Post
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

1. RECHNUNGSWESEN

1. Verfahren

Bezeichnung: Rechnungswesen

Fachabteilung: Verwaltung

Kontakt: [Name des Abteilungsleiters]

1. Zweckbestimmung

Abrechnung von Leistungen gegenüber Kunden, Abwicklung und Bezahlung von Leistungen von Lieferanten und externen Trainern, Erfüllung der Aufgaben eines ordnungsgemäßen Rechnungswesens.

1. Details zur Datenverarbeitung
   1. Betroffene Personen  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |
| --- | --- | --- |
|  | Personengruppe | Anmerkung |
| 01 | Kunden |  |
| 02 | externe Trainer |  |
| 03 | sonstige Geschäftspartner |  |
| 04 | Kontaktpersonen |  |
|  |  |  |

* 1. Datenverwendung & Weitergabe  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

Verwendung intern

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
| 01 | Marketing | Einwilligung |
|  |  |  |

Weitergabe extern

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
| 02 | Banken | Vertrag |
| 03 | Steuerberatung, Rechtsanwälte | Abwägung 1) |
| 04 | Gerichte, Behörden | Gesetz |
|  |  |  |

1. Interesse des Verarbeiters an steuerlicher, rechtlicher und sonstiger Beratung überwiegt das Geheimhaltungsinteresse des Betroffenen, wenn die Empfänger zur Verschwiegenheit gegenüber Dritten gesetzlich oder vertraglich verpflichtet sind.

Weitergabe Drittstaaten

Nein.

* 1. Auftragsverarbeiter

Firma Steuerberatungskanzlei ………….

Adresse [Postanschrift]

Kontaktperson [Name, E-Mail, TelNr.]

Vertragsnummer

(Mehrere Auftragsverarbeiter gesondert anführen.)

1. Datenkategorien
   1. Kunden  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | Löschfrist | Empfänger, siehe 3.2. | Anmerkung |
| 01 | Name | Person | 7J | 01-04 | § 212 UGB, § 132 BAO |
| 02 | Postadresse | Person | 7J | 01-04 |  |
| 03 | Kundennummer | intern | 7J | 01-04 |  |
| 04 | Bankverbindung | Person | 7J | 02-04 |  |
| 05 | Zahlungskonditionen | intern | 7J | 01,03,04 |  |
| 06 | Ausgangsrechnungen | intern | 7J | 01-04 |  |
| 07 | Zahlungen | intern | 7J | 02-04 |  |
| 08 | offene Posten | intern | 7J | 01,03,04 |  |
| 09 | Mahnstufe | intern | 7J | 01,03,04 |  |
| 10 | Bonität | KSV | 7J | 01 |  |
| 11 | Daten zur Akquisition (Provisionen etc) | intern | 7J | 01,03,04 |  |
| 12 | Daten zur Steuerberechnung (USt-Pflicht, UID-Nr. etc) | Person | 7J | 03,04 |  |
| 13 | Buchhaltungsspezifische Daten (Anzahlung, Wertberichtigung udgl.) | intern | 7J | 03,04 |  |
| 14 | Daten zur Kostenrechnung | intern | 7J | 01 |  |
|  |  |  |  |  |  |

* 1. Externe Trainer  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | Löschfrist | Empfänger, siehe 3.2. | Anmerkung |
| 01 | Name | Person | 7J | 01-04 | § 212 UGB, § 132 BAO |
| 02 | Postadresse und Kontaktdaten | Person | 7J | 01-04 |  |
| 04 | Vertragsnummer | intern | 7J | 01-04 |  |
| 05 | Bankverbindung | Person | 7J | 02,03 |  |
| 06 | Zahlungskonditionen | intern | 7J | 03,04 |  |
| 07 | Eingangsrechnungen | intern | 7J | 01-04 |  |
| 08 | Zahlungen | intern | 7J | 02-04 |  |
| 09 | offene Posten | intern | 7J | 01,03,04 |  |
| 11 | Bonität | KSV | 7J | 01 |  |
| 12 | Daten zur Akquisition (Provisionen etc) | intern | 7J | 01,03,04 |  |
| 13 | Daten zur Steuerberechnung (USt-Pflicht, UID-Nr. etc) | Person | 7J | 03,04 |  |
| 14 | Buchhaltungsspezifische Daten (Anzahlung, Wertberichtigung udgl.) | intern | 7J | 03,04 |  |
| 15 | Daten zur Kostenrechnung | intern | 7J | 01 |  |
|  |  |  |  |  |  |

* 1. Sonstige Geschäftspartner  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | | Löschfrist | | Empfänger, siehe 3.2. | Anmerkung | |
| 01 | Name, Firma | | Person | | 7J | 01-04 | | § 212 UGB § 132 BAO |
| 02 | Postadresse und Kontaktdaten | | Person | | 7J | 01-04 | |  |
| 03 | Kontaktperson | | Person | | 7J | 01 | |  |
| 04 | Kundennummer | | intern | | 7J | 01-04 | |  |
| 05 | Bankverbindung | | Person | | 7J | 02-04 | |  |
| 06 | Eingangsrechnungen (alle Rechnungsdaten) | | Person | | 7J | 01-04 | |  |
| 07 | Zahlungen | | intern | | 7J | 02-04 | |  |
| 08 | offene Posten | | intern | | 7J | 01,03,04 | |  |
| 09 | Bonität | | KSV | | 7J | 01 | |  |
|  |  | |  | |  |  | |  |

* 1. Kontaktpersonen  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | Löschfrist | Empfänger  siehe 3.2. | Anmerkung |
| 01 | Name | Person | 5J | 04 |  |
| 02 | Firma, Funktion | Person | 5J | 04 |  |
| 03 | Postadresse | Person | 5J | 04 |  |
| 04 | Kontaktdaten inkl. TelNr. | Person | 5J | 04 |  |
|  |  |  |  |  |  |

1. Technisch-organisatorische Maßnahmen (TOMs)
   1. Applikationen  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Applikation | Auftragsverarbeiter | Maßnahmen |
| 01 | zB BMD | Steuerberater | siehe Richtlinie für die Vergabe von User-Berechtigungen |
| 02 | Telebanking (zB ELBA) |  | 4-Augenprinzip bei Freigabe von Zahlungsaufträgen |
|  |  |  |  |

* 1. Datenschutz durch Technologiegestaltung („privacy by design“) ist gewährleistet durch:
* Restriktive Zugriffsberechtigungen
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Datenschutz durch datenminimierende Voreinstellungen („privacy by default“) ist gewährleistet durch:
* Grundeinstellungen in der BMD-Software
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Datensicherheit (Vertraulichkeit, Verfügbarkeit, Integrität)

Elektronische Verarbeitungen

* Verschlüsselung sämtlicher Datenträger auf denen personenbezogene Daten gespeichert werden;
* Verschlüsselung bei Übermittlungen an Auftragsverarbeiter oder Behörden;
* Mehrstufige Systemsicherungen (B2D2T). Sämtliche Sicherungsdaten sind ebenfalls verschlüsselt und die Aufbewahrung der Archivbänder erfolgt georedundant.
* Hohe Sicherungsmechanismen im Bereich der Netzwerktechnologie. Physisch getrenntes WLAN für Kunden.
* Regelmäßige Überprüfung der Maßnahmen durch den Datenschutzverantwortlichen und den Auftragsverarbeiter.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

Analoge Verarbeitungen

* Strukturierte Sammlungen von personenbezogenen Daten werden nicht für jedermann zugänglich aufbewahrt: in versperrbaren Schränken bzw. Räumen zu denen nur berechtigte Mitarbeiter Zugang haben.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Methoden zur Datenlöschung

Elektronische Verarbeitungen

* Die eingesetzten Applikationen (allenfalls ergänzt durch spezielle Software-Tools wie zB Tealium) gewährleisten, dass sämtliche elektronisch erfasste Datenkategorien mit entsprechenden Tags versehen werden. Dadurch wird die automatische Löschung bzw. Anonymisierung einzelner Datenkategorien, nach Wegfall der Rechtsgrundlage zur Verarbeitung, ermöglicht.
* Betroffenenbegehren auf Löschung von Buchhaltungsdaten sind unzulässig.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

Analoge Verarbeitungen

* Da kein strukturierter Zugriff auf Papierakten, zB in Form einer dezentralen Abfrage bestimmter personenbezogener Daten, möglich ist, ist eine langfristige Aufbewahrung zur Beweissicherung bis maximal 10 Jahre nach dem letzten Kontakt gerechtfertigt.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

1. Profiling

* Nein
* Ja, und zwar:

(Zutreffendes ankreuzen oder ergänzen.)

1. Entscheidungsautomatisierung

* Nein
* Ja, und zwar:

Automatische Mahnläufe an Kunden, bei Überschreitung bestimmter Zahlungsziele.

Sperre von Kunden für Buchungen bei negativer Bonität oder Überziehung von Zahlungszielen.

Sperre von Geschäftspartnern bei Insolvenz.

Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

1. Betroffenenrechte
   1. Information Betroffener

* Standardformat: PDF
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Art der Information des Betroffenen
* E-Mail, wenn Anfrage per E-Mail, sonst per Post
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

1. PERSONALWESEN

1. Verfahren

Bezeichnung: Personalwesen

Fachabteilung: Personalabteilung / HR

Kontakt: [Name des Abteilungsleiters]

1. Zweckbestimmung

Erfüllung der Aufgaben eines ordnungsgemäßen Personalwesens einschließlich Recruiting und Personalentwicklung, Schulung und Training

1. Details zur Datenverarbeitung
   1. Betroffene Personen  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |
| --- | --- | --- |
|  | Personengruppe | Anmerkung |
| 01 | Mitarbeiter |  |
| 02 | externe Trainer |  |
| 03 | Bewerber |  |
|  |  |  |

* 1. Datenverwendung & Weitergabe

Verwendung intern

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
| 01 | Fachabteilung | Vertrag, Einwilligung, Betriebsvereinbarung, Kollektivvertrag |
| 02 | Sicherheitsdienst | Einwilligung, Betriebsvereinbarung, Kollektivvertrag |
| 03 | Rechnungswesen |  |
|  |  |  |

Weitergabe extern

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
| 04 | Banken | Vertrag |
| 05 | Steuerberatung, Rechtsanwälte | Abwägung 1) |
| 06 | Gerichte, Behörden | Gesetz |
| 07 | Betreibende Gläubiger | Drittschuldnererklärung |
| 08 | Weiterbildungs- und Schulungseinrichtungen | Vertrag, Einwilligung |

1. Interesse des Verarbeiters an steuerlicher, rechtlicher und sonstiger Beratung überwiegt das Geheimhaltungsinteresse des Betroffenen, wenn die Empfänger zur Verschwiegenheit gegenüber Dritten gesetzlich oder vertraglich verpflichtet sind.

Weitergabe Drittstaaten

Nein

* 1. Auftragsverarbeiter

Firma [genauer Firmenname]

Adresse [Postanschrift]

Kontaktperson [Name, E-Mail, TelNr.]

Vertragsnummer

(Mehrere Auftragsverarbeiter gesondert anführen.)

1. Datenkategorien
   1. Mitarbeiter  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | Löschfrist | Empfänger, siehe 3.2. | Anmerkung |
| 01 | Name, Geburtsdatum | Person | 30J | 01  02—07,08 | § 1478 ABGB |
| 02 | SozVersNr | Person | 30J | 01  02-07 | § 1478 ABGB |
| 03 | Postadresse | Person | 30J | 01  02-07 | § 1478 ABGB |
| 04 | Familienstand, Name des Partners, Anzahl und Namen der Kinder | Person | 5J | 01,03,05-07 |  |
| 05 | Religionsbekenntnis | Person | 5J | 01 | sensibel |
| 06 | Beginn, Ende Dienstverhältnis | intern | 30J | 01  02,03,05-07 | § 1478 ABGB |
| 07 | Bankverbindung | Person | 5J | 03,05,06 |  |
| 08 | Kontaktdaten inkl. TelNr. | Person | 5J | 01,02,03,08 |  |
| 09 | Staatsangehörigkeit | Person | 5J | 01,03,05,06 |  |
| 10 | Ausbildung, Qualifikation, Einstufung | Person | 30J | 01  03,08 | § 1478 ABGB |
| 11 | Arbeitsplatzbeschreibung | intern | 30J | 01  03,05,08 | § 1478 ABGB |
| 12 | Dienstvertrag | intern | 30J | 01,03,05 |  |
| 13 | Bruttogehalt/lohn; Lohnzettel | intern | 5J | 01,03,05,06 | Netto-Bezug für Drittschuldner |
| 14 | Boni, Provisionen, Dienst-PKW | intern | 5J | 01,03,05,06 |  |
| 15 | Arbeitszeiten Plan und Ist | intern | 5J | 01,03,05 |  |
| 16 | Dienst-PKW | intern | 5J | 01,03,05,06 |  |
| 17 | Abrechnung KM-Geld | intern | 5J | 01,03,05,06 |  |
| 18 | Abrechnung Reisespesen, Diäten | intern | 5J | 01,03,05,06 |  |
| 19 | Gewerkschaftszugehörigkeit | Person, Betriebsrat | 5J | 01,05 | sensibel |
| 20 | Buchhaltungsspezifische Daten (Vordienstzeiten, Urlaubsanspruch udgl.) | intern | 7J | 01,03,05 |  |
| 21 | Krankenstände | intern | 5J | 01,03,05 | sensibel |
| 22 | Quantitative Leistungsparameter | intern | 5J | 01 | arbeitsrechtl. sensibel |
| 23 | Qualitative Leistungsparameter | intern | 5J | 01 | arbeitsrechtl. sensibel |
| 24 | Softwarespezifische Nutzungsdaten (Protokoll-Daten) | intern | 5J | 01,02 | arbeitsrechtl. sensibel |
| 25 | Zutrittsdaten zu bestimmten Räumlichkeiten | intern | 5J | 01,02 | arbeitsrechtl. sensibel |
| 26 | Privates Umfeld, Interessen | Person | 3M | 01,02 |  |
| 27 | Daten über Aussehen und Gesundheitszustand | intern | 3M | 02 | sensibel |
| 28 | biometrische Daten | intern | 3M | 02 | sensibel |
|  |  |  |  |  |  |

* 1. Externe Trainer  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | Löschfrist | Empfänger, siehe 3.2. | Anmerkung |
| 01 | Name, Geburtsdatum | Person | 5J | 01-06 |  |
| 02 | SozVersNr | Person | 5J | 01-06 |  |
| 03 | Postadresse | Person | 5J | 01-06 |  |
| 04 | Beginn, Ende der Beschäftigung | intern | 5J | 01-03,05-06 |  |
| 05 | Kontaktdaten inkl. TelNr. | Person | 5J | 01-03 |  |
| 06 | Ausbildung, Qualifikation, Einstufung | Person | 5J | 01 |  |
| 07 | Arbeitsplatz-Beschreibung | intern | 5J | 01,03,05 |  |
| 08 | Arbeitszeiten Plan und Ist | intern | 5J | 01,03,05 |  |
| 09 | Quantitative Leistungsparameter | intern | 5J | 01 | arbeitsrechtl. sensibel |
| 10 | Qualitative Leistungsparameter | intern | 5J | 01 | arbeitsrechtl. sensibel |
| 11 | Abrechnung Reisespesen, Diäten | intern | 5J | 01,03,05,06 |  |
| 11 | Softwarespezifische Nutzungsdaten (Protokoll-Daten) | intern | 5J | 01,02 | arbeitsrechtl. sensibel |
| 12 | Zutrittsdaten zu bestimmten Räumlichkeiten | intern | 5J | 01,02 | arbeitsrechtl. sensibel |
| 13 | Daten über Aussehen und Gesundheitszustand | intern | 3M | 02 | sensibel |
| 14 | biometrische Daten | intern | 3M | 02 | sensibel |
|  |  |  |  |  |  |

* 1. Bewerber  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | | Löschfrist | | Empfänger, siehe 3.2. | Anmerkung |
| 01 | Name, Geburtsdatum | Person | | 6M | | 01 | § 29 Abs 1 GlBG |
| 02 | Postadresse | Person | | 6M | | 01 | § 29 Abs 1 GlBG |
| 03 | Familienstand, Name des Partners, Anzahl und Namen der Kinder | Person | | 6M | | 01 | § 29 Abs 1 GlBG |
| 04 | Religionsbekenntnis | Person | | 6M | | 01 | sensibel, § 29 Abs 1 GlBG |
| 05 | Möglicher Beginn des Dienstverhältnisses | Person | | 6M | | 01 | § 29 Abs 1 GlBG |
| 06 | Kontaktdaten inkl. TelNr. | Person | | 6M | | 01 | § 29 Abs 1 GlBG |
| 07 | Staatsangehörigkeit | Person | | 6M | | 01 | § 29 Abs 1 GlBG |
| 08 | Ausbildung, Qualifikation, Einstufung | Person | | 6M | | 01 | § 29 Abs 1 GlBG |
| 09 | Wunsch-Bruttogehalt/lohn | Person | | 6M | | 01 | § 29 Abs 1 GlBG |
| 10 | Privates Umfeld, Interessen | | Person | 6M | 01,02 | | § 29 Abs 1 GlBG |
| 11 | Frühere Dienstgeber | Person | | 6M | | 01 | § 29 Abs 1 GlBG |
| 12 | Wunsch-Arbeitsplatz | Person | | 6M | | 01 | § 29 Abs 1 GlBG |
| 13 | Daten über Aussehen und Gesundheitszustand |  | | 6M | | 01,02 | sensibel, § 29 Abs 1 GlBG |
|  |  |  | |  | |  | § 29 Abs 1 GlBG |

1. Technisch-organisatorische Maßnahmen (TOMs)
   1. Applikationen  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Applikation | Auftragsverarbeiter | Maßnahmen |
| 01 | HR-Software |  | siehe Richtlinie für die Vergabe von User-Berechtigungen |
|  |  |  |  |

* 1. Datenschutz durch Technologiegestaltung („privacy by design“) ist gewährleistet durch:
* Restriktive Zugriffsberechtigungen; arbeitsrechtlich oder datenschutzrechtlich sensible Daten werden besonders geschulten und qualifizierten Personen zugänglich gemacht.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Datenschutz durch datenminimierende Voreinstellungen („privacy by default“) ist gewährleistet durch:
* Grundeinstellungen in der HR-Software
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Datensicherheit (Vertraulichkeit, Verfügbarkeit, Integrität)

Elektronische Verarbeitungen

* Verschlüsselung sämtlicher Datenträger auf denen personenbezogene Daten gespeichert werden;
* Verschlüsselung bei Übermittlungen an Auftragsverarbeiter oder Behörden;
* Mehrstufige Systemsicherungen (B2D2T). Sämtliche Sicherungsdaten sind ebenfalls verschlüsselt und die Aufbewahrung der Archivbänder erfolgt georedundant.
* Hohe Sicherungsmechanismen im Bereich der Netzwerktechnologie. Physisch getrenntes WLAN für Kunden.
* Regelmäßige Überprüfung der Maßnahmen durch den Datenschutzverantwortlichen und den Auftragsverarbeiter.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

Analoge Verarbeitungen

* Strukturierte Sammlungen von personenbezogenen Daten werden nicht für jedermann zugänglich aufbewahrt: in versperrbaren Schränken bzw. Räumen zu denen nur berechtigte Mitarbeiter Zugang haben.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Methoden zur Datenlöschung

Elektronische Verarbeitungen

* Die eingesetzten Applikationen (allenfalls ergänzt durch spezielle Software-Tools wie zB Tealium) gewährleisten, dass sämtliche elektronisch erfasste Datenkategorien mit entsprechenden Tags versehen werden. Dadurch wird die automatische Löschung bzw. Anonymisierung einzelner Datenkategorien, nach Wegfall der Rechtsgrundlage zur Verarbeitung, ermöglicht.
* Betroffenenbegehren auf Löschung von Buchhaltungsdaten sind unzulässig.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

Analoge Verarbeitungen

* Strukturierte Sammlungen von personenbezogenen Daten werden nach der angegebenen Aufbewahrungsfrist vernichtet.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

1. Profiling

* Nein
* Ja, und zwar durch:
  + Performance-Analyse der Mitarbeiter

(Zutreffendes ankreuzen oder ergänzen)

1. Entscheidungsautomatisierung

* Nein
* Ja, und zwar:

(Zutreffendes ankreuzen oder ergänzen.)

1. Betroffenenrechte
   1. Information Betroffener

* Standardformat: PDF
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Art der Information des Betroffenen
* E-Mail, wenn Anfrage per E-Mail, sonst per Post
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

1. Korrespondenz

1. Verfahren

Bezeichnung: Korrespondenz

Fachabteilung: Alle

Kontakt: [Name des Leiters Verwaltung]

1. Zweckbestimmung

Gesamte geschäftliche Korrespondenz mit Mitarbeitern, Kunden, Interessenten, externen Trainern, sonstigen Geschäftspartnern, Behörden, Gerichten etc.

1. Details zur Datenverarbeitung
   1. Betroffene Personen  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |
| --- | --- | --- |
|  | Personengruppe | Anmerkung |
| 01 | Kunden |  |
| 02 | Interessenten |  |
| 03 | Geschäftspartner | einschließlich externe Trainer |
| 04 | Kontaktpersonen |  |
| 05 | Mitarbeiter |  |
| 06 | Bewerber |  |

* 1. Datenverwendung & Weitergabe  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

Verwendung intern

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
| 01 | Rechtsabteilung | Abwägung 1) |
| 02 | Rechnungswesen | Gesetz |
|  |  |  |

1. Interesse des Verarbeiters an rechtlicher Prüfung der Korrespondenz überwiegt in der Regel das Geheimhaltungsinteresse des Betroffenen.

Weitergabe extern

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
| 03 | Leistungsträger | Vertrag |
| 04 | Steuerberatung, Rechtsanwälte | Abwägung 1) |
| 05 | Gerichte, Behörden | Gesetz |
| 06 | externe Berater | Abwägung 1) |
| 07 | sonstige Dritte | Vertrag, Abwägung 2) |
|  |  |  |

1. Das Interesse des Verarbeiters an steuerlicher, rechtlicher und sonstiger Beratung überwiegt das Geheimhaltungsinteresse des Betroffenen, wenn die Empfänger zur Verschwiegenheit gegenüber Dritten gesetzlich oder vertraglich verpflichtet sind.
2. Die Weitergabe von Korrespondenz an Dritte kann zur Vertragserfüllung notwendig sein. In Einzelfällen wird eine Interessensabwägung vorgenommen, ob das Interesse des Betroffenen an der Geheimhaltung das Interesse des Verantwortlichen an der Weitergabe überwiegt.

Weitergabe Drittstaaten

Nein.

* 1. Auftragsverarbeiter  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

Firma zB Microsoft Ireland Operations Ltd

Adresse Atrium Building Block B, Carmanhall Road Sandyford Industrial Estate   
Dublin 18, Irland

Kontaktperson nicht bekannt.

Vertragsnummer

(Mehrere Auftragsverarbeiter gesondert anführen.)

1. Datenkategorien
   1. Endkunden, Interessenten, Geschäftspartner, Kontaktpersonen, Mitarbeiter, Bewerber  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | Löschfrist | Empfänger, siehe 3.2. | Anmerkung |
| 01 | Korrespondenz Eingang | Betroffener | 5J |  |  |
| 02 | Korrespondenz Ausgang | intern | 5J |  |  |
| 03 |  |  |  |  |  |

1. Technisch-organisatorische Maßnahmen (TOMs)
   1. Applikationen  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Applikation | Auftragsverarbeiter | Maßnahmen |
| 01 | zB Office 365 | zB Microsoft | siehe Richtlinie für die Vergabe von User-Berechtigungen für die zB Microsoft Cloud |
| 02 | zB Outlook |  | nur persönliche Konten, generelle Rechte-Policy für lokale Mailboxen |

* 1. Datenschutz durch Technologiegestaltung („privacy by design“) ist gewährleistet durch:
* Restriktive Zugriffs- und Vertretungsberechtigungen.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Datenschutz durch datenminimierende Voreinstellungen („privacy by default“) ist gewährleistet durch:
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Datensicherheit (Vertraulichkeit, Verfügbarkeit, Integrität)

Elektronische Verarbeitungen

* Verschlüsselung sämtlicher Datenträger auf denen Korrespondenz einschließlich E-Mails gespeichert werden;
* Verschlüsselung bei Übermittlungen von Korrespondenz an Empfänger, Auftragsverarbeiter oder Dritte;
* Mehrstufige Systemsicherungen (B2D2T). Sämtliche Sicherungsdaten sind ebenfalls verschlüsselt und die Aufbewahrung der Archivbänder erfolgt georedundant.
* Hohe Sicherungsmechanismen im Bereich der Netzwerktechnologie. Physisch getrenntes WLAN für Kunden.
* Regelmäßige Überprüfung der Maßnahmen durch den Datenschutzverantwortlichen und den Auftragsverarbeiter.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

Analoge Verarbeitungen

* Strukturierte Sammlungen von personenbezogenen Daten werden nicht für jedermann zugänglich aufbewahrt: in versperrbaren Schränken bzw. Räumen zu denen nur berechtigte Mitarbeiter Zugang haben.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Methoden zur Datenlöschung

Elektronische Verarbeitungen

* Die Fachabteilungen haben Richtlinien erlassen, nach welchen Kriterien Korrespondenz einschließlich E-Mail-Verkehr aufzubewahren bzw zu löschen ist. Soferne sich daraus nichts anderes ergibt, wird sämtliche Korrespondenz, die keinen längeren gesetzlichen Aufbewahrungsfristen unterliegt, 5 Jahre nach dem letzten Kontakt gelöscht. Diese Frist ergibt sich aus der Frist für die Verjährung von Schadenersatzforderungen von drei Jahren (§ 1489 ABGB) und einem Sicherheitsaufschlag für Schäden, die erst mit Verzögerung bekannt werden.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

Analoge Verarbeitungen

* Strukturierte Sammlungen von personenbezogenen Daten werden nach der angegebenen Aufbewahrungsfrist vernichtet.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

1. Profiling

* Nein
* Ja, und zwar durch:

(Zutreffendes ankreuzen oder ergänzen)

1. Entscheidungsautomatisierung

* Nein
* Ja, und zwar:

(Zutreffendes ankreuzen oder ergänzen.)

1. Betroffenenrechte
   1. Information Betroffener

* Standardformat: PDF
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Art der Information des Betroffenen
* E-Mail, wenn Anfrage per E-Mail, sonst per Post
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

1. Videoüberwachung

(Datenschutz-Folgenabschätzung zwingend erforderlich !)

1. Verfahren

Bezeichnung: Videoüberwachung

Fachabteilung: Security

Kontakt: [Name des Abteilungsleiters]

1. Zweckbestimmung

Vorbeugender Schutz von Personen und Sachen, insbesondere des Eigentums der Kunden und des Verantwortlichen durch Bildaufzeichnungen (Video-Überwachung) aller Trainingsbereiche.

1. Details zur Datenverarbeitung
   1. Betroffene Personen  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |
| --- | --- | --- |
|  | Personengruppe | Anmerkung |
| 01 | Kunden |  |
| 02 | Interessenten |  |
| 03 | Geschäftspartner |  |
| 05 | Mitarbeiter inkl. externer Trainer |  |
| 06 | Bewerber |  |
|  |  |  |

* 1. Datenverwendung & Weitergabe  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

Verwendung intern

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
| 01 | Rechtsabteilung | Abwägung 1) |
| 02 | Personalabteilung / HR | Einwilligung |
|  |  |  |

1. Interesse des Verarbeiters an rechtlicher Prüfung der mit Überwachungskameras aufgezeichneter Vorgänge überwiegt das Geheimhaltungsinteresse des Betroffenen.

Weitergabe extern

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
| 03 | Gerichte, Behörden | Gesetz |
| 04 | externe Berater | Abwägung 1) |
|  |  |  |

1. Interesse des Verarbeiters an fachlicher Prüfung, zB zur Beweissicherung oder technischer Analyse von aufgezeichneten Videodaten überwiegt das Geheimhaltungsinteresse des Betroffenen, wenn der Empfänger zur Verschwiegenheit gegenüber Dritten gesetzlich oder vertraglich verpflichtet ist.

Weitergabe Drittstaaten

Nein.

* 1. Auftragsverarbeiter  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

Firma [genauer Firmenname]

Adresse [Postanschrift]

Kontaktperson [Name, E-Mail, TelNr.]

Vertragsnummer

1. Datenkategorien
   1. Kunden, Interessenten, Geschäftspartner, Kontaktpersonen, Mitarbeiter, Bewerber  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | Löschfrist | Empfänger, siehe 3.2. | Anmerkung |
| 01 | Video-Aufzeichnung von Überwachungskameras (Bildaufnahmen) | intern | 72 Stunden |  | § 13 DSG |
| 02 | Standbilder von Überwachungskameras | intern | 72 Stunden |  | § 13 DSG |
| 03 |  |  |  |  |  |

1. Technisch-organisatorische Maßnahmen (TOMs)
   1. Applikationen  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Applikation | Auftragsverarbeiter | Maßnahmen |
| 01 |  |  |  |
| 02 |  |  |  |

* 1. Datenschutz durch Technologiegestaltung („privacy by design“) ist gewährleistet durch:
* Der Zugang zur den Bildaufnahmen ist auf eigens geschulte Mitarbeiter der Security-   
  Abteilung beschränkt. Eine nachträgliche Veränderung der Aufnahmen ist ausgeschlossen   
  (§ 13 DSG).
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Datenschutz durch datenminimierende Voreinstellungen („privacy by default“) ist gewährleistet durch:
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Datensicherheit (Vertraulichkeit, Verfügbarkeit, Integrität)

Elektronische Verarbeitungen

* Verschlüsselung sämtlicher Datenträger auf denen Bildaufnahmen (Aufzeichnungen von Überwachungskameras) gespeichert werden;
* Verschlüsselung bei Übermittlungen von Bildaufnahmen an Empfänger, Auftragsverarbeiter oder Dritte;
* Hohe Sicherungsmechanismen im Bereich der Netzwerktechnologie. Physisch getrenntes WLAN für Kunden.
* Regelmäßige Überprüfung der Maßnahmen durch den Datenschutzverantwortlichen und den Auftragsverarbeiter.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

Analoge Verarbeitungen

* Ausdrucke von Bildaufnahmen werden nur im Anlassfall angelegt.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Methoden zur Datenlöschung

Elektronische Verarbeitungen

* Aufzeichnungsdaten werden automatisch 72 Stunden nach der Aufnahme gelöscht, wenn nicht nach einem Vorfall bestimmte Daten bis zur endgültigen (allenfalls gerichtlichen) Klärung des Vorfalls gespeichert werden.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

Analoge Verarbeitungen

* Analoge Auswertungen von Überwachungsdaten werden bis zur endgültigen (allenfalls gerichtlichen) Klärung des Vorfalls aufbewahrt.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

1. Profiling

* Nein
* Ja, und zwar durch:

(Zutreffendes ankreuzen oder ergänzen)

1. Entscheidungsautomatisierung

* Nein
* Ja, und zwar:

(Zutreffendes ankreuzen oder ergänzen.)

1. Betroffenenrechte
   1. Information Betroffener

* Nur die Tatsache einer Aufzeichnung wird bekanntgegeben, nicht aber die Aufzeichnung selbst.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Art der Information des Betroffenen
* E-Mail, wenn Anfrage per E-Mail, sonst per Post
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)