****

**Gerhard Frank**

**ims media gmbh**

**m:+ 43 650 88 99 1 99 | e:office@ims-media.at |**

**w:www.ims-media.at | a:1220 Wien , Hagedornweg 73a**

**Datenverarbeitungsverzeichnis nach Art 30 Abs 1 EU-Datenschutz-Grundverordnung (DSGVO)**

**(Verantwortlicher)**

**Inhalt**

1. **Stammdatenblatt: Allgemeine Angaben**
2. **Datenverarbeitungen/Datenverarbeitungszwecke**
3. **Detailangaben zu den einzelnen Datenverarbeitungszwecken**
4. **Allgemeine Beschreibung organisatorisch-technischer Maßnahmen**
5. **Stammdatenblatt**

**Name und Kontaktdaten des für die Verarbeitung Verantwortlichen:**

* 1. **Name(n) und Anschrift(en):**

**Ims media gmbH, Gerhard Frank, 1220 Wien , Hagedornweg 73a**

* 1. **E-Mail-Adresse(n) (und allenfalls weitere Kontaktdaten wie zB Tel.Nr.):**

**office@ims-media.at** **, + 43 650 88 99 1 99**

* 1. **Name und Kontaktdaten Datenschutzkoordinator:**

**Gerhard Frank, + 43 650 88 99 1 99**

* 1. **Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Vertreters des (der) Verantwortlichen:[[1]](#footnote-1)**

**Ims media gmbH, Anika Frank, 1220 Wien , Hagedornweg 73a**

**office@ims-media.at** **, + 43 660 314 77 13**

1. **Datenverarbeitungen/Datenverarbeitungszwecke**
2. **Zwecke und Beschreibung der Datenverarbeitung[[2]](#footnote-2):**
	1. **Rechnungswesen und Geschäftsabwicklung:** Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit Kunden und Lieferanten, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zB Korrespondenzen oder Verträge) in diesen Angelegenheiten
	2. **Personalverwaltung**: Verarbeitung und Übermittlung von Daten für die Personalplanung, Personalanstellung, Personalentlohnung sowie die Personalentwicklung und die damit verbundenen Verarbeitungen und Übermittlungen für Lohn-, Gehalts-, Entgeltsverrechnung und Einhaltung von arbeits- und sozialrechtlich vorgegebener Aufzeichnungs-, Auskunfts- und Meldepflichten, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (zB Korrespondenzen, Bewerbungsschreiben, Dienstzeugnisse, Testergebnisse, Stellenbeschreibungen) in diesen Angelegenheiten
	3. **Geschäftspartnerdatenbank:** Online my-bookings.org (nur B2B Kunden)
	4. **Kundendatenbank:** Online – Buchungsverwaltung (my-bookings.org)
	5. **Marketing:** keine online Aktivitäten
3. **Wurde eine Datenschutz-Folgenabschätzung durchgeführt?[[3]](#footnote-3)**

**Ja 🞎 Nein 🞎**

**Wenn Ja, wann? Anfang 2018 mündlich mit Anika Frank**

**Wenn Nein, aus welchem Grund nicht?[[4]](#footnote-4)**

1. **Kategorien der betroffenen Personen**

Lfd.Nr. *Beschreibung der Kategorien betroffener Personen (zB Kunden, Mitarbeiter, Lieferanten usw.)*

1 Kunden und Lieferanten inkl. Kontaktpersonen beim Kunden und Lieferanten

2 Mitarbeiter

3 *Lieferanten*

4 Gäste

5 An der Geschäftsabwicklung mitwirkende Dritte inkl. Kontaktpersonen bei den Dritten

1. **Rechtsgrundlagen[[5]](#footnote-5)**

Art 6 Abs 1 lit a (Einwilligung der Betroffenen), lit b (zur Vertragserfüllung erforderlich), lit c (gesetzliche Verpflichtungen nach der BAO und dem UGB), lit f (berechtigte Interessen des Verantwortlichen) DSGVO § 132 BAO §§ 190, 212 UGB

1. **Verträge , Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten[[6]](#footnote-6)) sind abgelegt:***[[7]](#footnote-7)* **(freiwillig)**

Unterlagen zu aufrechten Geschäftsabwicklungen in der Verkaufsabteilung, Rechnungen (auch) in der Finanzabteilung, erledigte Geschäftsfälle im Archiv. Verträge mit Auftragsverarbeitern sind, je nach Thematik, in der Rechtsabteilung, Finanzabteilung, Vertriebsabteilung oder IT-Abteilung abgelegt.

1. **Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen[[8]](#footnote-8)**
	1. **Kategorien der verarbeiteten Daten und ankreuzen, ob sie an Empfänger[[9]](#footnote-9) übermittelt werden**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes** | **Lfd. Nr.** | **Datenkategorien** | **Besondere Datenkategorien iSd Art 9 DSGVO[[10]](#footnote-10), strafrechtlich relevant iSd Art 10 DSGVO[[11]](#footnote-11)** | **Steurberater** | **Banken / Kreditkarteninstitute** | **Behörden** | **Versicherung im Anlassfall** | **Rechtsvertreter im Geschäftsfall** | **Mitwirkende Vertrags- und Geschäftspartner** |
| **ALLE** | 1 | *Name, Firma oder sonstige**Geschäftsbezeichnung* | *Nein* | *X* | *X* | *X* | *X* | *X* | *X* |
| 2 | *Anschrift* | *Nein* | *X* | *X* | *X* | *X* | *X* | *X* |
| 3 | *Kontaktdaten* | *Nein* | *X* | *X* | *X* | *X* | *X* | *X* |
| 4 | *Kreditkartennummern und -**unternehmen* | *Nein* | *X* | *X* | *X* |  | *X* | *X* |
|  | 5 | Passdaten | Ja | *X* | *X* | *X* |  | *X* |  |
| 6 | Kontodaten | *Nein* | *X* | *X* | *X* |  | *X* |  |
| 7 | Geburtsdaten | Ja | *X* | *X* | *X* |  | *X* |  |
| 8 | Persönliche Mitarbeiter-daten | Ja | *X* | *X* | *X* |  | *X* |  |
| 9 | Bankverbindungen | *Nein* | *X* | *X* | *X* | *X* | *X* | *X* |
| 10 | UID-Nummer / Firmenbuchnr. | *Nein* | *X* | *X* | *X* | *X* | *X* | *X* |

* 1. **Löschungs- und Aufbewahrungsfristen (wenn möglich)**

|  |  |
| --- | --- |
| **Daten aus 4.a. (Lfd. Nr.)** | **Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen** |
| ALLE Details auf: <https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html> ) | Aufgrund der gesetzlichen Aufbewahrungs- fristen auf jeden Fall 7 Jahre; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristenoder bei B2B-Geschäfts-beziehungen bis zur Beendigung der Geschäftsbeziehung. |

1. **Kategorien von Empfängern[[12]](#footnote-12), an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern[[13]](#footnote-13)**
	1. **Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation wie zB UNO, OSZE)**

|  |  |  |
| --- | --- | --- |
| **Empfängerkategorien bzw. Empfänger in Drittstaaten oder Internationalen Organisationen (aus 4.a.)** | **Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)** | **Internationale Organisation (Angabe der intern. Organisation)** |
| SteuerberaterBanken / KreditkarteninstituteBehörden Versicherung im Anlassfall Rechtsvertreter im Geschäftsfall Mitwirkende Vertrags- und Geschäftspartner | Keine | Keine |

* 1. **Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Abs 1 Unterabsatz 1 DSGVO erfolgt** (vor allem wenn kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, keine Standardvertragsklauseln der Europäischen Kommission oder der nationalen Datenschutzbehörde verwendet werden oder genehmigte Zertifizierungsmechanismen in Anspruch genommen werden, keine Corporate binding rules zur Anwendung kommen (genehmigte verbindliche konzerninterne Datenschutzvorschriften), die Übermittlung nicht für Vertragserfüllungszwecke erforderlich ist oder keine ausdrückliche Einwilligung vorliegt)**:**

**Es werden keine personenbezogenen Daten in Drittländer übertragen.**

1. **Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen**
	1. **Vertraulichkeit[[14]](#footnote-14):**

i. Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch Schlüssel

ii. Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch sichere Kennwörter (einschließlich entsprechender Policy)

iii. Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, da Zugriff nur für Unternehmensinhaber und Mitarbeiter / Partner, die an der Geschäftsabwicklung beteiligt sind

* 1. **Verfügbarkeit und Belastbarkeit:**

 Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust: durch regelmäßige Backups, Einsatz eines aktuellen Virenschutzes und einer Firewall

* 1. **Pseudonymisierung:**

Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.

* 1. **Evaluierungsmaßnahmen:**

 Datenschutz-Management durch regelmäßige Kontrollen.

1. [↑](#footnote-ref-1)
2. Zum Begriff „Verarbeitung“ siehe das Merkblatt [„Wichtige Begriffsbestimmungen“](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung%3A-Wichtige-Begriffsbestimmu.html); sollten Daten auch an „Dritte“ oder an Auftragsverarbeiter übermittelt werden, sind auch die Zwecke dieser Datenübermittlungen im Verarbeitungsverzeichnis zu dokumentieren. [↑](#footnote-ref-2)
3. Zur Datenschutz-Folgenabschätzung siehe das Merkblatt „[Datenschutz-Folgenabschätzung](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-datenschutz-grundverordnung-datenschutz-folgenabschaetzu.html)“. Im Verarbeitungsverzeichnis sind zwar Angaben zur Datenschutz-Folgenabschätzung nicht zwingend vorgesehen. Aus Gründen der Rechenschaftspflicht empfehlen sich aber grundsätzliche Angaben darüber auch ins Verarbeitungsverzeichnis aufzunehmen. [↑](#footnote-ref-3)
4. Eine Datenschutz-Folgenabschätzung ist nicht durchzuführen, wenn durch die Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte der Betroffenen besteht oder die Datenverarbeitungsart in der sogenannten „white list“ der Datenschutzbehörde gelistet ist (derzeit besteht noch keine „white list“); Näheres dazu siehe auch das Merkblatt [„Datenschutz-Folgenabschätzung“](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-datenschutz-grundverordnung-datenschutz-folgenabschaetzu.html). [↑](#footnote-ref-4)
5. Die Rechtsgrundlagen (zB rechtliche Verpflichtung, Einwilligung, Vertragserfüllung, lebenswichtige Interessen des Betroffenen, kein überwiegendes berechtigtes Interesse des Betroffenen) sind nach der DSGVO zwar nicht verpflichtend ins Verarbeitungsverzeichnis aufzunehmen. Allerdings unterliegt der verantwortliche Verarbeiter einer sogenannten Rechenschaftspflicht. Diese besagt eine Nachweispflicht bzgl. der Einhaltung der Pflichten nach der DSGVO. Dazu gehört unter anderem auch der Nachweis, dass die Datenverarbeitung nach den in der DSGVO normierten Rechtmäßigkeitsgrundlagen erfolgt. Siehe das Merkblatt [„Grundsätze und Rechtmäßigkeit der Verarbeitung“](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung%3A-Grundsaetze-und-Rechtmaes.html). [↑](#footnote-ref-5)
6. Siehe zu den Informationspflichten das Merkblatt [„Informationspflichten“](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung%3A-Informationspflichten.html). [↑](#footnote-ref-6)
7. Die Angabe, wo die Unterlagen innerhalb der Organisation abgelegt wurden, ist nicht verpflichtend im Verarbeitungsverzeichnis zu dokumentieren, erleichtert aber vor allem in größeren, arbeitsteilig organisierten Organisationen das Auffinden der entscheidenden Unterlagen (dient also lediglich der innerbetrieblichen Arbeitserleichterung). [↑](#footnote-ref-7)
8. Nach der DSGVO sind die Löschfristen bzw. Aufbewahrungsfristen nach Möglichkeit ins Verarbeitungsverzeichnis aufzunehmen. Beispielsweise kann bei unbefristeten Verträgen keine konkrete Löschfrist angegeben werden, da der konkrete Vertragsablauf unbestimmt ist. Es empfiehlt sich hier allerdings eine abstrakte Frist anzugeben (zB „nach Ablauf des Vertrages“). [↑](#footnote-ref-8)
9. In der Rubrik „Empfänger“ sind nur die „Empfängerkategorien“ (zB „Gerichte“, „Banken“ oder „Sozialversicherungsträger“) einzutragen. Bei der Umschreibung der Empfängerkategorien ist darauf zu achten, dass eine Überprüfung der Rechtmäßigkeit ermöglicht wird (so wird zB die bloße Angabe von „Konzern“ als Empfänger nicht ausreichen, weil daraus nicht eruierbar sein wird, ob die Daten rechtmäßig an die Muttergesellschaft und/oder an Schwestergesellschaften übertragen werden). [↑](#footnote-ref-9)
10. Daten nach Art 9 DSGVO sind besondere Datenkategorien („sensible Daten): rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische und biometrische Daten zur Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung. [↑](#footnote-ref-10)
11. Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln unter behördlicher Aufsicht. [↑](#footnote-ref-11)
12. Es sind vor allem Übermittlungsempfänger („Dritte“) als auch Auftragsverarbeiter hier zu dokumentieren. Bei der Umschreibung der Empfängerkategorien ist darauf zu achten, dass eine Überprüfung der Rechtmäßigkeit ermöglicht wird (so wird zB die bloße Angabe von „Konzern“ als Empfänger nicht ausreichen, weil daraus nicht eruierbar sein wird, ob die Daten rechtmäßig an die Muttergesellschaft und/oder an Schwestergesellschaften übertragen werden). [↑](#footnote-ref-12)
13. Siehe dazu das Merkblatt [„Internationaler Datenverkehr“](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung%3A-Internationaler-Datenverk.html). Bei Empfängern in Drittstaaten (speziell in den USA wegen dem „Privacy Shield“-System) empfiehlt sich eine namentliche Nennung des Empfängers. [↑](#footnote-ref-13)
14. Verhinderung von (unbeabsichtigter) Offenlegung oder unbefugten Zugang zu personenbezogenen Daten. [↑](#footnote-ref-14)