

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

Inhalt

- A. Stammdatenblatt: Allgemeine Angaben**
- B. Datenverarbeitungen/Datenverarbeitungszwecke**
- C. Detailangaben zu den einzelnen Datenverarbeitungszwecken**
- D. Allgemeine Beschreibung organisatorisch-technischer
Maßnahmen**

A. Stammdatenblatt

Name und Kontaktdaten des (der) für die Verarbeitung (gemeinsam) Verantwortlichen

a. Name(n) und Anschrift(en):

Hotelbetriebsgesellschaft Metzler GmbH
Ziggamweg 227
6791 St. Gallenkirch

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

info@zamangspitze.at
Tel: 05557-6238
Fax: 05557-6238-5

c. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Datenschutzbeauftragten¹:

Keiner

d. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Vertreters des (der) Verantwortlichen:²

Keiner

¹ Sofern ein Datenschutzbeauftragter verpflichtend oder auf freiwilliger Basis bestellt wurde.

HINWEIS: Wenn keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht, der Verantwortliche aber freiwillig einen bestellen möchte, müssen trotzdem alle den Datenschutzbeauftragten betreffenden Bestimmungen der DSGVO eingehalten werden; möchte man das nicht, darf die bestellte Person nicht „Datenschutzbeauftragter“ genannt werden, sondern sollte eine andere Bezeichnung gewählt werden (zB „Datenschutzkoordinator“). Dieser kann, muss aber nicht ins Verarbeitungsverzeichnis aufgenommen werden. Siehe dazu das WKO-Merkblatt „[Datenschutzbeauftragter](#)“.

² Darunter sind Vertreter von nicht in der EU niedergelassenen Verantwortlichen zu verstehen.

B. Datenverarbeitungen/Datenverarbeitungszwecke

1. Zwecke und Beschreibung der Datenverarbeitung³:

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. Marketing:

Verarbeitung und Übermittlung von Daten für Werbezwecke

4. Gästedatenbank:

Verarbeitung von Daten zur Erstellung von Angeboten, Reservierungen

5. Mitarbeitersuche:

Verarbeitung und Übermittlung von Daten von Personen, welche Interesse an einer Anstellung bei der Hotelbetriebsges. Metzler GmbH haben (Lebenslauf und Bewerbungen)

6. Concierge:

Verarbeitung und Übermittlung von Daten für die Erstellung von Skipässen oder Montafon Brandnertal Card, sowie Buchung von geführten Touren von sportlichen Aktivitäten oder von geführten und nicht geführten Bergerlebnissen

2. Wurde eine Datenschutz-Folgenabschätzung durchgeführt?⁴

Ja Nein

Wenn Ja, wann?

Wenn Nein, aus welchem Grund nicht?⁵ Fehlende Voraussetzung

³ Zum Begriff „Verarbeitung“ siehe das Merkblatt [„Wichtige Begriffsbestimmungen“](#); sollten Daten auch an „Dritte“ oder an Auftragsverarbeiter übermittelt werden, sind auch die Zwecke dieser Datenübermittlungen im Verarbeitungsverzeichnis zu dokumentieren.

⁴ Zur Datenschutz-Folgenabschätzung siehe das Merkblatt [„Datenschutz-Folgenabschätzung“](#). 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.

⁵ 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“](#).

C. Detailangaben zu 1. (Einfügung der konkreten Datenverarbeitung aus dem B-Blatt, zB des Datenverarbeitungszweckes „Rechnungswesen“; das C-Blatt kann dann für jede der im B-Blatt angegebenen Datenverarbeitungszwecke verwendet werden, ohne dass die allgemeinen Angaben aus dem A- und B-Blatt wiederholt werden müssen)

1. Kategorien der betroffenen Personen

Lfd.Nr. Beschreibung der Kategorien betroffener Personen

- | | |
|---|---|
| 1 | Kunden und Lieferanten inkl. Kontaktpersonen beim Kunden und Lieferanten |
| 2 | ??Sachbearbeiter beim Verantwortlichen |
| 3 | An der Geschäftsabwicklung mitwirkende Dritte inkl. Kontaktpersonen bei den Dritten |

2. Rechtsgrundlagen⁶

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

3. Verträge , Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten⁷) sind abgelegt:⁸ (freiwillig)

Unterlagen zu aufrechten Geschäftsabwicklungen sowie Rechnungen in der Rezeption, erledigte Geschäftsfälle im Archiv. Verträge mit Auftragsverarbeitern sind, je nach Thematik, in der Rezeption und/oder Archiv.

4. Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen⁹

a. Kategorien der verarbeiteten Daten und ankreuzen, ob sie an Empfänger¹⁰ übermittelt werden

⁶ 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“](#).

⁷ Siehe zu den Informationspflichten das Merkblatt [„Informationspflichten“](#).

⁸ 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 Arbeits erleichterung).

⁹ 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“).

¹⁰ 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

Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO ¹¹ , strafrechtlich relevant iSd Art 10 DSGVO ¹²	Banken	Rechtsvertreter im Geschäftsfall	Wirtschaftstreuhänder	Gerichte im Anlassfall	Verwaltungsbehörden im Anlassf.	Inkassounternehmen im Anlassf.	Tourismuspartner (Bergbahnen, MT)	Mitwirkende Vertrags- u. Geschäftspartner	Versicherungen im Anlassfall	Provider (ID-Dienstleister)
1	1	Name, Firma oder sonstige Geschäftsbezeichnung	Nein	X	X	X	X	X	X	X	X	X	X
	2	Anschrift	Nein	X	X	X	X	X	X	X	X	X	X
	3	Kontaktdaten	Nein	X	X	X	X	X	X	X	X	X	X
	4	Firmenbuchdaten	Nein	X	X	X	X	X	X	X	X	X	X
	5	Daten zur Bonität inkl. Mahn- und Klagsdaten	Nein		X		X						
	6	Bankverbindungen	Nein	X	X	X	X	X	X	X	X	X	
	7	Kreditkartennummern und -unternehmen	Nein	X	X	X	X						
	8	UID-Nummer	Nein	X	X	X	X	X	X	X	X	X	
	9	Namen der Kontaktperson	Nein	X	X	X	X	X	X	X	X	X	X

Empfänger nicht ausreichen, weil daraus nicht eruiert werden kann, ob die Daten rechtmäßig an die Muttergesellschaft und/oder an Schwestergesellschaften übertragen werden).

¹¹ 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.

¹² Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen unter behördlicher Aufsicht.

	10	<i>Kontaktdaten der Kontaktperson (Tel., Mail, Fax, Anschrift odgl.)</i>	<i>Nein</i>	X	X	X	X	X	X	X	X	X	X
	11	<i>Vertragstexte und Geschäftskorrespondenzen</i>	<i>Nein</i>	X	X	X	X	X	X	X		X	
2	12	Name	<i>Nein</i>	X	X	X	X	X	X	X	X	X	X
	13	Funktion des betroffenen Sachbearbeiters beim Verantwortlichen	<i>Nein</i>	X	X	X	X	X	X	X	X	X	X
	14	Vom betroffenen Sachbearbeiter bearbeitete Fälle	<i>Nein</i>	X	X	X	X	X	X	X	X	X	X
	15	Umfang der Vertretungsbefugnis	<i>Nein</i>	X	X	X	X	X	X	X	X	X	X
3	16	Name, Firma oder sonstige Geschäftsbezeichnung	<i>Nein</i>	X	X	X	X	X	X	X	X	X	X
	17	Anschrift	<i>Nein</i>	X	X	X	X	X	X	X	X	X	X
	18	Kontaktdaten (Tel., Mail, Fax odgl.)	<i>Nein</i>	X	X	X	X	X	X	X	X	X	X
	19	Firmenbuchdaten		X	X	X	X	X	X	X	X	X	X
	20	Namen der Kontaktpersonen		X	X	X	X	X	X	X	X	X	X
	21	Kontaktdaten der Kontaktpersonen (Tel., Mail, Fax, Anschrift odgl.)		X	X	X	X	X	X	X	X	X	X
	22	UID-Nummer		X	X	X	X	X	X	X	X	X	X
	23	Bankverbindungen		X	X	X	X	X	X	X	X	X	
	24	Kreditkartennummern und -unternehmen		X	X	X	X						
	25	Daten zur Bonität inkl. Mahn- und Klagsdaten			X	X	X						

b. Löschungs- und Aufbewahrungsfristen (wenn möglich)

Daten aus 4.a. (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1-4; 6-25;	Aufgrund der gesetzlichen Aufbewahrungsfristen auf jeden Fall 7 Jahre; darüberhinausgehend bis zur Beendigung eines allfälligen Rechtsstreits,
5; 25;	Bis zur Beendigung der Geschäftsbeziehung

5. Kategorien von Empfängern¹³, an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern¹⁴

a. 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)
Banken		
Rechtsvertreter im Geschäftsfall		
Wirtschaftstreuhand		
Gerichte		
Verwaltungsbehörden		
Inkassounternehmen		
Fremdfinanzierer		
Mitwirkende Vertrags- und Geschäftspartner		
Versicherungen im Anlassfall		
Privider (IT-Dienstleister)		

b. 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):

¹³ 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 eruiert werden kann, ob die Daten rechtmäßig an die Muttergesellschaft und/oder an Schwestergesellschaften übertragen werden).

¹⁴ Siehe dazu das Merkblatt „[Internationaler Datenverkehr](#)“. Bei Empfängern in Drittstaaten (speziell in den USA wegen dem „Privacy Shield“-System) empfiehlt sich eine namentliche Nennung des Empfängers.

D. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

a. Vertraulichkeit¹⁵:

Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen und zum Datenarchiv (Digital und Ordner) mit Schließanlage und Alarmanlage

Zugangskontrolle: Schutz vor unbefugter Systembenutzung: Kennwörter

Zugriffskontrolle: Benutzerverwaltung bzw. Dateiverwaltung (Rechteverwaltung)

b. Integrität¹⁶:

Weitergabekontrolle: Verschlüsselung

Eingabekontrolle: Protokollierung und Rechtekontrolle der Datenverarbeitungsprogramme

c. Verfügbarkeit und Belastbarkeit:

Verfügbarkeitskontrolle: Backup-Strategie , Firewall, Virenschutz

d. Pseudonymisierung und Verschlüsselung:

e. Evaluierungsmaßnahmen:

Datenschutz-Management: jeweils zum Saisonstart gibt es eine Schulung sowie eine Analyse

¹⁵ Verhinderung von (unbeabsichtigter) Offenlegung oder unbefugten Zugang zu personenbezogenen Daten.

¹⁶ Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.