

## Vertrag für die Auftragsverarbeitung gem Art 28 EU-DSGVO

zwischen

---

---

---

**Kundennummer**

nachstehend „Auftraggeber“ genannt,

---

**Techem Messtechnik GmbH**

**St. Bartlmä 2a**

**A-6020 Innsbruck**

nachstehend „Auftragnehmer“ genannt.

### 1. Allgemeines

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers iSd Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (EU-DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung der personenbezogenen Daten.
2. Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ iSd Art. 4 Nr. 2 EU-DSGVO zugrunde gelegt. Gleiches gilt für den Begriff „personenbezogene Daten“ analog; hier wird Art. 4 Nr. 1 EU-DSGVO zugrunde gelegt
3. Die Datenverarbeitung erfolgt im Rahmen der Erbringung von unter Punkt 2. beschriebenen Dienstleistungen aufgrund gesonderter Beauftragungen (hiernach „Leistungsvereinbarungen“) des Auftragnehmers durch den Auftraggeber als Eigentümer der von den Leistungsvereinbarungen betroffenen Objekte oder handelnd als bevollmächtigter Vertreter (Verwalter) im Namen der jeweiligen Eigentümer/Eigentümergeinschaften.
4. Der Auftraggeber ist im Zusammenhang mit den jeweiligen Leistungsvereinbarungen entweder selbst (ggf gemeinsamer) Verantwortlicher iSd EU-DSGVO oder Auftragsverarbeiter des Verantwortlichen und wird die Geltendmachung der Rechte des/der (anderen) Verantwortlichen koordinieren und alleine gegenüber dem Auftragnehmer wahrnehmen. Die Stellung der vom Auftraggeber im Rahmen der Leistungsvereinbarungen vertretenen Eigentümer/Eigentümergeinschaften als (ggf gemeinsame) Verantwortliche bleiben hiervon ebenso unberührt, wie ihre Stellung als Vertragspartner des Auftragnehmers und die Ausübung ihrer Rechte nach den jeweiligen Leistungsvereinbarungen.
5. Mit Unterfertigung dieses Vertrages ersetzt er eine eventuell bestehende Vereinbarung oder einen bestehenden Vertrag zur Auftragsdatenverarbeitung nach Art. 28 EU-DSGVO zwischen den Vertragsparteien.

### 2. Gegenstand des Auftrags

1. Dieser Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien hinsichtlich der jeweiligen Leistungsvereinbarungen und findet Anwendung auf alle hiermit verbundenen Tätigkeiten und Geschäftsbeziehungen mit dritten Parteien.
2. Dieser Vertrag betrifft die Durchführung von

- a) Lieferung, Aufnahme, Montage und Inbetriebnahme von Mess- und Erfassungsgeräten zum Zwecke der Verteilung und Abrechnung von Wärmekosten (und gegebenenfalls Kaltwasser- und Kältekosten),
- b) Ablesen der Mess- und Erfassungsgeräte zum Zwecke der Abrechnung von Wärmekosten (und gegebenenfalls Kaltwasser- und Kältekosten),
- c) Verarbeitung, Plausibilisierung und Abrechnung von Wärmekosten (und gegebenenfalls Kaltwasser, Kälte und Hausnebenkosten) gemäß gesetzlicher Vorschriften,
- d) Zurverfügungstellung von Verbrauchsinformationen,
- e) Zurverfügungstellung und Aufbereitung von Verbrauchs- und Abrechnungsinformationen über das Online-Kundenportal/Datentausch,
- f) Übermittlung der Abrechnungen an Auftraggeber und / oder Abnehmer durch den Auftragnehmer.

### **3. Dauer des Auftrags**

1. Der Vertrag beginnt mit Unterzeichnung und wird auf unbestimmte Zeit geschlossen. Beide Parteien können den Vertrag mit einer Frist von sechs Monaten unter gleichzeitiger Beendigung der Geschäftsbeziehungen zum Monatsende kündigen.
2. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer die Kontrollrechte des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus den Vorschriften der Art. 28 - 34 EU-DSGVO abgeleiteten Pflichten stellen einen solch schweren Verstoß dar, der zur Kündigung berechtigt.
3. Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht oder nicht rechtzeitig, so ist der Auftraggeber zur fristlosen Kündigung berechtigt.
4. Klarstellend wird festgehalten, dass die Auflösung von Leistungsvereinbarungen nur für einzelne, nicht aber für alle Objekte, zu keiner Auflösung dieser Vereinbarung führt.

### **4. Konkretisierung von Art, Zweck und Kategorien**

1. Art und Zweck der Verarbeitung sind
  - a) Ablesung der Verbrauchserfassungsgeräte,
  - b) verbrauchsabhängige Abrechnung,
  - c) Zurverfügungstellung von Verbrauchsinformationen,
  - d) Zurverfügungstellung und Aufbereitung von Verbrauchs- und Abrechnungsinformationen über das Online-Kundenportal/Datentausch.
2. Folgende Arten von personenbezogenen Daten können von der Verarbeitung betroffen sein:
  - a) Personenstammdaten (zB Name, Titel, Geschlecht)
  - b) Kommunikationsdaten (zB Telefon, E-Mail)
  - c) Verbrauchsdaten (zB Wärmeverbrauch, Wasserverbrauch)
  - d) Sonstige Abrechnungsdaten und Abrechnungshistorie (zB beheizbare Nutzfläche, Art und Anzahl der Messgeräte)
  - e) Kunden- und Anlagenhistorie (zB Einlagezahl)
  - f) Finanzdaten (zB UID-Nr)
3. Folgende Kategorien von Personen können von der Verarbeitung betroffen sein:
  - a) Abnehmer gemäß § 2 Z 4 Heiz- und Kältekostenabrechnungsgesetz – HeizKG sowie sonstige Nutzer/-innen und Eigentümer/-innen von Wohnungen und gewerblichen Einheiten

## **5. Rechte und Pflichten des Auftraggebers**

1. Für die Beurteilung der Rechtmäßigkeit der Verarbeitung nach Art. 6 Abs. 1 EU-DSGVO sowie für den Zweck der Verarbeitung ist allein der Auftraggeber verantwortlich. Dieser ist „Verantwortlicher“ iSd Art. 4 Nr. 7 EU-DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer.
2. Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte im Zusammenhang mit dieser Verarbeitung von Daten im Auftrag gegenüber dem Auftragnehmer geltend machen.
3. Der Auftraggeber kann weisungsberechtigte Personen benennen. Für den Fall, dass weisungsberechtigte Personen benannt werden oder sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.
4. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) oder Schriftform und von hierzu berechtigten Personen erfolgen.
5. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.
6. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.
7. Für den Fall, dass eine Informationspflicht gegenüber Dritten aufgrund einer Verletzung des Schutzes personenbezogener Daten nach Art. 33, 34 EU-DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

## **6. Allgemeine Pflichten des Auftragnehmers**

1. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen als die in diesem Vertrag vereinbarten, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen und Zustimmung des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit diese zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder zur Einhaltung von gesetzlichen Aufbewahrungspflichten erforderlich sind.
2. Der Auftragnehmer sichert zu, die erforderlichen technischen und organisatorischen Maßnahmen, wie in Anlage 1 beschrieben, einzuhalten, fortzuentwickeln und diese den sich verändernden Bedingungen anzupassen. Ein Unterschreiten der beschriebenen Maßnahmen wird ausgeschlossen.
3. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.
4. Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. Eine Verarbeitung der personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers, die zumindest in Textform (z.B. E-Mail durch berechtigte Personen) erfolgen muss. Eine Zustimmung des Auftraggebers kommt nur dann in Betracht, wenn gewährleistet ist, dass die jeweils nach den Art. 44 ff. EU-DSGVO einzuhaltenden Rechtsvorschriften eingehalten werden, um ein angemessenes Schutzniveau für den Schutz der personenbezogenen Daten zu gewährleisten.

5. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten oder rechtlich verpflichtenden Maßnahmen zu.
6. Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme oder Einflussnahme Dritter geschützt sind.
7. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.
8. Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

## **7. Datenschutzbeauftragter des Auftragnehmers**

1. Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 EU-DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt.

---

### **Externer Datenschutzbeauftragter des Auftragnehmers:**

#### **b-pisec GmbH**

Herr Björn Bausch  
Frankfurter Straße 2  
65549 Limburg an der Lahn  
Deutschland  
+49 6431 90291 22  
kontakt@b-pisec.com

---

## **8. Meldepflichten des Auftragnehmers**

1. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.
2. Der Auftragnehmer informiert den Auftraggeber unverzüglich über die Anfrage auf Datenzugriff durch eine Behörde oder andere staatliche Stelle, die die Daten des Auftraggebers betrifft. Der Auftragnehmer stellt sicher, rechtzeitig gegen dieses Zugriffersuchen Widerspruch einzulegen, sofern der Auftraggeber dies wünscht.
3. Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht im Falle von Datenschutzverletzungen nach Art. 33, 34 EU-DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten nach besten Kräften unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
  - eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
4. Meldungen an die Aufsichtsbehörden nach Art. 33 oder 34 EU-DSGVO liegen im Verantwortungsbereich des Auftraggebers und dürfen nur nach voriger Weisung des Auftraggebers (Schriftform oder Textform) durch den Auftragnehmer erfolgen.
  5. Wendet sich eine betroffene Person direkt an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen und den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer darf dem Betroffenen in diesem Zusammenhang die Kontaktdaten des Verantwortlichen mitteilen. Hat der Auftragnehmer den Antrag der betroffenen Person unverzüglich weitergeleitet, so haftet dieser nicht, wenn der Auftraggeber das Ersuchen nicht, nicht richtig oder nicht rechtzeitig beantwortet.

## **9. Mitwirkungspflichten des Auftragnehmers**

1. Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12 - 23 EU-DSGVO nach besten Kräften.
2. Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber nach besten Kräften mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.
3. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32 - 36 EU-DSGVO genannten Pflichten nach besten Kräften.
4. Soweit der Auftraggeber einer Kontrolle, einem Ordnungswidrigkeiten- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Leistungserbringung durch den oder Auftragsverarbeitung bei dem Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

## **10. Kontrollbefugnisse**

1. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht zur Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen, sei es auch durch von ihm beauftragte Dritte, eingeräumt, wobei der Auftraggeber dem Auftragnehmer die beabsichtigte Ausübung dieses Rechts unter Einhaltung einer angemessenen Frist voranzukündigen hat. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

## **11. Unterauftragsverhältnisse**

1. Der Auftragnehmer kann weitere Auftragsverarbeiter für Tätigkeiten gemäß Punkt 2 (2) hinzuziehen.
2. Eine Liste der vom Auftraggeber hiermit genehmigten Sub-Auftragsverarbeiter findet sich auf [www.techem.at/dsgvo](http://www.techem.at/dsgvo) (Liste der Sub-Auftragsverarbeiter) und [www.techem.at/ableserliste](http://www.techem.at/ableserliste) (Ableserliste).
3. Der Auftragnehmer hat den Auftraggeber von der beabsichtigten Heranziehung weiterer Auftragsverarbeiter so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. Der Auftragnehmer kommt dieser Informationspflicht dergestalt nach, dass er mindestens 14 Tage vor der beabsichtigten Heranziehung eines

weiteren Auftragnehmers die Liste unter [www.techem.at/dsgvo](http://www.techem.at/dsgvo) bzw. [www.techem.at/ableserliste](http://www.techem.at/ableserliste) aktualisiert. Der Auftraggeber wird diese Liste regelmäßig einsehen.

4. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art. 28 Abs. 4 DSGVO mit dem weiteren Auftragsverarbeiter ab.
5. Der Auftragnehmer hat sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingetht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.
6. Nicht als Unterauftragsverhältnisse iSd Absätze 1 bis 5 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten.
7. Die Wartung und Pflege von IT-Systemen oder Applikationen durch Dritte stellt ein zustimmungs-pflichtiges Unterauftragsverhältnis und Auftragsverarbeitung iSd Art. 28 EU-DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betreffen, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und z.B. bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

## **12. Vertraulichkeitsverpflichtung**

1. Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten verpflichtet, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt. Der Auftragnehmer verpflichtet sich, mindestens die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.
2. Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.
3. Die Verpflichtung auf Vertraulichkeit besteht auch nach Beendigung des Vertrages fort.

## **13. Wahrung von Betroffenenrechten**

1. Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12 - 23 EU-DSGVO zu bearbeiten, nach besten Kräften zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 EU-DSGVO nachkommen kann.
2. Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer unverzüglich die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach besten Kräften mit geeigneten technischen und

organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

3. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

#### **14. Regellöschung von Daten**

1. Die Löschung der Daten erfolgt – unter Berücksichtigung der gesetzlichen Aufbewahrungsfristen und sofern sie für die Erbringung der Leistungen nicht mehr erforderlich sind – nach einer Lösungsfrist von 7 Jahren nach Erhebung. Abweichende Einzelweisungen sind zulässig, wenn sie nicht den gesetzlichen Aufbewahrungsfristen widersprechen; der Auftragnehmer kann hierzu eine angemessene Vergütung verlangen.

#### **15. Geheimhaltungspflichten**

1. Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.
2. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

#### **16. Vergütung**

1. Etwaige Regelungen zu einer Vergütung von Leistungen sind zwischen den Parteien gesondert zu vereinbaren.

#### **17. Technische und organisatorische Maßnahmen zur Datensicherheit**

1. Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 EU-DSGVO.
2. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 1 zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.
3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit hin kontrollieren.

#### **18. Beendigung**

1. Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

2. Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

## 19. Zurückbehaltungsrecht

1. Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer iSd § 471 ABGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

## 20. Schlussbestimmungen

1. Für Nebenabreden ist die Schriftform erforderlich.
2. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht. Die Vertragsparteien verpflichten sich, solche Teile des Vertrages durch neue Bestimmungen zu ersetzen, die dem Zweck und Willen der Parteien sowie dem hiervon betroffenen Teil des Vertrages in rechtlich zulässiger Weise entsprechen.
3. Es gilt österreichisches Recht. Ausschließlicher Gerichtsstand für Streitigkeiten aus oder im Rahmen dieses Vertragsverhältnisses ist Innsbruck.

*Hinweis: Bevor Sie diese Vereinbarung bestätigen, vergewissern Sie sich Ihrer Vertretungsbefugnis (bzw. Ihrer internen Bevollmächtigung).*

---

Der Auftraggeber:

---

---

Datum, Unterschrift

---

---

Der Auftragnehmer:

---

---

Datum, Unterschrift

---

# Anlage 1

## Technische und organisatorische Maßnahmen

### Vertraulichkeit

---

#### Zutrittskontrolle

Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen mit denen personenbezogene Daten verarbeitet werden durch:

- Schlüsselregelung
- Elektrische Türöffner mit personenbezogenen RFID-Transpondern
- Alarmanlagen

---

#### Zugangskontrolle

Schutz vor unbefugter Systembenutzung durch:

- Authentifikation mit Benutzer + Passwort + Multifaktor Authentifizierung
- Die Richtlinien der Passwörter wird dem Stand der Technik angepasst
- Verschlüsselung von Datenträgern
- Automatische Sperrmechanismen Mitarbeiterclients
- Einsatz von Firewalls
- Einsatz von Mobile Device Management

---

#### Zugriffskontrolle

Gewährleistung, dass die zu Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können durch:

- Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb der Dokumentenablagen durch rollenbasierte Berechtigung.
- Überprüfen der vergebenen Berechtigungen bzw. wechseln der Administratorkennwörter durch administrative Benutzerkonten.
- Löschen/Deaktivieren ausgeschiedener Benutzerkonten bzw. Änderung des Passwortes.
- Ordnungsgemäße Vernichtung von Datenträgern
- Sichere Aufbewahrung von Datenträgern
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Einsatz von Dienstleistern zur Akten- und Datenvernichtung mit Zertifikat

---

#### Pseudonymisierung

Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung so anonymisiert, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

---

### Integrität

---

#### Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

- Virtual Private Networks
- Client- und Benutzerzertifikaten
- lokaler Gruppenrichtlinien
- Zertifikate für Kunden
- Verschlüsselung

---

#### Eingabekontrolle:

- Protokollierung der Eingabe, Änderung und Löschung von Daten durch ein Dokumentenmanagement System.
  - Dokumentation mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
  - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes
-

## Verfügbarkeit und Belastbarkeit

---

### Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

- USV
  - Backup-Strategie
  - Virenschutz
  - Firewall
  - Security Checks auf Infrastruktur- und Applikationsebene
  - Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
  - Auslagerung der Sicherung in ein Ausweichrechenzentrum
  - Klimaanlage in Serverräumen
  - Löschanlage
- 

### Wiederherstellbarkeit

- Spiegelung der Infrastruktur in Ausweichrechenzentrum
- 

### Trennungsgebot

- Trennung von Produktiv- und Testsystemen
  - Festlegung von Datenbankrechten
  - Logische Mandantentrennung (softwareseitig)
  - Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- 

## Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

---

- Datenschutz-Management durch Datenschutzbeauftragten
  - Regelmäßige Mitarbeiter Schulungen
  - Incident-Response-Management durch Notfallpläne
  - Zertifizierung des Konzernrechenzentrums mit ISO
-